TeleTrusT Germany
The IT Security Association.

Glossary of IT Security Terminology Terms and definitions

(ISO/IEC JTC 1 SC 27 Standing Document No. 6; V2010-09)

Imprint

Publisher:

TeleTrusT Germany (TeleTrusT Deutschland e.V.)
Chausseestrasse 17
10115 Berlin
GERMANY
Tel.: +49 30 400 54 306
Fax: +49 30 400 54 311
E-Mail: info@ TeleTrusT.de
http://www.TeleTrusT.de

Printing:

DATEV eG, Nuremberg

This documentation comprises IT security related terms and definitions as laid down in ISO/IEC JTC 1 SC 27 Standing Document 6 ("SD 6") "Glossary of IT Security Terminology - Terms and definitions" (Version 2010-09). Some notes contain references to documents the definition originates from.

TeleTrusT wants to thank the Standards Committee for Information Technology and Applications (NIA; DIN German Institute for Standardization) for kindly providing support.

Abbreviations:

ISO	International Organization for Standardization
IEC	International Electrotechnical Commission
JTC 1	Joint Technical Committee 1 ("Information technology")
SC	Subcommittee (JTC 1/SC 27: "IT Security techniques")
WD	Working Draft
ed.	Edition

Term	Definition	ISO/IEC JTC 1/SC 27 Document
ACBio instance	report generated by a biometric processing unit (BPU) compliant to this International Standard to show the validity of the result of one or more subprocesses executed in the BPU ■	ISO/IEC 24761: 2009-05-15 (1st ed.)
acceptance criteria	criteria to be applied when performing the acceptance procedures (e.g. successful document review, or successful testing in the case of software, firmware or hardware) ■	ISO/IEC 15408-1: 2009-12-15 (3rd ed.)
acceptance procedures	procedures followed in order to accept newly created or modified configuration items as part of the TOE, or to move them to the next step of the life-cycle NOTE These procedures identify the roles or individuals responsible for the acceptance and the criteria to be applied in order to decide on the acceptance. There are several types of acceptance situations some of which may overlap: a) acceptance of an item into the configuration management system for the first time, in particular inclusion of software, firmware and hardware components from other manufacturers into the TOE ("integration"); b) progression of configuration items to the next life-cycle phase at each stage of the construction of the TOE (e.g. module, subsystem, quality control of the finished TOE); c) subsequent to transports of configuration items (for example parts of the TOE or preliminary products) between different development sites; d) subsequent to the delivery of the TOE to the consumer. ■	ISO/IEC 15408-1: 2009-12-15 (3rd ed.)
access control	means to ensure that access to assets (2.3) is authorized and restricted based on business and security requirements ■	N8718: 1st WD 27000: 2010-05-27
access control	The ability to allow only authorized users, programs or processes system or resource access An entire set of procedures performed by hardware, software and administrators, to monitor access, identify users requesting access, record access attempts, and grant or deny access based on pre-established rules ■	N8812: 3rd WD 29146: 2010-07-14
access management	Processes of securing the access to ICT information resources ■	N8812: 3rd WD 29146: 2010-07-14
Access Point - AP	the system providing access from a wireless network to a terrestrial network. ■	ISO/IEC 18028-4: 2005-04-01 (1st ed.)
account provisioning	Access to ICT resources may be provided through temporary IT accounts. IT account provisioning is specific to each system and involves the assignment of a unique identifier for each account. Entities will be held accountable for their use of the account by linking activities with the assigned identifier ■	N8812: 3rd WD 29146: 2010-07-14
accountability	assignment of actions and decisions to an entity ■	N8718: 1st WD 27000: 2010-05-27

Term	Definition	ISO/IEC JTC 1/SC 27 Document
accountability	property that ensures that the actions of an entity may be traced uniquely to the entity [ISO 7498-2] ■	ISO/IEC 13888-1: 2009-07-15 (3rd ed)
accountability	property that ensures that the actions of an entity can be traced uniquely to the entity [ISO/IEC 7498-2:1989] ■	ISO/IEC 21827: 2008-10-15 (2nd ed.)
accountability	property that ensures that the actions of an entity may be traced uniquely to the entity [ISO 7498-2] ■	N8812: 3rd WD 29146: 2010-07-14
accreditation	formal declaration by a designated approving authority that a system is approved to operate in a particular security mode using a prescribed set of safeguards NOTE This definition is generally accepted within the security community; within ISO the more generally used definition is: Procedure by which an authoritative body gives formal recognition that a body or person is competent to carry out specific tasks [ISO/IEC Guide 2]. ■	ISO/IEC 21827: 2008-10-15 (2nd ed.)
accreditation	Procedure by which an authoritative body gives formal recognition, approval, and acceptance of the associated residual risk: a) for the operation of an automated system in a particular security mode using a particular set of safeguards [adapted from AGCA]; b) that a security body or person is competent to carry out specific tasks [adapted from ISO/IEC Guide 2]; and c) that a security service is suitable for the target environment. ■	ISO/IEC TR 15443-1: 2005-02-01 (1st ed.)
accreditation exponent	secret number related to the verification exponent and used in the production of private keys ■	ISO/IEC 9798-5: 2009-12-15 (3rd ed.)
acquirer	individual or organization that acquires or procures a product or online service from a supplier NOTE 1 Adapted from ISO/IEC 12207:2008. NOTE 2 The acquirer could be one of the following: buyer, customer, owner, purchaser. ■	N8780: 1st CD 29147: 2010-06-10
acquirer	organization that procures a service from a supplier ■	N8638: 3rd WD 27036: 2010-08-13

Term	Definition	ISO/IEC JTC 1/SC 27 Document
acquisition	process of creating an evidential copy of all data within a defined set NOTE The product of an acquisition is a digitally accurate and evidentially reliable duplicate of the original source data ■	N8640: 3rd WD 27037: 2010-05-31
action	evaluator action element of ISO/IEC 15408-3 NOTE These actions are either explicitly stated as evaluator actions or implicitly derived from developer actions (implied evaluator actions) within ISO/IEC 15408-3 assurance components. ■	N8912: Corrected 18045: 2010-09-15
active	state of an entity in which the entity can obtain the *shared secret key* ■	N8743: 2nd CD 11770-5: 2010-07-29
active impostor attempt	attempt in which an individual tries to match the stored template of a different individual by presenting a simulated or reproduced biometric sample, or by intentionally modifying his/her own biometric characteristics ■	ISO/IEC 19792: 2009-08-01 (1st ed.)
activity	application of an assurance class of ISO/IEC 15408-3 ■	N8912: Corrected 18045: 2010-09-15
actor	someone or something initiating interaction with any process in the Application Life Cycle Security Reference Model or any process provided or impacted by the application ■	N8632: FCD 27034-1: 2010-05-27
actor	entity involved in a step within a scenario. The actor and associated step are labelled in a sequence diagram. Actors are classes that define roles that objects external to a system may play. They are used to model users outside of a system that interact directly with the system as part of coherent work units. This includes human users and other systems. [UML] ■	N8812: 3rd WD 29146: 2010-07-14
actual application level of trust	result of a verification process that confirms by providing evidence that all Application Security Controls required by the application's targeted level of trust were correctly implemented, correctly verified and produced the expected result ■	N8632: FCD 27034-1: 2010-05-27
adaptation parameter	public key specific to the modulus and used in the definition of public keys in the GQ2 mechanisms ■	ISO/IEC 9798-5: 2009-12-15 (3rd ed.)
administrator	entity that has a level of trust with respect to all policies implemented by the TSF NOTE Not all PPs or STs assume the same level of trust for administrators. Typically administrators are assumed to adhere at all times to the policies in the ST of the TOE. Some of these policies may be related to the functionality of the TOE, others may be related to the operational environment. ■	ISO/IEC 15408-1: 2009-12-15 (3rd ed.)

Term	Definition	ISO/IEC JTC 1/SC 27 Document
administrator guidance	written material that is used by the Crypto Officer and/or other administrative roles for the correct configuration, maintenance, and administration of the cryptographic module ■	N8776: 2nd WD 19790: 2010-07-16
Advanced Encryption Standard - AES	a symmetric encryption mechanism providing variable key length and allowing an efficient implementation specified as Federal Information Processing Standard (FIPS) 197. ■	ISO/IEC 18028-4: 2005-04-01 (1st ed.)
adversarial model	description of adversary with which a protocol is supposed to be executed NOTE It includes restriction on available resources, ability of intruders, etc. ■	N8778: 3rd CD 29128: 2010-06-11
adverse actions	actions performed by a threat agent on an asset ■	ISO/IEC 15408-1: 2009-12-15 (3rd ed.)
advisory	announcement or bulletin that serves to inform, advise and usually warn users about a vulnerability of a product NOTE A vulnerability advisory may include advice on how to deal with the vulnerability. An advisory typically contains a description of the vulnerability including a list of vulnerable software, potential impact, resolution and mitigation information, and references. An advisory may be published by a vendor, finder, or coordinator. ■	N8780: 1st CD 29147: 2010-06-10
adware	application which pushes advertising to users and/or gathers user online behaviour. The application may or may not be installed with the user's knowledge or consent or forced onto the user via licensing terms for other software ■	N8624: 2nd CD 27032: 2010-06-15
aggregation	process of generating a proxy data item for a group of data items that are linked together, producing a verifiable cryptographic link between each data item and the rest of the group ■	ISO/IEC 18014-3: 2009-12-15 (2nd ed.)
alert	"instant" indication that an information system and network may be under attack, or in danger because of accident, failure or human error ■	ISO/IEC 27033-1: 2009-12-15 (1st ed.)
algorithm	clearly specified mathematical process for computation; a set of rules that, if followed, will give a prescribed result ■	N8745: FCD 18031: 2010-05-18
allocated space	space on electronic media that is currently used by any file, file system information or media information ■	N8640: 3rd WD 27037: 2010-05-31
alternate site	alternate operating location selected to be used by an organization when normal business operations cannot be carried out using the normal location after a disruption has occurred ■	N8622: PreFDIS 27031: 2010-08-18
analytical model	algorithm or calculation combining one or more base and/or derived measures with associated decision criteria [ISO/IEC 15939:2007] ■	ISO/IEC 27004: 2009-12-15 (1st ed.)

Term	Definition	ISO/IEC JTC 1/SC 27 Document
ancestor keys of key k	set of *keys* in a *logical key hierarchy* and these *keys* are assigned to the *ancestor nodes* of the node where k is assigned NOTE One of the keys in a set of ancestor keys must be the shared secret key or a key encryption key. ■	N8743: 2nd CD 11770-5: 2010-07-29
ancestor nodes of node v	set of nodes in a *tree* and these nodes can be reached by repeatedly going to the *parent node* from v ■	N8743: 2nd CD 11770-5: 2010-07-29
anonymity	condition which requires that a PII controller or any other party/entity is unable to directly or indirectly determine the identity of the PII principal ■	N8806: 4th CD 29100: 2010-06-10
anonymization	process by which PII is irreversibly removed or altered in such a way that a PII principal can no longer be identified directly or indirectly neither by the PII controller alone nor in collaboration with any other party ■	N8806: 4th CD 29100: 2010-06-10
anonymized PII	PII that has been subject to a process of anonymization and that can no longer be used to identify, or re-identify, a PII principal ■	N8806: 4th CD 29100: 2010-06-10
anonymous digital signature	digital signature mechanism in which given a digital signature, the signer's identifier cannot be discovered by any unauthorised entity ■	N8763: 1st WD 20009-2: 2010-06-20
anonymous entity authentication	entity authentication in which the identifier of the claimant is not revealed to any unauthorized party, including the verifier ■	N8762: 1st WD 20009-1: 2010-07-13
anonymous identifier	identifier (3.1.4) that contains no PII (3.6.1) NOTE An anonymous identifier contains sufficient identity information to allow a verifier to distinguish two entities while not being able to link to a specific known identity. EXAMPLE A pseudonym created in one domain might be used as an anonymous identifier in another domain. ■	N8804: 3rd CD 24760-1: 2010-06-11
anonymous signature	signature which can be verified by using a group public key or multiple public keys, and which can not be traced to the distinguishing identifier for its signer by any unauthorised entity ■	N8760: 1st WD 20008-1: 2010-06-14
anonymous signature	signature which can be verified using a group public key or multiple individual public keys, and which cannot be traced to the distinguishing identifier of its signer by any unauthorized entity ■	N8762: 1st WD 20009-1: 2010-07-13
anonymous signature mechanism	signature mechanism in which given a signature, the distinguishing identifier for its signer cannot be discovered by any unauthorised entity ■	N8760: 1st WD 20008-1: 2010-06-14
appendix	string of bits formed by the signature and an optional text field ■	ISO/IEC 14888-1: 2008-04-15 (2nd ed.)

Term	Definition	ISO/IEC JTC 1/SC 27 Document
applicant	an entity (organisation, individual etc.) which requests the assignment of a register entry and entry label ■	ISO/IEC 15292: 2001-12-15 (1st ed.)
application	IT solution, including application software, designed to help users perform particular tasks or handle particular types of IT problems [ISO/IEC 27034(to be published)] ■	N8624: 2nd CD 27032: 2010-06-15
application	IT solution, including application software, designed to help users perform particular tasks or handle particular types of IT problems that helps an organization to automate a business process or function NOTE Business processes include people and technologies ■	N8632: FCD 27034-1: 2010-05-27
Application Life Cycle Security Reference Model	set of processes, linked through precedence relationships, involved in application project management, application realisation and maintenance, infrastructure management and application audit, covering the project and operation stages of application projects ■	N8632: FCD 27034-1: 2010-05-27
Application Normative Framework	set of normative elements relevant for a specific application project, selected from the Organization Normative Framework ■	N8632: FCD 27034-1: 2010-05-27
application owner	role named by the organization to be responsible for the management, utilisation and protection of the application and of the data involved by the application NOTE 1 The application owner makes all decisions pertaining to the security of the application NOTE 2 In this document, the term "owner" is used as a synonym for "application owner". ■	N8632: FCD 27034-1: 2010-05-27
application project	endeavour with defined start and finish criteria undertaken to acquire an application in accordance with specified resources and requirements NOTE 1 Adapted from ISO 9000:2005. NOTE 2 For the purposes of this International Standard the start and finish criteria are such that the entire life cycle of the application is included in the application project. ■	N8632: FCD 27034-1: 2010-05-27
application security control	data structure containing a precise enumeration and description of a security activity and its associated verification measurement that will be performed at a specific point in an application life cycle NOTE This data structure should be described using the ebXML specifications from ISO/IEC 15000 ■	N8632: FCD 27034-1: 2010-05-27
application security management process	overall process involved in the management of security activities, actors, artefacts and verification for each specific application used by an organization ■	N8632: FCD 27034-1: 2010-05-27

Term	Definition	ISO/IEC JTC 1/SC 27 Document
application service provider	operator who provides a hosted software solution that provides application services which includes web based or client-server delivery models. Examples include online game operators, office application providers and online storage providers ■	N8624: 2nd CD 27032: 2010-06-15
application services	software with functionality delivered on-demand to subscribers through an online model which includes web based or client-server applications ■	N8624: 2nd CD 27032: 2010-06-15
application software	software designed to help users perform particular tasks or handle particular types of problems, as distinct from software that controls the computer itself [ISO/IEC 18019] ■	N8624: 2nd CD 27032: 2010-06-15
application software	software designed to help users perform particular tasks or handle particular types of problems, as distinct from software that controls the computer itself [ISO/IEC 18019] ■	N8632: FCD 27034-1: 2010-05-27
application specification	functionality, characteristic, component or service implemented in, or used by, an application. -> To be completed, if needed. ■	N8634: 2nd WD 27034-2: 2010-08-01
approach	The method used or steps taken in setting about a task or problem. ■	ISO/IEC TR 15443-1: 2005-02-01 (1st ed.)
approval authority	any national or international organization/ authority mandated to approve and/or evaluate security functions [ISO/IEC 19790:2006, 3.1] NOTE An approval authority in the context of this definition evaluates and approves security functions based on their cryptographic or mathematical merits but is not the testing entity which would test for conformance to this International Standard and ISO/IEC 19790:2006. ■	ISO/IEC 24759: 2008-07-01 (1st ed.)
approval authority	any national or international organisation/ authority mandated to approve security functions ■	N8776: 2nd WD 19790: 2010-07-16
approved data authentication technique	approved method that may include the use of a digital signature, message authentication code or keyed hash (e.g. HMAC) ■	N8776: 2nd WD 19790: 2010-07-16
approved integrity technique	approved hash, message authentication code or a digital signature algorithm ■	N8776: 2nd WD 19790: 2010-07-16
approved mode of operation	set of services which include at least one service that utilises an approved cryptographic algorithm, security function or process NOTE Not to be confused with a specific mode of an approved security function, e.g., Cipher Block Chaining (CBC) mode ■	N8776: 2nd WD 19790: 2010-07-16
approved security function	security function (e.g., cryptographic algorithm) that is specified in Annex C ■	N8776: 2nd WD 19790: 2010-07-16

Term	Definition	ISO/IEC JTC 1/SC 27 Document
architecture	fundamental organization of a system embodied in its components, their relationships to each other, and to the environment, and the principles guiding its design and evolution [ISO/IEC 15288:2008, definition 4.5] ■	ISO/IEC 27033-1: 2009-12-15 (1st ed.)
arity	number of arguments ■	N8778: 3rd CD 29128: 2010-06-11
assessment	verification of a product, system or service against a standard using the corresponding assessment method to establish compliance and determine the assurance NOTE Adapted from ISO/IEC TR 15443-1:2005. ■	ISO/IEC 21827: 2008-10-15 (2nd ed.)
assessment	verification of a deliverable against a standard using the corresponding method to establish compliance and determine the assurance. ■	ISO/IEC TR 15443-1: 2005-02-01 (1st ed.)
assessment	systematic examination of the extent to which an entity is capable of fulfilling specified requirements; synonymous to evaluation when applied to a deliverable [ISO/IEC 14598-1] ■	ISO/IEC TR 15443-3: 2007-12-15 (1st ed.)
assessment method	action of applying specific documented assessment criteria to a deliverable for the purpose of determining acceptance or release of that deliverable ■	ISO/IEC TR 15443-3: 2007-12-15 (1st ed.)
asset	any item that has a distinct value to the organization NOTE There are many types of assets, including: a) information (2.21); b) software, such as a computer program; c) physical, such as computer; d) services; e) people, and their qualifications, skills, and experience; and f) intangibles, such as reputation and image. ■	N8718: 1st WD 27000: 2010-05-27
asset	anything that has value to the organization [ISO/IEC TR 13335-1:1996] ■	ISO/IEC 21827: 2008-10-15 (2nd ed.)
asset	anything that has value to an individual, an organization or a government NOTE Adapted from ISO/IEC 27000 to make provision for individuals and the separation of governments from organizations (see the definition of organization). ■	N8624: 2nd CD 27032: 2010-06-15
assets	anything that has value to the organization ■	ISO/IEC TR 15443-3: 2007-12-15 (1st ed.)
assets	entities that the owner of the TOE presumably places value upon ■	ISO/IEC 15408-1: 2009-12-15 (3rd ed.)
assignment	specification of an identified parameter in a component (of ISO/IEC 15408) or requirement ■	ISO/IEC 15408-1: 2009-12-15 (3rd ed.)

Term	Definition	ISO/IEC JTC 1/SC 27 Document
assurance	grounds for confidence that a deliverable meets its security objectives NOTE 1 Adapted from ISO/IEC 15408-1:2005. NOTE 2 This definition is generally accepted within the security community; within ISO the more generally used definition is: Activity resulting in a statement giving confidence that a product, process or service fulfills specified requirements [ISO/IEC Guide 2]. ■	ISO/IEC 21827: 2008-10-15 (2nd ed.)
assurance	Performance of appropriate activities or processes to instil confidence that a deliverable meets its security objectives. a) Grounds for confidence that an entity meets its security objectives [ISO/IEC 15408–1]. ■	ISO/IEC TR 15443-1: 2005-02-01 (1st ed.)
assurance	grounds for confidence that a TOE meets the SFRs ■	ISO/IEC 15408-1: 2009-12-15 (3rd ed.)
assurance administrator	responsible (accountable) person for the selection, implementation, or acceptance deliverable ■	ISO/IEC TR 15443-3: 2007-12-15 (1st ed.)
assurance approach	grouping of assurance methods according to the aspect examined. ■	ISO/IEC TR 15443-1: 2005-02-01 (1st ed.)
assurance Argument	set of structured assurance claims, supported by evidence and reasoning, that demonstrate clearly how assurance needs have been satisfied ■	ISO/IEC 21827: 2008-10-15 (2nd ed.)
assurance argument	set of structured assurance claims, supported by evidence and reasoning, that demonstrate clearly how assurance needs have been satisfied. ■	ISO/IEC TR 15443-1: 2005-02-01 (1st ed.)
assurance assessment	verification and recording of the overall types and amounts of assurance associated with the deliverable (entered into the assurance argument). ■	ISO/IEC TR 15443-1: 2005-02-01 (1st ed.)
assurance authority	person or organisation delegated the authority for decisions (i.e. selection, specification, acceptance, enforcement) related to a deliverable's assurance that ultimately leads to the establishment of confidence in the deliverable. Note: In specific schemes or organisations, the term for assurance authority may be different such as evaluation authority. ■	ISO/IEC TR 15443-1: 2005-02-01 (1st ed.)
assurance authority	person or organisation delegated the authority for decisions (i.e. selection, specification, acceptance, enforcement) related to a deliverable's assurance that ultimately leads to the establishment of confidence in the deliverable NOTE In specific schemes or organisations, the term for assurance authority could be different such as evaluation authority. ■	ISO/IEC TR 15443-3: 2007-12-15 (1st ed.)
assurance case	a structured set of claims, arguments and a corresponding body of evidence to demonstrate that a system satisfies specific claims with respect to its security properties ■	N8784: 1st WD 20004: 2010-08-06

Term	Definition	ISO/IEC JTC 1/SC 27 Document
assurance case	representation of a claim or claims, and the support for these claims [ISO/IEC TR 15026-1:2010] ■	N8732: 3rd WD 29193: 2010-08-06
assurance Claim	assertion or supporting assertion that a system meets a security need NOTE Claims address both direct threats (e.g. system data are protected from attacks by outsiders) and indirect threats (e.g. system code has minimal flaws). ■	ISO/IEC 21827: 2008-10-15 (2nd ed.)
assurance concern	general type of assurance objective pursued by a major group of assurance authorities NOTE In this part of ISO/IEC TR 15443, assurance concern is used for the purpose of establishing analyses and conclusions for assurance guidance given to that group of users. ■	ISO/IEC TR 15443-3: 2007-12-15 (1st ed.)
assurance evidence	data on which a judgment or conclusion about an assurance claim may be based NOTE The evidence may consist of observation, test results, analysis results and appraisals. ■	ISO/IEC 21827: 2008-10-15 (2nd ed.)
assurance evidence	Work products resulting from the assurance analysis of the deliverable (including summary reports or other justification) that supports the assurance claim. ■	ISO/IEC TR 15443-1: 2005-02-01 (1st ed.)
assurance evidence	Workproducts or any items generated from the assurance analysis of the deliverable including reports (justification) to support the assurance claim. ■	ISO/IEC TR 15443-1: 2005-02-01 (1st ed.)
assurance goal	overall security expectations to be satisfied through application of formal and informal assessment activities ■	ISO/IEC TR 15443-3: 2007-12-15 (1st ed.)
assurance level	amount of assurance obtained according to the specific scale used by the assurance method ■	ISO/IEC 19792: 2009-08-01 (1st ed.)
assurance level	amount of assurance obtained according to the specific scale used by the assurance method. NOTE 1. the assurance level may not be measurable in quantitative terms. NOTE 2. The amount of assurance obtained is generally related to the effort expended on the activities performed. ■	ISO/IEC TR 15443-1: 2005-02-01 (1st ed.)
assurance method	recognised specification for obtaining reproducible assurance results. ■	ISO/IEC TR 15443-1: 2005-02-01 (1st ed.)
assurance property	characteristic of an assurance method that contributes to the assurance result. ■	ISO/IEC TR 15443-1: 2005-02-01 (1st ed.)
assurance result	Documented numerical or qualitative assurance statement pertaining to a deliverable. ■	ISO/IEC TR 15443-1: 2005-02-01 (1st ed.)

Term	Definition	ISO/IEC JTC 1/SC 27 Document
assurance scheme	administrative and regulatory framework under which an assurance method is applied by an assurance authority within a specific community or organisation. a) The administrative and regulatory framework under which the Common Criteria is applied by an evaluation authority within a specific community [ISO/IEC 15408–1]. ■	ISO/IEC TR 15443-1: 2005-02-01 (1st ed.)
assurance stage	deliverable life cycle stage on which a given assurance method is focused. The overall deliverable assurance takes into account the results of the assurance methods applied throughout the deliverable life cycle. ■	ISO/IEC TR 15443-1: 2005-02-01 (1st ed.)
asymmetric cipher	alternative term for asymmetric encryption system. ■	ISO/IEC 18033-1: 2005-02-01 (1st ed.)
asymmetric cipher	system based on asymmetric cryptographic techniques whose public transformation is used for encryption and whose private transformation is used for decryption [ISO/IEC 18033-1] NOTE See Clause 7. ■	ISO/IEC 18033-2: 2006-05-01 (1st ed.)
asymmetric cipher	alternative term for asymmetric encryption system [ISO/IEC 18033-1] ■	N8751: FCD 29150: 2010-06-10
asymmetric cryptographic technique	cryptographic technique that uses two related operations: a public operation defined by a public data item, and a private operation defined by a private data item (the two operations have the property that, given the public operation, it is computationally infeasible to derive the private operation) ■	ISO/IEC 9798-5: 2009-12-15 (3rd ed.)
asymmetric cryptographic technique	cryptographic technique that uses two related transformations: a public transformation (defined by the public key) and a private transformation (defined by the private key) NOTE The two transformations have the property that, given the public transformation, it is computationally infeasible to derive the private transformation. ■	ISO/IEC 9798-1: 2010-07-01 (3rd ed.)
asymmetric cryptographic technique	cryptographic technique that uses two related transformations, a public transformation (defined by the public key) and a private transformation (defined by the private key). The two transformations have the property that, given the public transformation, it is computationally infeasible to derive the private transformation. [ISO/IEC 11770-1:1996]. ■	ISO/IEC 18033-1: 2005-02-01 (1st ed.)

Term	Definition	ISO/IEC JTC 1/SC 27 Document
asymmetric cryptographic technique	cryptographic technique that uses two related transformations, a public transformation (defined by the public key) and a private transformation (defined by the private key). The two transformations have the property that, given the public transformation, it is computationally infeasible to derive the private transformation. [ISO/IEC 11770-1:1996] ■	ISO/IEC 18033-2: 2006-05-01 (1st ed.)
asymmetric cryptographic technique	cryptographic technique that uses two related operations: a public operation defined by a public data item, and a private operation defined by a private data item (the two operations have the property that, given the public operation, it is computationally infeasible to derive the private operation) ■	N8759: 2nd WD 29192-4: 2010-06-15
asymmetric cryptographic technique	cryptographic technique that uses two related transformations, a public transformation (defined by the public key) and a private transformation (defined by the private key) [ISO/IEC 11770-1:1996] ■	N8751: FCD 29150: 2010-06-10
asymmetric cryptographic technique	cryptographic technique that uses two related transformations, a public transformation (defined by the public key) and a private transformation (defined by the private key) NOTE The two transformations have the property that, given the public transformation, it is computationally infeasible to derive the private transformation. ■	ISO/IEC FDIS 11770-1: 2010-07-26
asymmetric cryptographic technique	cryptographic technique that uses two related transformations; public transformation (defined by the public key) and private transformation (defined by the private key) NOTE The two transformations have the property that, given the public transformation, it is computationally infeasible to derive the private transformation in a given limited timeframe and with given computational resources. ■	ISO/IEC 24759: 2008-07-01 (1st ed.)
asymmetric cryptographic technique	cryptographic technique that uses two related transformations; a public transformation (defined by the public key) and a private transformation (defined by the private key). The two transformations have the property that, given the public transformation, it is computationally infeasible to derive the private transformation in a given limited time and computing power ■	N8776: 2nd WD 19790: 2010-07-16

Term	Definition	ISO/IEC JTC 1/SC 27 Document
asymmetric cryptographic technique	cryptographic technique that uses two related transformations, a public transformation (defined by the public key) and a private transformation (defined by the private key), and has the property that given the public transformation, it is computationally infeasible to derive the private transformation NOTE A system based on asymmetric cryptographic techniques can either be an encipherment system, a signature system, a combined encipherment and signature system, or a key agreement system. With asymmetric cryptographic techniques there are four elementary transformations: sign and verify for signature systems, encipher and decipher for encipherment systems. The signature and the decipherment transformation are kept private by the owning entity, whereas the corresponding verification and encipherment transformations are published. There exist asymmetric cryptosystems (e.g. RSA) where the four elementary functions can be achieved by only two transformations: one private transformation suffices for both signing and decrypting messages, and one public transformation suffices for both verifying and encrypting messages. However, since this does not conform to the principle of key separation, throughout this part of ISO/IEC 11770, the four elementary transformations and the corresponding keys are kept separate. ■	ISO/IEC 11770-3: 2008-07-15 (2nd ed.)
asymmetric encipherment system	alternative term for asymmetric encryption system ■	ISO/IEC 18033-1: 2005-02-01 (1st ed.)
asymmetric encipherment system	system based on asymmetric cryptographic techniques whose public transformation is used for encipherment and whose private transformation is used for decipherment ■	ISO/IEC 11770-3: 2008-07-15 (2nd ed.)
asymmetric encryption system	system based on asymmetric cryptographic techniques whose public operation is used for encryption and whose private operation is used for decryption ■	ISO/IEC 9798-5: 2009-12-15 (3rd ed.)
asymmetric encryption system	system based on asymmetric cryptographic techniques whose public operation is used for encryption and whose private operation is used for decryption ■	ISO/IEC 9798-1: 2010-07-01 (3rd ed.)
asymmetric encryption system	system based on asymmetric cryptographic techniques whose public transformation is used for encryption and whose private transformation is used for decryption [ISO/IEC 9798-1:1997]. ■	ISO/IEC 18033-1: 2005-02-01 (1st ed.)
asymmetric encryption system	system based on asymmetric cryptographic techniques whose public transformation is used for encryption and whose private transformation is used for decryption [ISO/IEC 9798-1:1997] ■	N8751: FCD 29150: 2010-06-10

Term	Definition	ISO/IEC JTC 1/SC 27 Document
asymmetric key pair	pair of related keys where the private key defines the private transformation and the public key defines the public transformation ■	ISO/IEC 9798-1: 2010-07-01 (3rd ed.)
asymmetric key pair	pair of related keys where the private key defines the private transformation and the public key defines the public transformation [ISO/IEC 9798-1:1997]. ■	ISO/IEC 18033-1: 2005-02-01 (1st ed.)
asymmetric key pair	pair of related keys, a public key and a private key, where the private key defines the private transformation and the public key defines the public transformation [ISO/IEC 9798-1:1997] NOTE See Clauses 7, 8.1. ■	ISO/IEC 18033-2: 2006-05-01 (1st ed.)
asymmetric key pair	pair of related keys where the private key defines the private transformation and the public key defines the public transformation NOTE Adapted from ISO/IEC 9798-1. ■	ISO/IEC 18014-2: 2009-12-15 (2nd ed.)
asymmetric key pair	pair of related keys where the private key defines the private transformation and the public key defines the public transformation [ISO/IEC 9798-1:1997] ■	N8751: FCD 29150: 2010-06-10
asymmetric key pair	pair of related keys where the private key defines the private transformation and the public key defines the public transformation [ISO/IEC 11770-3:2008] ■	ISO/IEC FDIS 11770-1: 2010-07-26
asymmetric key pair	pair of related keys where the private key defines the private transformation and the public key defines the public transformation ■	ISO/IEC 11770-3: 2008-07-15 (2nd ed.)
asymmetric pair	two related data items where the private data item defines a private operation and the public data item defines a public operation ■	ISO/IEC 9798-5: 2009-12-15 (3rd ed.)
asymmetric pair	two related data items where the private data item defines a private operation and the public data item defines a public operation ■	N8759: 2nd WD 29192-4: 2010-06-15
asymmetric signature system	system based on asymmetric cryptographic techniques whose private transformation is used for signing and whose public transformation is used for verification ■	ISO/IEC 9798-1: 2010-07-01 (3rd ed.)
asymmetric signature system	system based on asymmetric techniques whose private transformation is used for signing and whose public transformation is used for verification NOTE Adapted from ISO/IEC 9798-1. ■	ISO/IEC 18014-2: 2009-12-15 (2nd ed.)
attack	attempt to destroy, expose, alter, disable, steal or gain unauthorized access to or make unauthorized use of an asset (2.3) ■	N8718: 1st WD 27000: 2010-05-27
attack	attempts to destroy, expose, alter, or disable an Information System and/or information within it or otherwise breach the security policy ■	ISO/IEC 18043: 2006-06-15 (1st ed.)

Term	Definition	ISO/IEC JTC 1/SC 27 Document
attack	attempt to destroy, expose, alter, disable, steal or gain unauthorized access to or make unauthorized use of an asset [ISO/IEC 27000:2009] ■	N8624: 2nd CD 27032: 2010-06-15
attack pattern	an abstracted approach utilized to attack software ■	N8784: 1st WD 20004: 2010-08-06
attack potential	measure of the effort to be expended in attacking a TOE, expressed in terms of an attacker's expertise, resources and motivation ■	ISO/IEC 15408-1: 2009-12-15 (3rd ed.)
attack potential	measure of the effort to be expended in attacking a TOE, expressed in terms of an attacker's expertise, resources and motivation ■	N8784: 1st WD 20004: 2010-08-06
attack potential	perceived potential for success of an attack, should an attack be launched, expressed in terms of an attacker's expertise, resources and motivation [ISO/IEC 15408-1:2005] ■	N8624: 2nd CD 27032: 2010-06-15
attack signature	sequence of computer activities or alterations that are used to execute an attack and which are also used by an IDS to discover that an attack has occurred and often is determined by the examination of network traffic or host logs NOTE This may also be referred to as an attack pattern. ■	ISO/IEC 18043: 2006-06-15 (1st ed.)
attack vector	attack vector is a path or means by which an attacker can gain access to a computer or network server in order to deliver a malicious outcome ■	N8624: 2nd CD 27032: 2010-06-15
attacker	person seeking to exploit potential vulnerabilities of a biometric system ■	ISO/IEC 19792: 2009-08-01 (1st ed.)
attacker	person deliberately exploiting vulnerabilities in technical and non-technical security controls in order to steal or compromise information systems and networks, or to compromise availability to legitimate users of information system and network resources ■	ISO/IEC 27033-1: 2009-12-15 (1st ed.)
attempt	submission of one (or a sequence of) biometric samples to the system NOTE An attempt results in an enrolment template, a matching score (or scores), or possibly a failure-to-acquire. ■	ISO/IEC 19792: 2009-08-01 (1st ed.)
attestation	variant of public-key encryption that lets IDS software programs and devices authenticate their identity to remote parties. NOTE See Clause 2.21, Remote attestation. ■	ISO/IEC 18043: 2006-06-15 (1st ed.)
attribute	property or characteristic of an object that can be distinguished quantitatively or qualitatively by human or automated means [ISO/IEC 15939:2007] ■	ISO/IEC 27004: 2009-12-15 (1st ed.)

Term	Definition	ISO/IEC JTC 1/SC 27 Document
attribute	property or characteristic of an entity (3.1.1) that can be used to describe its state, appearance or other qualities EXAMPLE An entity type, address information, telephone number, a privilege, a MAC address, a domain name are possible attributes. ■	N8804: 3rd CD 24760-1: 2010-06-11
attribute Authority (AA)	An entity trusted by one or more entities to create and sign attribute certificates. NOTE Note that a CA may also be an AA. ■	ISO/IEC TR 14516: 2002-06-15 (1st ed.)
audit	systematic and documented process for obtaining audit evidence and evaluating it objectively to determine the extent to which audit criteria are fulfilled [adapted from ISO/IEC 9000:2005] ■	N8632: FCD 27034-1: 2010-05-27
audit logging	recording of data on information security events for the purpose of review and analysis, and ongoing monitoring ■	ISO/IEC 27033-1: 2009-12-15 (1st ed.)
audit scope	extent and boundaries of an audit [ISO 19011] ■	N8718: 1st WD 27000: 2010-05-27
audit tools	automated tools to aid the analysis of the contents of audit logs ■	ISO/IEC 27033-1: 2009-12-15 (1st ed.)
augmentation	addition of one or more requirement(s) to a package ■	ISO/IEC 15408-1: 2009-12-15 (3rd ed.)
augmented password-authenticated key agreement	password-authenticated key agreement where entity *A* uses a password-based weak secret and entity *B* uses verification data derived from a one-way function of *A*'s weak secret to negotiate and authenticate one or more shared secret keys ■	ISO/IEC 11770-4: 2006-05-01 (1st ed.)
authenticated encryption	(reversible) transformation of data by a cryptographic algorithm to produce ciphertext that cannot be altered by an unauthorized entity without detection, i.e. it provides data confidentiality, data integrity, and data origin authentication [ISO/IEC 19772:---[1)]] 1) To be published. ■	ISO/IEC 9798-2: 2008-12-15 (3rd ed.)
authenticated encryption	(reversible) transformation of data by a cryptographic algorithm to produce ciphertext that cannot be altered by an unauthorized entity without detection, i.e. it provides data confidentiality, data integrity, and data origin authentication ■	ISO/IEC 19772: 2009-02-15 (1st ed.)
authenticated encryption mechanism	cryptographic technique used to protect the confidentiality and guarantee the origin and integrity of data, and which consists of two component processes: an encryption algorithm and a decryption algorithm ■	ISO/IEC 19772: 2009-02-15 (1st ed.)

Term	Definition	ISO/IEC JTC 1/SC 27 Document
authenticated identity	identity (3.1.2) for an entity (3.1.1) created as result of authentication (3.3.2) NOTE 1 An authenticated identity typically contains information obtained in the authentication process, e.g., the assurance level attained. NOTE 2 The existence of an authenticated identity in a particular domain denotes that an entity has been recognized in that domain. NOTE 3 An authenticated identity typically has a lifespan restricted by an authentication policy. ■	N8804: 3rd CD 24760-1: 2010-06-11
authentication	provision of assurance that a claimed characteristic of an entity is correct ■	N8718: 1st WD 27000: 2010-05-27
authentication	provision of assurance of the claimed identity of an entity NOTE Adapted from ISO/IEC 18028-4. ■	ISO/IEC 18014-2: 2009-12-15 (2nd ed.)
authentication	provision of assurance of the claimed identity of an entity NOTE Definition from [1]. ■	ISO/IEC 19792: 2009-08-01 (1st ed.)
authentication	process of corroborating an identity or attribute with a specified or understood level of assurance. ■	N8810: 1st CD 29115 | X.eaa: 2010-06-10
authentication	formalized process of identification (3.2.1) that if successful results in an authenticated identity (3.3.3) for a claimant, (3.3.1) NOTE 1 The authentication process involves tests by a verifier on one or more identity attributes provided by a claimant to determine (with the required degree of assurance) their correctness. NOTE 2 Authentication typically involves the use of a policy to specify a required assurance level for the result after a successful completion. NOTE 3 Identification is usually done as authentication to obtain a specific level of confidence in the result NOTE 4 Adapted from ISO/IEC10181-2. ■	N8804: 3rd CD 24760-1: 2010-06-11
authentication	process of establishing an understood level of confidence that a specific entity or claimed identity is genuine NOTE 1 Authentication includes the process of ascertaining an understood level of confidence of the truth of a claimed identity before the entity can be registered and recognized in a domain. NOTE 2 Although this definition is generic, its use within this standard is limited to the biometric authentication of human subjects. [ISO 19092:2007] ■	N8802: FCD 24745: 2010-05-19

Term	Definition	ISO/IEC JTC 1/SC 27 Document
authentication	provision of assurance of the claimed identity of an entity. In case of user authentication, users are identified either by knowledge (e.g., password), by possession (e.g., token) or by a personal characteristic (biometrics). Strong authentication is either based on strong mechanisms (e.g., biometrics) or makes use of at least two of these factors (so-called multi-factor authentication). ■	ISO/IEC 18028-4: 2005-04-01 (1st ed.)
authentication context for biometrics ACBio	International Standard that specifies the form and encoding of ACBio instances ■	ISO/IEC 24761: 2009-05-15 (1st ed.)
authentication data	information used to verify the claimed identity of a user ■	ISO/IEC 15408-1: 2009-12-15 (3rd ed.)
authentication protocol	Defined sequence of messages between a claimant and a verifier that enables the verifier to corroborate the claimant's identity. ■	N8810: 1st CD 29115 | X.eaa: 2010-06-10
authenticity	property that an entity is what it claims to be ■	N8718: 1st WD 27000: 2010-05-27
authenticity	property that ensures that the identity of a subject or resource is the one claimed NOTE 1 Authenticity applies to entities such as users, processes, systems and information. NOTE 2 Adapted from ISO/IEC TR 13335-1:1996. ■	ISO/IEC 21827: 2008-10-15 (2nd ed.)
authorised user	TOE user who may, in accordance with the SFRs, perform an operation ■	ISO/IEC 15408-1: 2009-12-15 (3rd ed.)
authorization	approval of a request by an entity (3.1.1) to perform an action upon evaluation of applicable policy NOTE 1 Authorization often happens in a successful authentication process as may be specified in the authorization policy. NOTE 2 Authorization may be made explicit with the addition of a set of attributes that are valid for the duration of the approval. NOTE 3 The activity permitted after authorization typically involves the access or use of a resource pertaining to the domain. ■	N8804: 3rd CD 24760-1: 2010-06-11
authorization	Process of establishing to an understood level of assurance that a claimed identity may be given privileges NOTE: granting or denying, according to a particular security policies, of certain privileges and permissions to access a resource ■	N8812: 3rd WD 29146: 2010-07-14
automated	without manual intervention or input (e.g. electronic means such as through a computer network) ■	N8776: 2nd WD 19790: 2010-07-16

Term	Definition	ISO/IEC JTC 1/SC 27 Document
auxiliary data AD	subject-dependent data that is part of a renewable biometric reference and may be required to reconstruct pseudonymous identifiers during verification, or for verification in general NOTE 1 If auxiliary data is part of a renewable biometric reference, it is not necessarily stored in the same place as the corresponding pseudonymous identifiers. NOTE 2 Auxiliary data may contain data elements for diversification (i.e., diversification data). NOTE 3 Auxiliary data is not the element for comparison during biometric reference verification. NOTE 4 Auxiliary data are generated by the biometric system during enrolment. EXAMPLE Secret number encrypted by a key derived from a biometric sample using a helper data approach, fuzzy commitment scheme, or fuzzy vault. See Annex D, Table D.1 for concrete examples of instances for PI and AD. ■	N8802: FCD 24745: 2010-05-19
availability	property of being accessible and usable upon demand by an authorized entity ■	N8718: 1st WD 27000: 2010-05-27
availability	property of being accessible and useable upon demand by an authorized entity [ISO/IEC 7498-2:1989] ■	ISO/IEC 21827: 2008-10-15 (2nd ed.)
availability	degree to which the services of a system or component are operational and accessible when needed by their intended/authorized users. In the context of security, availability pertains to authorized services/actions only, and the need for availability generates the requirement that the system or component is able to resist or withstand attempts at unauthorized deletion or denial of service, regardless of whether those attempts are intentional or accidental. [Avizienis et al, IEEE Std 610.12-1990, NIST SP 800-27-Rev.A] ■	N8732: 3rd WD 29193: 2010-08-06
avatar	representation of a person participating in the Cyberspace NOTE 1 An avatar can also be referred to as the person's alter ego. NOTE 2 An avatar can also be seen as an "object" representing the embodiment of the user. ■	N8624: 2nd CD 27032: 2010-06-15
backward secrecy	assurance that previous values cannot be determined from the current value or subsequent values ■	N8745: FCD 18031: 2010-05-18
backward security with interval T	security condition in which an entity is joining at time $t = t_0$ cannot obtain any former *shared secret keys* at time $t < t_0$ - T ■	N8743: 2nd CD 11770-5: 2010-07-29

Term	Definition	ISO/IEC JTC 1/SC 27 Document
balanced password-authenticated key agreement	password-authenticated key agreement where two entities *A* and *B* use a shared common password-based weak secret to negotiate and authenticate one or more shared secret keys ■	ISO/IEC 11770-4: 2006-05-01 (1st ed.)
base component	entity in a composed TOE, which has itself been the subject of an evaluation, providing services and resources to a dependent component ■	ISO/IEC 15408-1: 2009-12-15 (3rd ed.)
base measure	measure defined in terms of an attribute and the method for quantifying it [ISO/IEC 15939:2007] NOTE A base measure is functionally independent of other measures. ■	ISO/IEC 27004: 2009-12-15 (1st ed.)
baseline	specification or product that has been formally reviewed and agreed upon, that thereafter serves as the basis for further development, and that can be changed only through formal change control procedures [IEEE-Std. 610] ■	ISO/IEC 21827: 2008-10-15 (2nd ed.)
batch rekeying	*rekeying* method in which the *shared secret key*, and optionally, *key encryption keys* are updated for every *rekeying* interval T ■	N8743: 2nd CD 11770-5: 2010-07-29
biased source	source of bit strings (or numbers) from a sample space is said to be biased if some bit strings (or numbers) are more likely than some other bit strings (or numbers) to be chosen NOTE 1 Equivalently, if the sample space consists of *r* elements, some elements will occur with probability different from 1/*r*. NOTE 2 This term can be contrasted to unbiased source. ■	N8745: FCD 18031: 2010-05-18
big-endian	method of storage of multi-byte numbers with the most significant bytes at the lowest memory addresses ■	ISO/IEC 10118-1: 2000-06-15 (2nd ed.)
big-endian	method of storage of multi-byte numbers with the most significant bytes at the lowest memory addresses [ISO/IEC 10118-1:2000] ■	N8749: 2nd CD 18033-4: 2010-05-19
big-endian	method of storage of multi-byte numbers with the most significant bytes at the lowest memory addresses [ISO/IEC 10118-1: 2000] ■	N8757: 2nd WD 29192-3: 2010-07-01
biometric	pertaining to the field of biometrics ■	ISO/IEC 24761: 2009-05-15 (1st ed.)

Term	Definition	ISO/IEC JTC 1/SC 27 Document
biometric application decision	conclusion based on the application decision policy after consideration of one or more comparison decisions, comparison scores and possibly other non-biometric data NOTE 1 Definition from [2]. NOTE 2 Biometric application decisions can be made on the basis of complex policies, allowing for variable numbers of positive comparison decisions. NOTE 3 A biometric verification application could allow a positive biometric application decision even if there are one or more non-matches against enrolled biometric references. EXAMPLE A biometric application decision could be "accept claim". ■	ISO/IEC 19792: 2009-08-01 (1st ed.)
biometric characteristic	biological and behavioural characteristic of an individual that can be detected and from which distinguishing, repeatable biometric features can be extracted for the purpose of automated recognition of individuals NOTE 1 Definition from [2]. NOTE 2 Biological and behavioural characteristics are physical properties of body parts, physiological and behavioural processes created by the body and combinations of any of these. NOTE 3 Distinguishing does not necessarily imply individualization. EXAMPLE Examples of biometric characteristics are: Galton ridge structure, face topography, facial skin texture, hand topography, finger topography, iris structure, vein structure of the hand, ridge structure of the palm or retinal pattern. ■	ISO/IEC 19792: 2009-08-01 (1st ed.)
biometric characteristic	physiological or behavioural characteristic of an individual that can be detected and from which distinguishing, repeatable biometric features can be extracted for the purpose of automated recognition of individuals [ISO/IEC SC37 SD2 (v.11)] ■	N8802: FCD 24745: 2010-05-19
biometric data	biometric sample at any stage of processing, biometric reference, biometric feature or biometric property NOTE Definition from [2]. ■	ISO/IEC 19792: 2009-08-01 (1st ed.)
biometric data	biometric sample, biometric feature, biometric model, biometric property, other description data for the original biometric characteristics, or aggregation of above data [ISO/IEC SC37 SD2 (v.11)] ■	N8802: FCD 24745: 2010-05-19
biometric data record	data which consists of an identity reference and its relevant biometric reference or renewable biometric reference ■	N8802: FCD 24745: 2010-05-19

Term	Definition	ISO/IEC JTC 1/SC 27 Document
biometric feature	numbers or labels extracted from biometric samples and used for comparison NOTE 1 Biometric features are the output of a completed biometric feature extraction. NOTE 2 The use of this term should be consistent with its use by the pattern recognition and mathematics communities. NOTE 3 A biometric feature set can also be considered a processed biometric sample. ■	ISO/IEC 19792: 2009-08-01 (1st ed.)
biometric feature	numbers or labels extracted from biometric samples and used for comparison [ISO/IEC SC37 SD2 (v.11)] ■	N8802: FCD 24745: 2010-05-19
biometric identification	biometric system function that performs a one-to-many search to obtain a candidate list NOTE Definition from [2]. ■	ISO/IEC 19792: 2009-08-01 (1st ed.)
biometric information privacy	right to control the collection, transfer, use, storage, archiving, disposal and renewal of one's own biometric information throughout its lifecycle ■	N8802: FCD 24745: 2010-05-19
biometric model	stored function (dependent on the biometric data subject) generated from a biometric feature(s) NOTE 1 Definition from [2]. NOTE 2 Comparison applies the function to the biometric features of a recognition biometric sample to give a comparison score. NOTE 3 The function may be determined through training. NOTE 4 A biometric model may involve intermediate processing similar to biometric feature extraction. EXAMPLE Examples for the stored function could be a Hidden Markov Model, Gaussian Mixture Model or an Artificial Neural Network. ■	ISO/IEC 19792: 2009-08-01 (1st ed.)
biometric model	stored function (dependent on the biometric data subject) generated from a biometric feature(s) NOTE Comparison applies the stored function to the biometric features of a probe biometric sample to give a comparison score. EXAMPLE Examples for the stored function could be a Hidden Markov Model, Gaussian Mixture Model or an Artificial Neural Network. [ISO/IEC SC37 SD2 (v.11)] ■	N8802: FCD 24745: 2010-05-19

Term	Definition	ISO/IEC JTC 1/SC 27 Document
biometric processing unit - BPU	entity that executes one or more subprocesses that perform a biometric verification at a uniform level of security NOTE A sensor, a smart card, and a comparison device are examples of BPUs. ■	ISO/IEC 24761: 2009-05-15 (1st ed.)
biometric processing unit certificate BPU certificate	X.509 certificate that is issued to a BPU by a certification organization which enables the validator to determine the reliability of the BPU ■	ISO/IEC 24761: 2009-05-15 (1st ed.)
biometric processing unit certification organization - BPU certification organization	organization which issues BPU certificates ■	ISO/IEC 24761: 2009-05-15 (1st ed.)
biometric processing unit function report - BPU function report	report on the function of the BPU, which contains the evaluation results on each function in the BPU ■	ISO/IEC 24761: 2009-05-15 (1st ed.)
biometric processing unit IO Index - BPU IO Index	integer assigned to each biometric data stream between BPUs by the subject, such as software, which utilizes the function of the BPU so that the validator can reconstruct the data flow among BPUs ■	ISO/IEC 24761: 2009-05-15 (1st ed.)
biometric processing unit report - BPU report	report on a BPU, which consists of a BPU function report and a BPU security report ■	ISO/IEC 24761: 2009-05-15 (1st ed.)
biometric processing unit security report - BPU security report	report on the security level of a BPU, which contains an evaluation result of the security level of the BPU ■	ISO/IEC 24761: 2009-05-15 (1st ed.)
biometric product	biometric component, system or application acting as the scope of an evaluation ■	ISO/IEC 19792: 2009-08-01 (1st ed.)
biometric property	descriptive attributes of the biometric data subject estimated or derived from the biometric sample by automated means NOTE Definition from [2]. EXAMPLE Fingerprints can be classified by the biometric properties of ridge-flow, i.e. arch, whorl, and loop types; In the case of facial recognition, this could be estimates of age or gender. ■	ISO/IEC 19792: 2009-08-01 (1st ed.)
biometric property	descriptive attributes of the biometric data subject estimated or derived from the biometric sample by automated means EXAMPLE Fingerprints can be classified by the biometric properties of ridge-flow (i.e., arch, whorl, and loop types); In the case of facial recognition, this could be estimates of age or gender. [ISO/IEC SC37 SD2 (v.11)] ■	N8802: FCD 24745: 2010-05-19
biometric recognition	recognition using a biometric product NOTE A biometric recognition can either be realized as a biometric verification or as a biometric identification process. ■	ISO/IEC 19792: 2009-08-01 (1st ed.)

Term	Definition	ISO/IEC JTC 1/SC 27 Document
biometric reference	one or more stored biometric samples, biometric templates or biometric models attributed to a biometric data subject and used for comparison NOTE 1 Definition from [2]. NOTE 2 A biometric reference may be created with implicit or explicit use of auxiliary data, such as Universal Background Models. EXAMPLE Face image on a passport; Fingerprint minutiae template on a National ID card; Gaussian Mixture Model, for speaker recognition, in a database. ■	ISO/IEC 19792: 2009-08-01 (1st ed.)
biometric reference BR	one or more stored biometric samples, biometric templates or biometric models attributed to a biometric data subject and used for comparison NOTE A biometric reference that can be renewed is referred to as renewable biometric reference. EXAMPLE Face image on a passport; Fingerprint minutiae template on a National ID card; Gaussian Mixture Model, for speaker recognition, in a database. [ISO/IEC SC37 SD2 (v.11)] ■	N8802: FCD 24745: 2010-05-19
biometric reference template	biometric sample or combination of biometric samples that has been stored as a reference for future comparison NOTE See also raw biometric reference template (3.34), intermediate biometric reference template (3.27), and processed biometric reference template (3.32). ■	ISO/IEC 24761: 2009-05-15 (1st ed.)
biometric reference template certificate BRT certificate	certificate that is issued to a biometric reference template by a BRT certification organization and enables the validator to determine the authenticity of the biometric reference template ■	ISO/IEC 24761: 2009-05-15 (1st ed.)
biometric reference template certification organization BRT certification organization	organization which issues BRT certificates ■	ISO/IEC 24761: 2009-05-15 (1st ed.)
biometric sample	analog or digital representation of biometric characteristics prior to biometric feature extraction and obtained from a biometric capture device or biometric capture subsystem NOTE 1 Definition from [2]. NOTE 2 A biometric capture device is a biometric capture subsystem with a single component. ■	ISO/IEC 19792: 2009-08-01 (1st ed.)
biometric sample	information obtained from a biometric sensor, either directly or after further processing NOTE See also raw biometric sample (3.33), intermediate biometric sample (3.26), and processed biometric sample (3.31). ■	ISO/IEC 24761: 2009-05-15 (1st ed.)

Term	Definition	ISO/IEC JTC 1/SC 27 Document
biometric sample	analog or digital representation of biometric characteristics obtained from a biometric capture device or biometric capture subsystem prior to biometric feature extraction [ISO/IEC SC37 SD2 (v.11)] ■	N8802: FCD 24745: 2010-05-19
biometric system	system for the purpose of the automated recognition of individuals based on their behavioural and physiological characteristics ■	N8802: FCD 24745: 2010-05-19
biometric template	set of stored biometric features comparable directly to biometric features of a recognition biometric sample NOTE 1 Definition from [2]. NOTE 2 A biometric reference consisting of an image, or other captured biometric sample, in its original, enhanced or compressed form, is not a biometric template. NOTE 3 The biometric features are not considered to be a biometric template unless they are stored for reference. ■	ISO/IEC 19792: 2009-08-01 (1st ed.)
biometric template	set of stored biometric features comparable directly to probe biometric features ■	N8802: FCD 24745: 2010-05-19
biometric verification	biometric product function that performs a one-to-one comparison NOTE Adapted from [2]. ■	ISO/IEC 19792: 2009-08-01 (1st ed.)
biometric verification	application that returns true or false for a claim about the similarity of one or more biometric reference templates and one or more recognition biometric samples by making one or more comparisons ■	ISO/IEC 24761: 2009-05-15 (1st ed.)
biometrics	automated recognition of individuals based on their behavioural and biological characteristics NOTE Definition from [2]. ■	ISO/IEC 19792: 2009-08-01 (1st ed.)
biometrics	automated recognition of individuals based on their behavioural and biological characteristics ■	ISO/IEC 24761: 2009-05-15 (1st ed.)
bit	one of the two symbols `0' or `1' NOTE See Clause 5.2.1. ■	ISO/IEC 18033-2: 2006-05-01 (1st ed.)
Bit ordering	Bit ordering in this part of ISO/IEC 10118 is as described in clause 3 of ISO/IEC 10118-1. ■	ISO/IEC 10118-4: 1998-12-15 (1st ed.)
bit stream	continuous output of bits from a device or mechanism ■	N8745: FCD 18031: 2010-05-18
bit string	sequence of bits NOTE See Clause 5.2.1. ■	ISO/IEC 18033-2: 2006-05-01 (1st ed.)
bit string	finite sequence of ones and zeroes ■	N8745: FCD 18031: 2010-05-18

Term	Definition	ISO/IEC JTC 1/SC 27 Document
black box	idealized mechanism that accepts inputs and produces outputs, but is designed such that an observer cannot see inside the box or determine exactly what is happening inside that box NOTE This term can be contrasted to glass box. ■	N8745: FCD 18031: 2010-05-18
blended attack	type of attack that seeks to maximize the severity of damage and speed of contagion by combining multiple attacking methods ■	N8624: 2nd CD 27032: 2010-06-15
block	a bit-string of length L1, i.e., the length of the first input to the round-function ■	ISO/IEC 10118-3: 2004-03-01 (3rd ed.)
block	a string of bits of length L_Φ which shall be an integer multiple of 16 (see also clause 6.1) EXAMPLE The length of the output H_j of the round-function. ■	ISO/IEC 10118-4: 1998-12-15 (1st ed.)
block	bit-string of length L_1, i.e. the length of the first input to the round-function [ISO/IEC 10118-3] ■	ISO/IEC FDIS 9797-2: 2009-09-18
block	string of bits of defined length ■	ISO/IEC FDIS 10118-2: 2010-03-10
block	string of bits of a defined length. ■	ISO/IEC 18033-1: 2005-02-01 (1st ed.)
block	string of bits of a defined length [ISO/IEC 18033-1] NOTE In this part of ISO/IEC 18033, a block will be restricted to be an octet string (interpreted in a natural way as a bit string). ■	ISO/IEC 18033-2: 2006-05-01 (1st ed.)
block	string of bits of defined length [ISO/IEC 18033-1:2005] ■	N8755: 1st CD 29192-2: 2010-06-22
block	string of bits of a defined length ■	N8751: FCD 29150: 2010-06-10
block	string of bits of defined length NOTE In this part of ISO/IEC 18033, the block length is either 64 or 128 bits. [ISO/IEC 18033-1:2005] ■	ISO/IEC FDIS 18033-3: 2010-07-12
block	bit string of length n ■	N8861: PreFDIS 9797-1: 2010-09-03
block chaining	encryption of information in such a way that each block of ciphertext is cryptographically dependent upon a preceding ciphertext block. ■	ISO/IEC 10116: 2006-02-01 (3rd ed.)
block cipher	symmetric encryption algorithm with the property that the encryption algorithm operates on a block of plaintext, i.e. a string of bits of a defined length, to yield a block of ciphertext. [ISO/IEC 18033-1] ■	ISO/IEC 10116: 2006-02-01 (3rd ed.)
block cipher	symmetric encryption system with the property that the encryption algorithm operates on a block of plaintext, i.e. a string of bits of a defined length, to yield a block of ciphertext. ■	ISO/IEC 18033-1: 2005-02-01 (1st ed.)

Term	Definition	ISO/IEC JTC 1/SC 27 Document
block cipher	symmetric cipher with the property that the encryption algorithm operates on a block of plain-text, i.e., a string of bits of a defined length, to yield a block of cipher text [ISO/IEC 18033-1] NOTE 1 See Clause 6.4. NOTE 2 In this part of ISO/IEC 18033, plaintext/cipher text blocks will be restricted to be octet strings (interpreted in a natural way as bit strings). ■	ISO/IEC 18033-2: 2006-05-01 (1st ed.)
block cipher	symmetric encryption system with the property that the encryption algorithm operates on a block of plaintext, i.e. a string of bits of a defined length, to yield a block of ciphertext [ISO/IEC 18033-1] ■	ISO/IEC 19772: 2009-02-15 (1st ed.)
block cipher	symmetric encipherment system with the property that the encryption algorithm operates on a block of plaintext, i.e. a string of bits of a defined length, to yield a block of ciphertext [ISO/IEC 18033-1:2005] ■	N8755: 1st CD 29192-2: 2010-06-22
block cipher	symmetric encipherment system with the property that the encryption operates on a block of plaintext, i.e., a string of bits of a defined length, to yield a block of ciphertext [ISO/IEC 18033-1] ■	N8745: FCD 18031: 2010-05-18
block cipher	symmetric encryption system with the property that encryption operates on a block of plaintext, i.e. a string of bits of a defined length, to yield a block of ciphertext, and decryption operates on the ciphertext to yield the original plaintext [ISO/IEC 18033-1] ■	N8751: FCD 29150: 2010-06-10
block cipher	symmetric encipherment system with the property that the encryption algorithm operates on a block of plaintext, i.e. a string of bits of a defined length, to yield a block of ciphertext [ISO/IEC 18033-1:2005] ■	ISO/IEC FDIS 18033-3: 2010-07-12
block cipher key	key that controls the operation of a block cipher ■	N8861: PreFDIS 9797-1: 2010-09-03
bot robot	automated software program used to carry out specific tasks NOTE 1 The word is often used to describe programs, usually run on a server, that automate tasks such as forwarding or sorting e-mail. NOTE 2 A bot is also described as a program that operates as an agent for a user or another program or simulates a human activity. On the Internet, the most ubiquitous bots are the programs, also called spiders or crawlers, which access Web sites and gather their content for search engine indexes. ■	N8624: 2nd CD 27032: 2010-06-15
botnet	type of remote control software, specifically a collection of malicious software robots, or bots, that run autonomously or automatically on compromised computers ■	N8624: 2nd CD 27032: 2010-06-15

Term	Definition	ISO/IEC JTC 1/SC 27 Document
bridge	network equipment that transparently connects a local area network (LAN) at OSI layer 2 to another LAN that uses the same protocol ■	ISO/IEC 18043: 2006-06-15 (1st ed.)
brute-force attack	attack on a cryptosystem that employs an exhaustive search of a set of keys, passwords or other data ■	ISO/IEC 11770-4: 2006-05-01 (1st ed.)
business continuity	procedures (2.39) and/or processes (2.40) for ensuring continued business operations ■	N8718: 1st WD 27000: 2010-05-27
business continuity management BCM	holistic management process that identifies potential threats to an organization and the impacts to business operations those threats, if realized, might cause, and which provides a framework for building organizational resilience with the capability for an effective response that safeguards the interests of its key stakeholders, reputation, brand and value-creating activities ■	N8622: PreFDIS 27031: 2010-08-18
business continuity plan BCP	documented procedures that guide organisations to respond, recover, resume, and restore to a pre-defined level of operation following disruption NOTE typically this covers resources, services and activities required to ensure the continuity of critical business functions ■	N8622: PreFDIS 27031: 2010-08-18
business impact analysis BIA	process of analyzing operational functions and the effect that a disruption might have upon them ■	N8622: PreFDIS 27031: 2010-08-18
bypass capability	the ability of a service to partially or wholly circumvent a cryptographic function ■	N8776: 2nd WD 19790: 2010-07-16
call coupling	relationship between two modules communicating strictly through their documented function calls NOTE Examples of call coupling are data, stamp and control. ■	ISO/IEC 15408-1: 2009-12-15 (3rd ed.)
call coupling	<data> relationship between two modules communicating strictly through the use of call parameters that represent single data items NOTE See also call coupling (3.2.8). ■	ISO/IEC 15408-1: 2009-12-15 (3rd ed.)
call coupling	<stamp> relationship between two modules communicating through the use of call parameters that comprise multiple fields or that have meaningful internal structures NOTE See also call coupling ■	ISO/IEC 15408-1: 2009-12-15 (3rd ed.)
call coupling	<control> relationship between two modules if one passes information that is intended to influence the internal logic of the other NOTE See also call coupling (3.2.8). ■	ISO/IEC 15408-1: 2009-12-15 (3rd ed.)

Term	Definition	ISO/IEC JTC 1/SC 27 Document
call tree	identifies the modules in a system in diagrammatic form showing which modules call one another NOTE Adapted from IEEE Std 610.12-1990. ■	ISO/IEC 15408-1: 2009-12-15 (3rd ed.)
call-back	mechanism to place a call to a pre-defined or proposed location (and address) after receiving valid ID parameters. ■	ISO/IEC 18028-4: 2005-04-01 (1st ed.)
capacity	positive integer indicating the number of bits available within the signature for the recoverable part of the message ■	ISO/IEC FDIS 9796-2: 2010-09-10
certificate	certificate issued by a certification body in accordance with the conditions of its accreditation and bearing an accreditation symbol or statement ■	ISO/IEC 27006: 2007-03-01 (1st ed.)
certificate	entity's data rendered unforgeable with the private or secret key of a certification authority ■	ISO/IEC 13888-1: 2009-07-15 (3rd ed)
certificate	declaration by an independent authority operating in accordance with ISO Guide 58, Calibration and testing laboratory accreditation systems - General requirements for operation and recognition, confirming that an evaluation pass statement is valid ■	ISO/IEC 15292: 2001-12-15 (1st ed.)
certificate	entity's data rendered unforgeable with the private or secret key of a certification authority NOTE Not to be confused with a modules validation certificate issued by a validation authority ■	N8776: 2nd WD 19790: 2010-07-16
certificate domain	collection of entities using public key certificates created by a single Certification Authority (CA) or a collection of CAs operating under a single security policy ■	ISO/IEC FDIS 9796-2: 2010-09-10
certificate domain parameters	cryptographic parameters specific to a certificate domain and which are known and agreed by all members of the certificate domain ■	ISO/IEC FDIS 9796-2: 2010-09-10
certificate management services	all services needed for the maintenance of the lifecycle of certificates, including registration, certification, distribution, and revocation of certificates. ■	ISO/IEC 15945: 2002-02-01 (1st ed.)
certification	process, producing written results, of performing a comprehensive evaluation of security features and other safeguards of a system to establish the extent to which the design and implementation meet a set of specified security requirements NOTE This definition is generally accepted within the security community; within ISO the more generally used definition is: Procedure by which a third party gives written assurance that a product, process or service conforms to specified requirements [ISO/IEC Guide 2]. ■	ISO/IEC 21827: 2008-10-15 (2nd ed.)

Term	Definition	ISO/IEC JTC 1/SC 27 Document
certification	procedure by which a formal assurance statement is given that a deliverable conforms to specified requirements. Certification may be performed by a third party or self-certified. [adapted from ISO/IEC Guide 2:1996]. a) The issue of a formal statement confirming the results of an evaluation, and that the evaluation criteria used where correctly applied [ITSEC]. b) The certification process is the independent inspection of the results of the evaluation leading to the production of the final certificate or approval [ISO/IEC 15408–1]. c) Certification The comprehensive assessment of the technical and non-technical security features of an information technology system, made in support of accreditation that establishes the extent to which a system satisfies a specified security policy [AGCA]. ■	ISO/IEC TR 15443-1: 2005-02-01 (1st ed.)
certification authority	authority trusted by one or more users to create and assign certificates NOTE 1 Adapted from ISO/IEC 9594-8:2001, 3.3.17. NOTE 2 Optionally the certification authority can create the users‘ keys. ■	ISO/IEC 13888-1: 2009-07-15 (3rd ed)
certification authority	entity trusted to create and assign public key certificates ■	ISO/IEC FDIS 11770-1: 2010-07-26
certification authority CA	centre trusted to create and assign public key certificates NOTE Optionally, the certification authority can create and assign keys to the entities. [ISO/IEC 11770-1:1996] ■	ISO/IEC 18014-1: 2008-09-01 (2nd ed.)
certification authority CA	authority trusted by one or more users to create and assign public-key certificates NOTE Optionally, the certification authority can create the users' keys. [ISO/IEC 9594-8:2005, definition 3.3.16] ■	ISO/IEC 18014-2: 2009-12-15 (2nd ed.)
certification authority CA	authority trusted by one or more users to create and assign public-key certificates NOTE 1 Optionally, the certification authority can create the users' keys. NOTE 2 The role of the certification authority (CA) in this process is to guarantee that the individual granted the unique certificate is, in fact, who he or she claims to be. Usually, this means that the CA has an arrangement with an institution which provides it with information to confirm an individual's claimed identity. CAs are a critical component in information security and electronic commerce because they guarantee that the two parties exchanging information are really who they claim to be. ■	ISO/IEC 27033-1: 2009-12-15 (1st ed.)

Term	Definition	ISO/IEC JTC 1/SC 27 Document
certification authority CA	authority trusted by one or more users to create and assign public-key certificates NOTE Optionally, the certification authority may create the users' keys. [ISO/IEC 9594-8:2005] ■	N8642: 2nd PDTR 29149: 2010-06-22
certification authority CA	centre trusted to create and assign public key certificates ■	ISO/IEC 11770-3: 2008-07-15 (2nd ed.)
certification body	third party that assesses and certifies the ISMS of a client organization with respect to published ISMS standards, and any supplementary documentation required under the system ■	ISO/IEC 27006: 2007-03-01 (1st ed.)
certification document	document indicating that a client organization's ISMS conforms to specified ISMS standards and any supplementary documentation required under the system ■	ISO/IEC 27006: 2007-03-01 (1st ed.)
certification service	service of creating and assigning certificates performed by a CA and described in ISO/IEC 9594-8:1995. ■	ISO/IEC 15945: 2002-02-01 (1st ed.)
challenge	procedure parameter used in conjunction with secret parameters to produce a response ■	ISO/IEC 9798-5: 2009-12-15 (3rd ed.)
challenge	data item chosen at random and sent by the verifier to the claimant, which is used by the claimant, in conjunction with secret information held by the claimant, to generate a response which is sent to the verifier ■	ISO/IEC 9798-1: 2010-07-01 (3rd ed.)
challenge	procedure parameter used in conjunction with secret parameters to produce a response ■	N8759: 2nd WD 29192-4: 2010-06-15
Challenge-Handshake Authentication Protocol - CHAP	three-way authentication protocol defined in RFC 1994. ■	ISO/IEC 18028-4: 2005-04-01 (1st ed.)
check	generate a verdict by a simple comparison NOTE Evaluator expertise is not required. The statement that uses this verb describes what is mapped. ■	N8912: Corrected 18045: 2010-09-15
check character	added character which may be used to verify the accuracy of the string by a mathematical relationship to that string. ■	ISO/IEC 7064: 2003-02-15 (2nd ed.)
check character system	set of rules for generating check characters and checking strings incorporating check characters. ■	ISO/IEC 7064: 2003-02-15 (2nd ed.)
check-value	string of bits, computed as the output of a check-value function, sent from the data originator to the data recipient that enables the recipient of data to check its correctness ■	ISO/IEC FDIS 9798-6: 2010-08-05

Term	Definition	ISO/IEC JTC 1/SC 27 Document
check-value function	function *f* which maps a string of bits and a short secret key, i.e. a key that can readily be entered into or read from a user device, to a fixed-length string of bits, i.e. a *b*-bit check-value, satisfying the following properties: - for any key *k* and any input string *d*, the function *f*(*d*, *k*) can be computed efficiently; - it is computationally infeasible to find a pair of distinct data strings (*d*, *d*') for which the number of keys which satisfy *f*(*d*, *k*) = *f*(*d*', *k*) is more than a small fraction of the possible set of keys. NOTE In practice, a short key would typically contain 4-6 digits or alphanumeric characters. ■	ISO/IEC FDIS 9798-6: 2010-08-05
child keys of key k	set of *keys* in a *logical key hierarchy* and these *keys* are assigned to the *child nodes* of the node where k is assigned NOTE One of the *keys* in a set of *child keys* must be a *key encryption key* or *individual key*. ■	N8743: 2nd CD 11770-5: 2010-07-29
child nodes of node v	set of nodes in a *tree* which hang on v ■	N8743: 2nd CD 11770-5: 2010-07-29
chip area	area occupied by a semiconductor circuit ■	N8753: 1st CD 29192-1: 2010-06-22
cipher	alternative term for encipherment system. ■	ISO/IEC 18033-1: 2005-02-01 (1st ed.)
cipher	cryptographic technique used to protect the confidentiality of data, and which consists of three component processes: an encryption algorithm, a decryption algorithm, and a method for generating keys [ISO/IEC 18033-1] ■	ISO/IEC 18033-2: 2006-05-01 (1st ed.)
cipher	alternative term for encryption system [ISO/IEC 18033-1] ■	N8751: FCD 29150: 2010-06-10
cipher text	data which has been transformed to hide its information content [ISO/IEC 10116:1997] ■	ISO/IEC 18033-2: 2006-05-01 (1st ed.)
ciphertext	data which has been transformed to hide its information content. ■	ISO/IEC 10116: 2006-02-01 (3rd ed.)
ciphertext	data which has been transformed to hide its information content [ISO/IEC 10116:2006] ■	ISO/IEC 9798-2: 2008-12-15 (3rd ed.)
ciphertext	data which has been transformed to hide its information content ■	ISO/IEC 9798-1: 2010-07-01 (3rd ed.)
ciphertext	data which has been transformed to hide its information content [ISO/IEC 10116:1997]. ■	ISO/IEC 18033-1: 2005-02-01 (1st ed.)
ciphertext	data which has been transformed to hide its information content [ISO/IEC 10116] ■	ISO/IEC 19772: 2009-02-15 (1st ed.)
ciphertext	data which has been transformed to hide its information content [ISO/IEC 9798-1:1997] ■	N8755: 1st CD 29192-2: 2010-06-22
ciphertext	data which has been transformed to hide its information content [ISO/IEC 10116:1997] ■	N8749: 2nd CD 18033-4: 2010-05-19

Term	Definition	ISO/IEC JTC 1/SC 27 Document
ciphertext	data which has been transformed to hide its information content [ISO/IEC 10116: 1997] ■	N8757: 2nd WD 29192-3: 2010-07-01
ciphertext	data which has been transformed to hide its information content [ISO/IEC 10116:2006] ■	N8751: FCD 29150: 2010-06-10
ciphertext	data which has been transformed to hide its information content [ISO/IEC 9798-1:1997] ■	ISO/IEC FDIS 18033-3: 2010-07-12
ciphertext	data which has been transformed to hide its information content [ISO/IEC 9798-1:2010] ■	N8861: PreFDIS 9797-1: 2010-09-03
claim	assertion of authenticity open to challenge ■	N8802: FCD 24745: 2010-05-19
claimant	entity whose identity can be authenticated, including the functions and the private data necessary to engage in authentication exchanges on behalf of a principal [ISO/IEC 9798-5:2004] ■	ISO/IEC 9798-2: 2008-12-15 (3rd ed.)
claimant	entity whose identity can be authenticated, including the functions and the private data necessary to engage in authentication exchanges on behalf of a principal ■	ISO/IEC 9798-5: 2009-12-15 (3rd ed.)
claimant	entity which is or represents a principal for the purposes of authentication NOTE A claimant includes the functions and the private data necessary for engaging in authentication exchanges on behalf of a principal. ■	ISO/IEC 9798-1: 2010-07-01 (3rd ed.)
claimant	entity which is or represents a principal for the purposes of authentication [ISO/IEC 9798-1] ■	N8762: 1st WD 20009-1: 2010-07-13
claimant	entity whose identity can be authenticated, including the functions and the private data necessary to engage in authentication exchanges on behalf of a principal ■	N8759: 2nd WD 29192-4: 2010-06-15
claimant	<biometric verification> individual who is seeking, and is the object of, biometric verification ■	ISO/IEC 24761: 2009-05-15 (1st ed.)
Claimant	entity which is or represents a principal for the purposes of authentication. NOTE A claimant includes the functions necessary for engaging in authentication exchanges on behalf of a principal. ■	N8810: 1st CD 29115 | X.eaa: 2010-06-10
claimant	entity (3.1.1) that is the subject in an authentication (3.3.2) NOTE A possible interaction between a claimant and a verifier is specified in ISO/IEC 9798, Entity Authentication. ■	N8804: 3rd CD 24760-1: 2010-06-11
claimant	individual making a claim that can be verified. NOTE Claims can be verified in a number of ways, some of which may be based on biometrics. ■	N8802: FCD 24745: 2010-05-19

Term	Definition	ISO/IEC JTC 1/SC 27 Document
claimant parameter	public data item, number or bit string, specific to a given claimant within the domain ■	ISO/IEC 9798-5: 2009-12-15 (3rd ed.)
claimant parameter	public data item, number or bit string, specific to a given claimant within the domain ■	N8759: 2nd WD 29192-4: 2010-06-15
class	set of ISO/IEC 15408 families that share a common focus ■	ISO/IEC 15408-1: 2009-12-15 (3rd ed.)
cleartext	alternative term for plaintext. ■	ISO/IEC 18033-1: 2005-02-01 (1st ed.)
cleartext	alternative term for plaintext ■	N8751: FCD 29150: 2010-06-10
CM documentation	all CM documentation including CM output, CM list (configuration list), CM system records, CM plan and CM usage documentation ■	ISO/IEC 15408-1: 2009-12-15 (3rd ed.)
coherent	logically ordered and having discernible meaning NOTE For documentation, this addresses both the actual text and the structure of the document, in terms of whether it is understandable by its target audience. ■	ISO/IEC 15408-1: 2009-12-15 (3rd ed.)
cohesion	module strength; manner and degree to which the tasks performed by a single software module are related to one another [IEEE Std 610.12-1990] NOTE Types of cohesion include coincidental, communicational, functional, logical, sequential, and temporal. These types of cohesion are described by the relevant term entry. ■	ISO/IEC 15408-1: 2009-12-15 (3rd ed.)
coincidental cohesion	module with the characteristic of performing unrelated, or loosely related, activities [IEEE Std 610.12-1990] NOTE See also cohesion (3.2.3). ■	ISO/IEC 15408-1: 2009-12-15 (3rd ed.)
collection	process of gathering the physical items that contain potential digital evidence ■	N8640: 3rd WD 27037: 2010-05-31
collision-resistant hash-function	hash-function satisfying the following property: it is computationally infeasible to find any two distinct inputs which map to the same output NOTE – computational feasibility depends on the specific security requirements and environment. ■	ISO/IEC 10118-1: 2000-06-15 (2nd ed.)
collision-resistant hash-function	hash-function satisfying the following property: - it is computationally infeasible to find any two distinct inputs which map to the same output [ISO/IEC 10118-1] ■	ISO/IEC FDIS 9797-2: 2009-09-18
collision-resistant hash-function	hash-function satisfying the following property: - it is computationally infeasible to find any two distinct inputs which map to the same output [ISO/IEC 10118-1] ■	ISO/IEC FDIS 9796-2: 2010-09-10

Term	Definition	ISO/IEC JTC 1/SC 27 Document
collision-resistant hash-function	hash-function satisfying the following property: it is computationally infeasible to find any two distinct inputs which map to the same output NOTE - Computational feasibility depends on the specific security requirements and environment. [ISO/IEC 10118-1:2000] ■	ISO/IEC 11770-4: 2006-05-01 (1st ed.)
collision-resistant hash-function	hash-function satisfying the following property: it is computationally infeasible to find any two distinct inputs which map to the same output NOTE Computational feasibility depends on the specific security requirements and environment. [ISO/IEC 10118-1:2000] ■	ISO/IEC 18014-1: 2008-09-01 (2nd ed.)
collision-resistant hash-function	hash-function satisfying the following property: it is computationally infeasible to find any two distinct inputs which map to the same output [ISO/IEC 10118-1:2000, definition 3.2] ■	ISO/IEC 18014-3: 2009-12-15 (2nd ed.)
collision-resistant hash-function	hash-function satisfying the following property: it is computationally infeasible to find any two distinct inputs which map to the same output NOTE - computational feasibility depends on the specific security requirements and environment. [ISO/IEC 10118-1] ■	N8760: 1st WD 20008-1: 2010-06-14
collision-resistant hash-function	hash-function satisfying the following property: it is computationally infeasible to find any two distinct inputs which map to the same output NOTE computational feasibility depends on the specific security requirements and environment. [ISO/IEC 10118-1] ■	N8763: 1st WD 20009-2: 2010-06-20
collision-resistant hash-function	hash-function satisfying the following property: it is computationally infeasible to find any two distinct inputs which map to the same output [ISO/IEC 10118-1] ■	N8751: FCD 29150: 2010-06-10
collision-resistant hash-function	hash-function satisfying the following property: it is computationally infeasible to find any two distinct inputs which map to the same output NOTE Computational feasibility depends on the specific security requirements and environment. [ISO/IEC 10118-1] ■	ISO/IEC 14888-1: 2008-04-15 (2nd ed.)
collocation	installation of telecommunications facilities on the premises of other telecommunications carriers. {ITU-T format} ■	ISO/IEC 27011/x.1051: 2008-12-15 (1st ed)
Common Attack Pattern Enumeration and Classification CAPEC	publicly available collection of structured attack patterns ■	N8784: 1st WD 20004: 2010-08-06

Term	Definition	ISO/IEC JTC 1/SC 27 Document
common coupling	relationship between two modules sharing a common data area or other common system resource NOTE Global variables indicate that modules using those global variables are common coupled. Common coupling through global variables is generally allowed, but only to a limited degree. For example, variables that are placed into a global area, but are used by only a single module, are inappropriately placed, and should be removed. Other factors that need to be considered in assessing the suitability of global variables are: The number of modules that modify a global variable: In general, only a single module should be allocated the responsibility for controlling the contents of a global variable, but there may be situations in which a second module may share that responsibility; in such a case, sufficient justification must be provided. It is unacceptable for this responsibility to be shared by more than two modules. (In making this assessment, care should be given to determining the module actually responsible for the contents of the variable; for example, if a single routine is used to modify the variable, but that routine simply performs the modification requested by its caller, it is the calling module that is responsible, and there may be more than one such module). Further, as part of the complexity determination, if two modules are responsible for the contents of a global variable, there should be clear indications of how the modifications are coordinated between them. The number of modules that reference a global variable: Although there is generally no limit on the number of modules that reference a global variable, cases in which many modules make such a reference should be examined for validity and necessity. ■	ISO/IEC 15408-1: 2009-12-15 (3rd ed.)
common identifier	identifier for correlating identity references and biometric references in physically or logically separated databases ■	N8802: FCD 24745: 2010-05-19
Common Weakness Enumeration - CWE	publicly available collection of software weaknesses ■	N8784: 1st WD 20004: 2010-08-06
communication bandwidth	number of bits per second that can be transmitted over a specified communication channel ■	N8753: 1st CD 29192-1: 2010-06-22
communication centre	building where facilities for providing telecommunications business are sited. {ITU-T format} ■	ISO/IEC 27011/x.1051: 2008-12-15 (1st ed)

Term	Definition	ISO/IEC JTC 1/SC 27 Document
communicational cohesion	module containing functions that produce output for, or use output from, other functions within the module [IEEE Std 610.12-1990] NOTE 1 See also cohesion (3.2.3). NOTE 2 An example of a communicationally cohesive module is an access check module that includes mandatory, discretionary, and capability checks. ■	ISO/IEC 15408-1: 2009-12-15 (3rd ed.)
comparison	estimation, calculation or measurement of similarity or dissimilarity between one or more recognition biometric samples and one or more biometric reference templates ■	ISO/IEC 24761: 2009-05-15 (1st ed.)
comparison decision	determination of whether the recognition biometric sample(s) and biometric reference(s) have the same biometric source, based on a comparison score(s), a decision policy(ies) including a threshold, and possibly other inputs NOTE 1 Definition from [2]. NOTE 2 A match is a positive comparison decision. NOTE 3 A non-match is a negative comparison decision. NOTE 4 A decision of "undetermined" can sometimes be given. ■	ISO/IEC 19792: 2009-08-01 (1st ed.)
comparison decision	determination of whether the recognition biometric sample(s) and biometric reference template(s) have the same biometric source, based on comparison scores, decision policies (including threshold values), and possibly other inputs to the comparison decision ■	ISO/IEC 24761: 2009-05-15 (1st ed.)
comparison score	numerical value (or set of values) resulting from a comparison NOTE Definition from [2]. ■	ISO/IEC 19792: 2009-08-01 (1st ed.)
comparison score	numerical value (or set of values) resulting from a comparison ■	ISO/IEC 24761: 2009-05-15 (1st ed.)
compatible	<components> property of a component able to provide the services required by the other component, through the corresponding interfaces of each component, in consistent operational environments ■	ISO/IEC 15408-1: 2009-12-15 (3rd ed.)
complete	property where all necessary parts of an entity have been provided NOTE In terms of documentation, this means that all relevant information is covered in the documentation, at such a level of detail that no further explanation is required at that level of abstraction. ■	ISO/IEC 15408-1: 2009-12-15 (3rd ed.)

Term	Definition	ISO/IEC JTC 1/SC 27 Document
complexity	measure of how difficult software is to understand, and thus to analyse, test, and maintain [IEEE Std 610.12-1990] NOTE Reducing complexity is the ultimate goal for using modular decomposition, layering and minimization. Controlling coupling and cohesion contributes significantly to this goal. A good deal of effort in the software engineering field has been expended in attempting to develop metrics to measure the complexity of source code. Most of these metrics use easily computed properties of the source code, such as the number of operators and operands, the complexity of the control flow graph (cyclomatic complexity), the number of lines of source code, the ratio of comments to executable code, and similar measures. Coding standards have been found to be a useful tool in generating code that is more readily understood. The TSF internals (ADV_INT) family calls for a complexity analysis in all components. It is expected that the developer will provide support for the claims that there has been a sufficient reduction in complexity. This support could include the developer's programming standards, and an indication that all modules meet the standard (or that there are some exceptions that are justified by software engineering arguments). It could include the results of tools used to measure some of the properties of the source code, or it could include other support that the developer finds appropriate. ■	ISO/IEC 15408-1: 2009-12-15 (3rd ed.)
component	smallest selectable set of elements on which requirements may be based ■	ISO/IEC 15408-1: 2009-12-15 (3rd ed.)
component	identifiable and distinct portion of an operational system that implements part of that system's functionality ■	ISO/IEC TR 19791: 2010-04-01 (2nd ed.)
component TOE	successfully evaluated TOE that is part of another composed TOE ■	ISO/IEC 15408-1: 2009-12-15 (3rd ed.)
composed assurance package	assurance package consisting of requirements drawn from ISO/IEC 15408-3 (predominately from the ACO class), representing a point on ISO/IEC 15408 predefined composition assurance scale ■	ISO/IEC 15408-1: 2009-12-15 (3rd ed.)
composed TOE	TOE comprised solely of two or more components that have been successfully evaluated ■	ISO/IEC 15408-1: 2009-12-15 (3rd ed.)
composite number **composite**	Integer $N > 1$ is composite if it is not prime, i.e. there exist divisors of N that are not trivial divisors. ■	ISO/IEC 18032: 2005-01-15 (1st ed.)
compromise	unauthorized disclosure, modification, substitution, or use of critical security parameters (ISO/IEC 19790:2006, 3.13) or the unauthorized modification or substitution of public security parameters (ISO/IEC 19790:2006, 3.58) ■	ISO/IEC 24759: 2008-07-01 (1st ed.)

Term	Definition	ISO/IEC JTC 1/SC 27 Document
compromise	the unauthorised disclosure, modification, substitution, or use of sensitive data or an unauthorised breach of physical security ■	N8776: 2nd WD 19790: 2010-07-16
computing and related equipment	computer, network, telecommunications and peripheral equipment that support the information processing activities of organizations ■	ISO/IEC 24762: 2008-02-01 (1st ed.)
concrete group	explicit description of a finite abelian group, together with algorithms for performing the group operation and for encoding and decoding group elements as octet strings NOTE See Clause 10.1. ■	ISO/IEC 18033-2: 2006-05-01 (1st ed.)
conditional self-test	a test performed by a cryptographic module when the conditions specified for the test occur ■	N8776: 2nd WD 19790: 2010-07-16
confidence	A belief that a deliverable will perform in the way expected or claimed (i.e. properly, trustworthy, enforce security policy, reliably, effectively). ■	ISO/IEC TR 15443-1: 2005-02-01 (1st ed.)
confidence interval	lower estimate L and an upper estimate U for a parameter x such that the probability of the true value of x being between L and U is the stated value (e.g. 95 %) [ISO/IEC 19795-1:2006, definition 4.8.2] NOTE A confidence interval is always associated with a corresponding stated value of probability. In this International Standard the stated value of probability is termed "confidence value" ■	ISO/IEC 19792: 2009-08-01 (1st ed.)
confidence value	stated value of probability corresponding to a specified confidence interval ■	ISO/IEC 19792: 2009-08-01 (1st ed.)
confidentiality	property that information is not made available or disclosed to unauthorized individuals, entities, or processes (2.40) ■	N8718: 1st WD 27000: 2010-05-27
confidentiality	property that information is not made available or disclosed to unauthorized individuals, entities, or processes [ISO/IEC PDTR 13335-1:2001] ■	N8749: 2nd CD 18033-4: 2010-05-19
confidentiality	property that information is not made available or disclosed to unauthorized individuals, entities or processes [ISO/IEC 7498-2:1989] ■	ISO/IEC 21827: 2008-10-15 (2nd ed.)
confidentiality	the property that information is not made available or disclosed to unauthorised entities ■	N8776: 2nd WD 19790: 2010-07-16
confidentiality	property that information is not made available or disclosed to unauthorized individuals, entities, or processes (2.31) [ISO 27000] ■	N8732: 3rd WD 29193: 2010-08-06

Term	Definition	ISO/IEC JTC 1/SC 27 Document
configuration item	object managed by the CM system during the TOE development NOTE These may be either parts of the TOE or objects related to the development of the TOE like evaluation documents or development tools. CM items may be stored in the CM system directly (for example files) or by reference (for example hardware parts) together with their version. ■	ISO/IEC 15408-1: 2009-12-15 (3rd ed.)
configuration list	configuration management output document listing all configuration items for a specific product together with the exact version of each configuration management item relevant for a specific version of the complete product NOTE This list allows distinguishing the items belonging to the evaluated version of the product from other versions of these items belonging to other versions of the product. The final configuration management list is a specific document for a specific version of a specific product. (Of course the list can be an electronic document inside of a configuration management tool. In that case it can be seen as a specific view into the system or a part of the system rather than an output of the system. However, for the practical use in an evaluation the configuration list will probably be delivered as a part of the evaluation documentation.) The configuration list defines the items that are under the configuration management requirements of ALC_CMC. ■	ISO/IEC 15408-1: 2009-12-15 (3rd ed.)
configuration management	Technical and organizational activities comprising: - configuration identification; - configuration control; - configuration status accounting; - configuration auditing. [ISO 10007:2003 - Quality management systems - Guidelines for configuration management] ■	N8638: 3rd WD 27036: 2010-08-13
configuration management CM	discipline applying technical and administrative direction and surveillance to identify and document the functional and physical characteristics of a configuration item, control changes to those characteristics, record and report change processing and implementation status and verify compliance with specified requirements NOTE Adapted from IEEE Std 610.12. ■	ISO/IEC 15408-1: 2009-12-15 (3rd ed.)
configuration management evidence	everything that may be used to establish confidence in the correct operation of the CM system NOTE For example, CM output, rationales provided by the developer, observations, experiments or interviews made by the evaluator during a site visit. ■	ISO/IEC 15408-1: 2009-12-15 (3rd ed.)

Term	Definition	ISO/IEC JTC 1/SC 27 Document
configuration management output	results, related to configuration management, produced or enforced by the configuration management system NOTE These configuration management related results could occur as documents (for example filled paper forms, configuration management system records, logging data, hard-copies and electronic output data) as well as actions (for example manual measures to fulfil configuration management instructions). Examples of such configuration management outputs are configuration lists, configuration management plans and/or behaviours during the product life-cycle. ■	ISO/IEC 15408-1: 2009-12-15 (3rd ed.)
configuration management plan	description of how the configuration management system is used for the TOE NOTE The objective of issuing a configuration management plan is that staff members can see clearly what they have to do. From the point of view of the overall configuration management system this can be seen as an output document (because it may be produced as part of the application of the configuration management system). From the point of view of the concrete project it is a usage document because members of the project team use it in order to understand the steps that they have to perform during the project. The configuration management plan defines the usage of the system for the specific product; the same system may be used to a different extent for other products. That means the configuration management plan defines and describes the output of the configuration management system of a company which is used during the TOE development. ■	ISO/IEC 15408-1: 2009-12-15 (3rd ed.)
configuration management system	set of procedures and tools (including their documentation) used by a developer to develop and maintain configurations of their products during their life-cycles NOTE Configuration management systems may have varying degrees of rigour and function. At higher levels, configuration management systems may be automated, with flaw remediation, change controls, and other tracking mechanisms. ■	ISO/IEC 15408-1: 2009-12-15 (3rd ed.)
configuration management system CMS	the management of security features and assurances through control of changes made to hardware, software and documentation of a cryptographic module ■	N8776: 2nd WD 19790: 2010-07-16

Term	Definition	ISO/IEC JTC 1/SC 27 Document
configuration management system records	output produced during the operation of the configuration management system documenting important configuration management activities NOTE Examples of configuration management system records are configuration management item change control forms or configuration management item access approval forms. ■	ISO/IEC 15408-1: 2009-12-15 (3rd ed.)
configuration management tools	manually operated or automated tools realising or supporting a configuration management system NOTE For example tools for the version management of the parts of the TOE. ■	ISO/IEC 15408-1: 2009-12-15 (3rd ed.)
configuration management usage documentation	part of the configuration management system which describes how the configuration management system is defined and applied by using, for example, handbooks, regulations and/or documentation of tools and procedures ■	ISO/IEC 15408-1: 2009-12-15 (3rd ed.)
confirm	declare that something has been reviewed in detail with an independent determination of sufficiency NOTE The level of rigour required depends on the nature of the subject matter. This term is only applied to evaluator actions. ■	ISO/IEC 15408-1: 2009-12-15 (3rd ed.)
conformity	fulfillment of a requirement NOTE The term "conformance" is synonymous but deprecated. ■	N8718: 1st WD 27000: 2010-05-27
congruence	property of a set of integers which differ from each other by a multiple of the modulus. Congruence is indicated by the symbol ≡. For example, 39 ≡ 6 (mod 11) indicates that 39 and 6 are congruent with respect to the modulus 11, i.e., 39 − 6 = 33, which is a multiple of 11. ■	ISO/IEC 7064: 2003-02-15 (2nd ed.)
connectivity	property of the TOE allowing interaction with IT entities external to the TOE NOTE This includes exchange of data by wire or by wireless means, over any distance in any environment or configuration. ■	ISO/IEC 15408-1: 2009-12-15 (3rd ed.)
consent	PII principal's freely given, specific and informed indication by which his agreement to the processing of his personally identifiable information is signified ■	N8806: 4th CD 29100: 2010-06-10
consequence	outcome of an event (2.18) affecting objectives [ISO Guide 73:2009] ■	N8718: 1st WD 27000: 2010-05-27
consequence	outcome of an event affecting objectives [ISO 31000] NOTE In the context of information security risks, only negative consequences (losses) are considered ■	N8923: FCD 27005: 2010-06-02

Term	Definition	ISO/IEC JTC 1/SC 27 Document
consistency	degree of uniformity, standardization and freedom from contradiction among the documents or parts of a system or component [IEEE-Std. 610] ■	ISO/IEC 21827: 2008-10-15 (2nd ed.)
consistent	relationship between two or more entities such that there are no apparent contradictions between these entities ■	ISO/IEC 15408-1: 2009-12-15 (3rd ed.)
content coupling	relationship between two modules where one makes direct reference to the internals of the other NOTE Examples include modifying code of, or referencing labels internal to, the other module. The result is that some or all of the content of one module are effectively included in the other. Content coupling can be thought of as using unadvertised module interfaces; this is in contrast to call coupling, which uses only advertised module interfaces. ■	ISO/IEC 15408-1: 2009-12-15 (3rd ed.)
control	measure that is modifying risk (2.45) NOTE Control is also used as a synonym for safeguard or countermeasure. ■	N8718: 1st WD 27000: 2010-05-27
control	measure that is modifying risk [ISO 31000:2009] NOTE 1 In information security context, control includes policies, procedures, guidelines, practices or organizational structures, which can be administrative, technical, management, or legal in nature (see ISO/IEC 27000:2009) NOTE 2 Control is also used as a synonym for safeguard or countermeasure. ■	N8923: FCD 27005: 2010-06-02
control information	information that is entered into a cryptographic module for the purposes of directing the operation of the module ■	N8776: 2nd WD 19790: 2010-07-16
control objective	statement describing what is to be achieved as a result of implementing controls (2.13) ■	N8718: 1st WD 27000: 2010-05-27
control value	random number provided by a validator that is a means by which the validator can check whether an ACBio instance is generated at the validator's request or not ■	ISO/IEC 24761: 2009-05-15 (1st ed.)
converting a number to a string	during computation of the round-function, integers need to be converted to strings of *L* bits. Where this is required, the string of bits shall be made equal to the binary representation of the integer, with the left-most bit of the string corresponding to the most significant bit of the binary representation. If the resulting string of bits has less than *L* bits, then the string shall be left-padded with the appropriate number of zeros to make it of length *L*. ■	ISO/IEC 10118-4: 1998-12-15 (1st ed.)

Term	Definition	ISO/IEC JTC 1/SC 27 Document
converting a string to a number	During computation of the round-function, strings of bits need to be converted into integers. Where this is required, the integer shall be made equal to the number having binary representation equal to the binary string, where the left-most bit of the string is considered as the most significant bit of the binary representation. ■	ISO/IEC 10118-4: 1998-12-15 (1st ed.)
cookie	<access control> capability or ticket in an access control system ■	N8624: 2nd CD 27032: 2010-06-15
cookie	<IPSec> data exchanged by ISAKMP to prevent certain Denial-of-Service attacks during the establishment of a security association ■	N8624: 2nd CD 27032: 2010-06-15
cookie	<HTTP> data exchanged between an HTTP server and a browser to store state information on the client side and retrieve it later for server use NOTE A web browser can be a client or a server. ■	N8624: 2nd CD 27032: 2010-06-15
coordinator	an optional participant that can assist vendors and finders in managing and disclosing vulnerability information NOTE Participation of a coordinator is optional ■	N8780: 1st CD 29147: 2010-06-10
copying	an accurate reproduction of information contained in the data objects independent of the original physical item [IOCE] ■	N8640: 3rd WD 27037: 2010-05-31
corporate information security policy	document that describes management direction and support for information security in accordance with business requirements and relevant laws and regulations NOTE The document describes the high level information security requirements that have to be followed throughout the organization. ■	ISO/IEC 27033-1: 2009-12-15 (1st ed.)
corrective action	action to eliminate the cause of a detected non-conformity (2.35) or other undesirable situation [ISO 9000:2005] ■	N8718: 1st WD 27000: 2010-05-27
correctness	for specified security requirements, the representation of a product or system that shows that the implementation of the requirement is correct ■	ISO/IEC 21827: 2008-10-15 (2nd ed.)
COTS	commercial-off-the-shelf product ■	N8732: 3rd WD 29193: 2010-08-06
counter	bit array of length n bits (where *n* is the size of the underlying block cipher) which is used in the Counter mode; its value when considered as the binary representation of an integer increases by one (modulo 2^n) after each block of plaintext is processed. ■	ISO/IEC 10116: 2006-02-01 (3rd ed.)
counter, verb	meet an attack where the impact of a particular threat is mitigated but not necessarily eradicated ■	ISO/IEC 15408-1: 2009-12-15 (3rd ed.)

Term	Definition	ISO/IEC JTC 1/SC 27 Document
countermeasure control	means of managing risk, including policies, procedures, guidelines, practices or organizational structures, which can be administrative, technical, management, or legal in nature [ISO/IEC 27000:2009] ■	N8624: 2nd CD 27032: 2010-06-15
coupling	manner and degree of interdependence between software modules [IEEE Std 610.12-1990] NOTE Types of coupling include call, common and content coupling. These are characterised below. ■	ISO/IEC 15408-1: 2009-12-15 (3rd ed.)
coupon	pair of pre-computed numbers to be used only once; one is kept secret and the other remains secret until its use by an entity ■	ISO/IEC 9798-5: 2009-12-15 (3rd ed.)
coupon	coupon is pre-computed numbers to be used only once; one shall be kept secret and the second shall remain secret until its use by an entity ■	N8759: 2nd WD 29192-4: 2010-06-15
covert channel	enforced, illicit signalling channel that allows a user to surreptitiously contravene the multi-level separation policy and unobservability requirements of the TOE ■	ISO/IEC 15408-1: 2009-12-15 (3rd ed.)
cracked	software or data whose behavior has been modified by another software, generally to get access right, less or more illicit ■	N8732: 3rd WD 29193: 2010-08-06
credential	representation of information elements which can be used to corroborate an identity. NOTE - This definition refers to both electronic and paper credentials. ■	N8810: 1st CD 29115 | X.eaa: 2010-06-10
credential	attribute (3.1.2) constructed to facilitate authentication(3.3.2) NOTE 1 A credential is typically constructed to facilitate data authentication of its value and possibly of other identity information in an identity. NOTE 2 A credential can be printed on paper that typically has been prepared in a manner to assert it as valid. NOTE 3 In this document the term credential is used in a specific sense referring to an attribute, and not an identity that contains such an attribute. NOTE 4 The data authentication supported by a credential usually allows asserting the scope of application and the timeliness of the value. ■	N8804: 3rd CD 24760-1: 2010-06-11
Credential Service Provider	trusted entity that issues and manages credentials. The Credential Service Provider (CSP) may encompass Registration Authorities (RAs) and verifiers that it operates. A CSP may be an independent third party, or it may issue credentials for its own use. ■	N8810: 1st CD 29115 | X.eaa: 2010-06-10

Term	Definition	ISO/IEC JTC 1/SC 27 Document
critical	qualitative description used to emphasize the importance of a resource, process or function that must be available and operational constantly or available and operational at the earliest possible time after an incident, emergency or disaster has occurred ■	N8622: PreFDIS 27031: 2010-08-18
critical security parameter CSP	security related information whose disclosure or modification can compromise the security of a cryptographic module EXAMPLE Secret and private cryptographic keys, authentication data such as passwords, PINs, certificates or other trust anchors NOTE A CSP may be plaintext or encrypted ■	N8776: 2nd WD 19790: 2010-07-16
crypto officer	role taken by an individual or a process (i.e. subject) acting on behalf of an individual, allowing to perform cryptographic initialization or management functions of a cryptographic module [ISO/IEC 19790:2006, 3.19] ■	ISO/IEC 24759: 2008-07-01 (1st ed.)
crypto officer	role taken by an individual or a process (i.e., subject) acting on behalf of an individual allowing to perform cryptographic initialisation or management functions of a cryptographic module ■	N8776: 2nd WD 19790: 2010-07-16
cryptographic algorithm	well-defined computational procedure that takes variable inputs, which may include cryptographic keys, and produces an output ■	N8776: 2nd WD 19790: 2010-07-16
cryptographic bilinear map	any field containing a finite number of elements NOTE For any positive integer m and a prime p, there exists a finite field containing exactly p^m elements. This field is unique up to isomorphism and is denoted by $F(p^m)$, where p is called the characteristic of $F(p^m)$. ■	ISO/IEC 15946-1: 2008-04-15 (2nd ed.)
cryptographic boundary	explicitly defined continuous perimeter that establishes the physical bounds of a cryptographic module and contains all the hardware, software and/or firmware components of a cryptographic module [ISO/IEC 19790] ■	N8745: FCD 18031: 2010-05-18
cryptographic boundary	an explicitly defined continuous perimeter that establishes the physical and/or logical bounds of a cryptographic module and contains all the hardware, software, and/or firmware components of a cryptographic module ■	N8776: 2nd WD 19790: 2010-07-16
cryptographic check function	cryptographic transformation which takes as input a secret key and an arbitrary string, and which gives a cryptographic check value as output ■	ISO/IEC 13888-1: 2009-07-15 (3rd ed)
cryptographic check function	cryptographic transformation which takes as input a secret key and an arbitrary string, and which gives a cryptographic check value as output [ISO/IEC 9798-1] ■	ISO/IEC FDIS 13888-2: 2010-08-06

Term	Definition	ISO/IEC JTC 1/SC 27 Document
cryptographic check function	cryptographic transformation which takes as input a secret key and an arbitrary string, and which gives a cryptographic check value as output NOTE The computation of a correct check value without knowledge of the secret key shall be infeasible. ■	ISO/IEC 9798-1: 2010-07-01 (3rd ed.)
cryptographic check value	information which is derived by performing a cryptographic transformation on the data unit ■	ISO/IEC 9798-1: 2010-07-01 (3rd ed.)
cryptographic hash function	function that maps octet strings of any length to octet strings of fixed length, such that it is computationally infeasible to find correlations between inputs and outputs, and such that given one part of the output, but not the input, it is computationally infeasible to predict any bit of the remaining output. The precise security requirements depend on the application. NOTE See Clause 6.1. ■	ISO/IEC 18033-2: 2006-05-01 (1st ed.)
cryptographic hash function	a computationally efficient function mapping binary strings of arbitrary length to binary strings of fixed length, such that it is computationally infeasible to find two distinct values that hash into a common value ■	N8776: 2nd WD 19790: 2010-07-16
cryptographic hash value	mathematical value that is assigned to a file and used to "test" the file at a later date to verify that the data contained in the file has not been maliciously changed ■	ISO/IEC 18043: 2006-06-15 (1st ed.)
cryptographic key key	sequence of symbols that controls the operation of a cryptographic transformation EXAMPLE A cryptographic transformation may include but not limited to encipherment, decipherment, cryptographic check function computation, signature generation, or signature verification. ■	N8776: 2nd WD 19790: 2010-07-16
cryptographic key component key component	parameter used in conjunction with other key components in an approved security function to form a plaintext CSP or perform a cryptographic function ■	N8776: 2nd WD 19790: 2010-07-16
cryptographic module module	set of hardware, software, and/or firmware that implements security functions and are contained within the cryptographic boundary ■	N8776: 2nd WD 19790: 2010-07-16
cryptographic module security policy security policy	precise specification of the security rules under which a cryptographic module shall operate, including the rules derived from the requirements of this International Standard and additional rules imposed by the module [ISO/IEC 19790:2006, 3.18] NOTE See ISO/IEC 19790:2006, Annex B. ■	ISO/IEC 24759: 2008-07-01 (1st ed.)

Term	Definition	ISO/IEC JTC 1/SC 27 Document
cryptographic module security policy security policy	a precise specification of the security rules under which a cryptographic module shall operate, including the rules derived from the requirements of this international standard and additional rules imposed by the module NOTE See Annex B ■	N8776: 2nd WD 19790: 2010-07-16
cryptographic protocol	protocol which performs a security-related function using cryptography ■	N8778: 3rd CD 29128: 2010-06-11
cryptographic synchronization	co-ordination of the encryption and decryption processes. ■	ISO/IEC 10116: 2006-02-01 (3rd ed.)
cryptography	discipline that embodies principles, means, and mechanisms for the transformation of data in order to hide its information content, prevent its undetected modification and/or prevent its unauthorized use [ISO/IEC 7498-2:1989, definition 3.3.20] ■	ISO/IEC 18014-2: 2009-12-15 (2nd ed.)
customer	recipient of a product provided by the supplier NOTE 1 In a contractual situation, the customer is called the purchaser. NOTE 2 The customer may be, for example, the ultimate consumer, user, beneficiary or purchaser. NOTE 3 The customer can be either external or internal to the organization. See ISO 9000 and ISO/IEC 15504. ■	ISO/IEC 21827: 2008-10-15 (2nd ed.)
cybercrime	criminal activity where services and applications in the Cyberspace are used for or is the target of a crime, or where the Cyberspace is the source, tool, target, or place of a crime NOTE Simply seen, cybercrime is the use of the Cyberspace for illegal activity. This explanation, however, is too broad to be used as a definition. ■	N8624: 2nd CD 27032: 2010-06-15
cybersafety	the condition of being protected against physical, social, spiritual, financial, political, emotional, occupational, psychological, educational or other types or consequences of failure, damage, error, accidents, harm or any other event in the Cyberspace which could be considered non-desirable NOTE 1 This can take the form of being protected from the event or from exposure to something that causes health or economical losses. It can include protection of people or of assets. NOTE 2 Safety in general is also defined as the state of being certain that adverse effects will not be caused by some agent under defined conditions. ■	N8624: 2nd CD 27032: 2010-06-15

Term	Definition	ISO/IEC JTC 1/SC 27 Document
Cybersecurity Cyberspace security	preservation of confidentiality, integrity and availability of information in the Cyberspace NOTE 1 In addition, other properties, such as authenticity, accountability, non-repudiation, and reliability can also be involved. NOTE 2 Adapted from the definition for information security in ISO/IEC 27000:2009. ■	N8624: 2nd CD 27032: 2010-06-15
cyberspace	the complex environment resulting from the interaction of people, software and services on the Internet by means of technology devices and networks connected to it, which does not exist in any physical form ■	N8624: 2nd CD 27032: 2010-06-15
cyberspace application services	definition required ■	N8624: 2nd CD 27032: 2010-06-15
cyber-squatter	individuals or organizations that register and hold on to URLs that resembles references or names of other organizations in the real world ■	N8624: 2nd CD 27032: 2010-06-15
cyclic group	group E of n elements that contains an element $a \in E$, called the generator, of order n ■	ISO/IEC 14888-3: 2006-11-15 (2nd ed.)
d-ary tree	*tree* where each node has *d* children ■	N8743: 2nd CD 11770-5: 2010-07-29
data	collection of values assigned to base measures, derived measures and/or indicators [ISO/IEC 15939:2007] ■	ISO/IEC 27004: 2009-12-15 (1st ed.)
data element	integer or bit string or set of integers or set of bit strings [ISO/IEC 14888-1] ■	N8760: 1st WD 20008-1: 2010-06-14
data element	integer or bit string or set of integers or set of bit strings [ISO/IEC 14888-1] ■	N8763: 1st WD 20009-2: 2010-06-20
data element	integer or bit string or set of integers or set of bit strings ■	N8751: FCD 29150: 2010-06-10
data element	integer, bit string, set of integers or set of bit strings ■	ISO/IEC 14888-1: 2008-04-15 (2nd ed.)
data encapsulation mechanism	cryptographic mechanism, based on symmetric cryptographic techniques, which protects both the confidentiality and the integrity of data NOTE See Clause 8.2. ■	ISO/IEC 18033-2: 2006-05-01 (1st ed.)
Data Encryption Standard - DES	well-known symmetric encryption mechanism using a 56 bit key. Due to its short key length DES was replaced by the AES, but is still used in multiple encryption mode, e.g., 3DES or Triple DES (FIPS 46-3). ■	ISO/IEC 18028-4: 2005-04-01 (1st ed.)
data input	octet string which depends on the entire message or a portion of the message and which forms a part of the input to the signature generation process ■	ISO/IEC 9796-3: 2006-09-15 (2nd ed.)
data integrity	property that data has not been altered or destroyed in an unauthorized manner [ISO 7498-2] ■	ISO/IEC 13888-1: 2009-07-15 (3rd ed)
data integrity	property that data has not been altered or destroyed in an unauthorized manner [ISO 7498-2] ■	ISO/IEC FDIS 13888-2: 2010-08-06

Term	Definition	ISO/IEC JTC 1/SC 27 Document
data integrity	the property that data has not been altered or destroyed in an unauthorized manner [ISO/IEC 9797-1] ■	ISO/IEC 19772: 2009-02-15 (1st ed.)
data integrity	property that data has not been altered or destroyed in an unauthorized manner [ISO/IEC 7498-2:1989, definition 3.3.21] ■	ISO/IEC 18014-2: 2009-12-15 (2nd ed.)
data integrity	property that data has not been altered or destroyed in an unauthorized manner [ISO/IEC 9797-1:1999] ■	N8749: 2nd CD 18033-4: 2010-05-19
data integrity	property that data has not been altered or destroyed in an unauthorized manner [ISO 7498-2:1989] ■	ISO/IEC FDIS 11770-1: 2010-07-26
data integrity	property that data has not been altered or destroyed in an unauthorized manner [ISO 7498-2] ■	N8861: PreFDIS 9797-1: 2010-09-03
data items' representation	data item or its respective hash value [ISO/IEC 18014-1: 2008] ■	ISO/IEC 18014-3: 2009-12-15 (2nd ed.)
data items' representation	data item or some representation thereof such as a cryptographic hash value ■	ISO/IEC 18014-1: 2008-09-01 (2nd ed.)
data origin authentication	corroboration that the source of data received is as claimed [ISO 7498-2] ■	ISO/IEC 13888-1: 2009-07-15 (3rd ed)
data origin authentication	corroboration that the source of data received is as claimed [ISO 7498-2] ■	ISO/IEC FDIS 9798-6: 2010-08-05
data origin authentication	corroboration that the source of data received is as claimed [ISO/IEC 7498-2:1989, definition 3.3.22] ■	ISO/IEC 18014-2: 2009-12-15 (2nd ed.)
data origin authentication	corroboration that the source of data received is as claimed [ISO 7498-2:1989] ■	ISO/IEC FDIS 11770-1: 2010-07-26
data path	physical or logical route over which data passes NOTE A physical data path may be shared by multiple logical data paths ■	N8776: 2nd WD 19790: 2010-07-16
data storage	means for storing information from which data is submitted for delivery, or into which data is put by the delivery authority ■	ISO/IEC 13888-1: 2009-07-15 (3rd ed)
data string (data)	string of bits which is the input to a hash-function ■	ISO/IEC 10118-1: 2000-06-15 (2nd ed.)
deceptive software	software which performs activities on a user's computer without first notifying the user as to exactly what the software will do on the computer, or asking the user for consent to these actions EXAMPLE 1 A program that hijacks user configurations. EXAMPLE 2 A program that causes endless popup advertisements which cannot be easily stopped by the user. E EXAMPLE 3 Adware and spyware. ■	N8624: 2nd CD 27032: 2010-06-15
decipherment	alternative term for decryption. ■	ISO/IEC 18033-1: 2005-02-01 (1st ed.)
decipherment	reversal of a corresponding encipherment [ISO/IEC 11770-1:1996] ■	ISO/IEC 11770-3: 2008-07-15 (2nd ed.)

Term	Definition	ISO/IEC JTC 1/SC 27 Document
decipherment algorithm	alternative term for decryption algorithm. ■	ISO/IEC 18033-1: 2005-02-01 (1st ed.)
decision criteria	thresholds, targets, or patterns used to determine the need for action or further investigation, or to describe the level of confidence in a given result [ISO/IEC 15939:2007] ■	ISO/IEC 27004: 2009-12-15 (1st ed.)
decision policy	collection of parameters, rules and values used to determine the acceptance or rejection of the biometric recognition of the subject ■	ISO/IEC 19792: 2009-08-01 (1st ed.)
decryption	reversal of a corresponding encryption. [ISO/IEC 18033-1] ■	ISO/IEC 10116: 2006-02-01 (3rd ed.)
decryption	reversal of a corresponding encryption NOTE Decryption [30] and decipherment [24] are equivalent terms. ■	ISO/IEC 9798-5: 2009-12-15 (3rd ed.)
decryption	reversal of a corresponding encryption ■	ISO/IEC 9798-1: 2010-07-01 (3rd ed.)
decryption	reversal of a corresponding encipherment [ISO/IEC 11770-1:1996]. ■	ISO/IEC 18033-1: 2005-02-01 (1st ed.)
decryption	reversal of the corresponding encryption [ISO/IEC 11770-1:1996] ■	ISO/IEC 18033-2: 2006-05-01 (1st ed.)
decryption	reversal of a corresponding encryption [ISO/IEC 18033-1] ■	ISO/IEC 19772: 2009-02-15 (1st ed.)
decryption	reversal of a corresponding encipherment [ISO/IEC 11770-1:1996] ■	N8749: 2nd CD 18033-4: 2010-05-19
decryption	reversal of a corresponding encipherment [ISO/IEC 11770-1: 1996] ■	N8757: 2nd WD 29192-3: 2010-07-01
decryption	reversal of encryption by a cryptographic algorithm to produce a plaintext ■	N8751: FCD 29150: 2010-06-10
decryption	reversal of a corresponding encryption NOTE Decryption [ISO/IEC 18033-1] and decipherment [ISO/IEC 9798-1] are equivalent terms. ■	ISO/IEC FDIS 11770-1: 2010-07-26
decryption	reversal of a corresponding encryption [ISO/IEC 9798-1:2010] ■	N8861: PreFDIS 9797-1: 2010-09-03
decryption algorithm	process which transforms ciphertext into plaintext. ■	ISO/IEC 18033-1: 2005-02-01 (1st ed.)
decryption algorithm	process which transforms ciphertext into plaintext [ISO/IEC 18033-1] ■	ISO/IEC 18033-2: 2006-05-01 (1st ed.)
decryption algorithm	process which transforms a ciphertext into a plaintext [ISO/IEC 18033-1] ■	N8751: FCD 29150: 2010-06-10
de-enrolment	deletion of the biometric reference from storage and if necessary, associated data in connection with the enduser's identity from the biometric system ■	ISO/IEC 19792: 2009-08-01 (1st ed.)
definition field of an elliptic curve	field that includes all the coefficients of the equation describing an elliptic curve ■	ISO/IEC 15946-5: 2009-12-15 (1st ed.)
degraded mode of operation	mode where a subset of the entire set of algorithms, security functions, services or processes are available and/or configurable as a result of reconfiguration from an error state ■	N8776: 2nd WD 19790: 2010-07-16

Term	Definition	ISO/IEC JTC 1/SC 27 Document
deliverable	IT security product, system, service, process, or environmental factor (i.e. personnel, organisation) or the object of an assurance assessment. An object may be a Protection Profile (PP) or Security Target (ST) as defined by ISO/IEC15408-1. Note: ISO 9000:2000 holds that a service is a type of product and "product and/or service" when used in the ISO 9000 family of standards. ■	ISO/IEC TR 15443-1: 2005-02-01 (1st ed.)
deliverable	IT security product, system, service, process, or environment factor (i.e. personnel, organisation) in particular as object of an assurance assessment NOTE 1 An object may be a Protection Profile (PP) or Security Target (ST) as defined by ISO/IEC15408-1. NOTE 2 ISO 9000 holds that a service is a type of product and “product and/or service” when used in the ISO 9000 family of standards. NOTE 3 For the purpose of this part of ISO/IEC TR 15443, and similar to the usage in ISO 9000, the term product will generally be used in place of deliverable throughout the document. ■	ISO/IEC TR 15443-3: 2007-12-15 (1st ed.)
delivery	transmission of the finished TOE from the production environment into the hands of the customer NOTE This product life-cycle phase may include packaging and storage at the development site, but does not include transportations of the unfinished TOE or parts of the TOE between different developers or different development sites. ■	ISO/IEC 15408-1: 2009-12-15 (3rd ed.)
delivery authority	authority trusted by the sender to deliver the data from the sender to the receiver, and to provide the sender with evidence on the submission and transport of data upon request ■	ISO/IEC 13888-1: 2009-07-15 (3rd ed)
de-militarised zone - DMZ	separated area of a local or site network whose access is controlled by a specific policy using firewalls. A DMZ is not part of the internal network and is considered less secure. ■	ISO/IEC 18028-4: 2005-04-01 (1st ed.)
de-militarized zone - DMZ	perimeter network (also known as a screened sub-net) inserted as a "neutral zone" between networks ■	ISO/IEC 27033-1: 2009-12-15 (1st ed.)
demilitarized zone - DMZ	logical and physical network space between the perimeter router and the exterior firewall NOTE 1 The DMZ may be between networks and under close observation but does not have to be so. NOTE 2 They are generally unsecured areas containing bastion hosts that provide public services. ■	ISO/IEC 18043: 2006-06-15 (1st ed.)

Term	Definition	ISO/IEC JTC 1/SC 27 Document
demonstrable conformance	relation between an ST and a PP, where the ST provides a solution which solves the generic security problem in the PP NOTE The PP and the ST may contain entirely different statements that discuss different entities, use different concepts etc. Demonstrable conformance is also suitable for a TOE type where several similar PPs already exist, thus allowing the ST author to claim conformance to these PPs simultaneously, thereby saving work. ■	ISO/IEC 15408-1: 2009-12-15 (3rd ed.)
demonstrate	provide a conclusion gained by an analysis which is less rigorous than a "proof" ■	ISO/IEC 15408-1: 2009-12-15 (3rd ed.)
denial of service - DoS	prevention of authorized access to a system resource or the delaying of system operations and functions, with resultant loss of availability to authorized users ■	ISO/IEC 27033-1: 2009-12-15 (1st ed.)
Denial of Service - DoS	attack against a system to deter its availability. ■	ISO/IEC 18028-4: 2005-04-01 (1st ed.)
dependability	the degree to which the software is operable and capable of performing functionality or of delivering a service that can justifiably be relied upon (i.e., trusted) to be correct. To achieve dependability, the software should be able to avoid service failures that are more frequent or severe, or longer in duration, than is acceptable to users. Dependability may be viewed according to different, but complementary, properties (or "instances of dependability") required for a system to be considered dependable: - Availability - Integrity - Reliability - Safety - Maintainability - Security Two other properties are closely related to dependability: 1. Survivability 2. Trustworthiness. ■	N8732: 3rd WD 29193: 2010-08-06
dependency	relationship between components such that if a requirement based on the depending component is included in a PP, ST or package, a requirement based on the component that is depended upon must normally also be included in the PP, ST or package ■	ISO/IEC 15408-1: 2009-12-15 (3rd ed.)
dependent component	entity in a composed TOE, which is itself the subject of an evaluation, relying on the provision of services by a base component ■	ISO/IEC 15408-1: 2009-12-15 (3rd ed.)
derived measure	measure that is defined as a function of two or more values of base measures [ISO/IEC 15939:2007] ■	ISO/IEC 27004: 2009-12-15 (1st ed.)
describe	provide specific details of an entity ■	ISO/IEC 15408-1: 2009-12-15 (3rd ed.)

Term	Definition	ISO/IEC JTC 1/SC 27 Document
determine	affirm a particular conclusion based on independent analysis with the objective of reaching a particular conclusion NOTE The usage of this term implies a truly independent analysis, usually in the absence of any previous analysis having been performed. Compare with the terms "confirm" or "verify" which imply that an analysis has already been performed which needs to be reviewed ■	ISO/IEC 15408-1: 2009-12-15 (3rd ed.)
determine	affirm a particular conclusion based on independent analysis with the objective of reaching a particular conclusion NOTE The usage of this term implies a truly independent analysis, usually in the absence of any previous analysis having been performed. Compare with the terms "confirm" or "verify" which imply that an analysis has already been performed which needs to be reviewed ■	N8784: 1st WD 20004: 2010-08-06
deterministic algorithm	characteristic of an algorithm that states that given the same input, the same output is always produced ■	N8745: FCD 18031: 2010-05-18
deterministic random bit generator - DRBG	random bit generator that produces a random-appearing sequence of bits by applying a deterministic algorithm to a suitably random initial value called a seed and, possibly, some secondary inputs upon which the security of the random bit generator does not depend NOTE In particular, non-deterministic sources may also form part of these secondary inputs. ■	N8745: FCD 18031: 2010-05-18
developer	organization responsible for the development of the TOE ■	ISO/IEC 15408-1: 2009-12-15 (3rd ed.)
development	product life-cycle phase which is concerned with generating the implementation representation of the TOE NOTE Throughout the ALC requirements, development and related terms (developer, develop) are meant in the more general sense to comprise development and production. ■	ISO/IEC 15408-1: 2009-12-15 (3rd ed.)
development environment	environment in which the TOE is developed ■	ISO/IEC 15408-1: 2009-12-15 (3rd ed.)
development tools	tools (including test software, if applicable) supporting the development and production of the TOE NOTE For example, for a software TOE, development tools are usually programming languages, compilers, linkers and generating tools. ■	ISO/IEC 15408-1: 2009-12-15 (3rd ed.)
dictionary attack (on a password-based system)	attack on a cryptosystem that employs a search of a given list of passwords NOTE A dictionary attack on a password-based system can use a stored list of specific password values or a stored list of words from a natural language dictionary. ■	ISO/IEC 11770-4: 2006-05-01 (1st ed.)

Term	Definition	ISO/IEC JTC 1/SC 27 Document
differential power analysis - DPA	analysis of the variations of the electrical power consumption of a cryptographic module, for the purpose of extracting information correlated to cryptographic operation ■	N8776: 2nd WD 19790: 2010-07-16
digest function	function *d* which maps a string of bits and a long secret key to a short and fixed-length string of bits, i.e. a *b*-bit digest-value, that can readily be entered into or read from a user device, satisfying the following properties: - for any key *k* and any input string *m*, the function $d(m, k)$ can be computed efficiently; - it is computationally infeasible to find a pair of distinct data strings (m, m') for which the proportion of keys which satisfy $d(m, k) = d(m', k)$ is greater than $(2^{-b} + \varepsilon)$, where *b* is the bit length of a digest-value and ε is a value that is negligible relative to 2^{-b}. NOTE 1 In practice, the second digest function property should be satisfied if the key *k* is of the size of a typical cryptographic hash value, for example, 160 bits. This requirement derives from theoretical lower bounds on the key length for universal hash-functions, which are a general class of digest functions. More detailed discussions of this issue can be found in Annex F. NOTE 2 See Annexes D, F, and G for further discussions of key and digest lengths. ■	ISO/IEC FDIS 9798-6: 2010-08-05
digest-value	string of bits, computed as the output of a digest function, sent from the data originator to the data recipient that enables the recipient of data to check its correctness ■	ISO/IEC FDIS 9798-6: 2010-08-05
digital device	electronic equipment used to process or store digital data ■	N8640: 3rd WD 27037: 2010-05-31
digital evidence	information or data, stored or transmitted in binary form that may be relied upon ■	N8640: 3rd WD 27037: 2010-05-31
digital evidence copy	copy of the digital evidence that has been produced to maintain the reliability and integrity of the evidence by including both the digital evidence and a means of verifying it ■	N8640: 3rd WD 27037: 2010-05-31
Digital Evidence First Responder - DEFR	person that is authorized, trained and qualified to act first at an incident scene in performing digital evidence collection and acquisition with the responsibility for handling that evidence NOTE Authority, training and qualification are the expected requirements necessary to produce reliable digital evidence, but individual circumstances may result in an individual not adhering to all three requirements. In this case, the local law, organizational policy and individual circumstances should be considered. ■	N8640: 3rd WD 27037: 2010-05-31

Term	Definition	ISO/IEC JTC 1/SC 27 Document
Digital Evidence Specialist	person who can carry out the tasks of a DEFR and has specialized knowledge, skills and abilities to handle specific technical issues ■	N8640: 3rd WD 27037: 2010-05-31
digital signature	data appended to, or a cryptographic transformation of, a data unit that allows the recipient of the data unit to prove the source and integrity of the data unit and protect against forgery e.g. by the recipient [ISO 7498-2] ■	ISO/IEC 13888-1: 2009-07-15 (3rd ed)
digital signature	data appended to, or a cryptographic transformation of, a data unit that allows a recipient of the data unit to prove the origin and integrity of the data unit and protect the sender and the recipient of the data unit against forgery by third parties and sender against forgery by the recipient [ISO/IEC 11770-3:1999] ■	ISO/IEC 18014-1: 2008-09-01 (2nd ed.)
digital signature	data appended to, or a cryptographic transformation (see cryptography) of, a data unit that allows a recipient of the data unit to prove the source and integrity of the data unit and protect against forgery, e.g. by the recipient [ISO/IEC 7498-2:1989, definition 3.3.26] ■	ISO/IEC 18014-2: 2009-12-15 (2nd ed.)
digital signature	data appended to, or a cryptographic transformation of, a data unit that allows a recipient of the data unit to prove the source and integrity of the data unit and protect against forgery e.g. by the recipient [ISO/IEC 9798-1:1997] ■	ISO/IEC FDIS 11770-1: 2010-07-26
digital signature	data appended to, or a cryptographic transformation of a data unit that allows the recipient of the data unit to prove the origin and integrity of the data unit and protect against forgery (e.g., by the recipient) ■	N8776: 2nd WD 19790: 2010-07-16
digital signature	cryptographic transformation of a data unit that allows a recipient of the data unit to prove the origin and integrity of the data unit and protect the sender and the recipient of the data unit against forgery by third parties, and the sender against forgery by the recipient. NOTE – Digital signatures may be used by end entities (see below) for the purposes of authentication, of data integrity, and of non-repudiation of creation of data. The usage for non-repudiation of creation of data is the most important one for legally binding digital signatures. The definition above is taken from ISO/IEC 9798-1. ■	ISO/IEC 15945: 2002-02-01 (1st ed.)
digital signature	data appended to, or a cryptographic transformation (see cryptography) of, a data unit that allows a recipient of the data unit to prove the source and integrity of the data unit and protect against forgery e.g. by the recipient [ISO/IEC 7498-2:1989] ■	N8642: 2nd PDTR 29149: 2010-06-22

Term	Definition	ISO/IEC JTC 1/SC 27 Document
digital signature	data unit appended to, or a cryptographic transformation of, a data unit that allows a recipient of the data unit to prove the origin and integrity of the data unit and protect the sender and the recipient of the data unit against forgery by third parties, and the sender against forgery by the recipient ■	ISO/IEC 11770-3: 2008-07-15 (2nd ed.)
digital signature (signature)	data appended to, or a cryptographic transformation of, a data unit that allows the recipient of the data unit to prove the source and integrity of the data unit and protect against forgery, e.g. by the recipient ■	ISO/IEC 9798-1: 2010-07-01 (3rd ed.)
Digital Subscriber Line - DSL	technology providing fast access to networks over local telecommunications loops. ■	ISO/IEC 18028-4: 2005-04-01 (1st ed.)
direct entry	entry of a SSP or key component into a cryptographic module, using a device such as a keyboard ■	N8776: 2nd WD 19790: 2010-07-16
directly trusted CA	directly trusted CA is a CA whose public key has been obtained and is being stored by an end entity in a secure, trusted manner, and whose public key is accepted by that end entity in the context of one or more applications. ■	ISO/IEC 15945: 2002-02-01 (1st ed.)
directly trusted CA key	directly trusted CA key is a public key of a directly trusted CA. It has been obtained and is being stored by an end entity in a secure, trusted manner. It is used to verify certificates without being itself verified by means of a certificate created by another CA. NOTE – If, for example, the CAs of several organizations cross-certify each other (see Annex A), the directly trusted CA for an entity may be the CA of the entity's organization. Directly trusted CAs and directly trusted CA keys may vary from entity to entity. An entity may regard several CAs as directly trusted CAs. ■	ISO/IEC 15945: 2002-02-01 (1st ed.)
directory maintenance authority	entity responsible for making the public key certificates available online for ready use by the user entities ■	ISO/IEC FDIS 11770-1: 2010-07-26
directory service	service to search and retrieve information from a catalogue of well defined objects, which may contain information about certificates, telephone numbers, access conditions, addresses, etc. An example is provided by a directory service conforming to the ITU-T Rec. X.500 | ISO/IEC 9594-1. ■	ISO/IEC 15945: 2002-02-01 (1st ed.)

Term	Definition	ISO/IEC JTC 1/SC 27 Document
Discretionary Access Control	This subsystem provides user-specified, controlled sharing of resources. This control is established from security policies which define, given identified subjects and objects, the set of rules that are used by the system to determine whether a given subject is authorized to gain access to a specific object. DAC features include the means for restricting access to objects; the means for instantiating authorizations for objects; and the mechanisms for distribution, review, and revocation of access privileges, especially during object creation and deletion (Reference: NCSC-TG-009) DAC, as the name implies, permits the granting and revoking of access privileges to be left to the discretion of the individual users. A DAC mechanism allows users to grant or revoke access to any of the objects under their control without the intercession of a system administrator (Reference: 15th National Computer Security Conference (1992), Baltimore MD, pp. 554 - 563, David F. Ferraiolo and D. Richard Kuhn, National Institute of Standards and Technology) ■	N8812: 3rd WD 29146: 2010-07-14
disjoint signature	one or more signatures which together represent an entire set of code ■	N8776: 2nd WD 19790: 2010-07-16
disruption	incident, whether anticipated (e.g. hurricane) or unanticipated (e.g. power failure / outage or earthquake) which disrupts the normal course of operations at an organization location ■	N8622: PreFDIS 27031: 2010-08-18
distinguished encoding rules - DER	encoding rules that may be applied to values of types defined using the ASN.1 notation NOTE 1 As defined in the introduction to ISO/IEC 18028-4. NOTE 2 Application of these encoding rules produces a transfer syntax for such values. It is implicit that the same rules are also to be used for decoding. The DER is more suitable if the encoded value is small enough to fit into the available memory and there is a need to rapidly skip over some nested values. ■	ISO/IEC 18014-2: 2009-12-15 (2nd ed.)
distinguishing identifier	information which unambiguously distinguishes an entity in the non-repudiation process ■	ISO/IEC 13888-1: 2009-07-15 (3rd ed)
distinguishing identifier	information which unambiguously distinguishes an entity in the context of an authentication exchange ■	ISO/IEC 9798-1: 2010-07-01 (3rd ed.)
distinguishing identifier	information which unambiguously distinguishes an entity [ISO/IEC 11770-2] ■	N8760: 1st WD 20008-1: 2010-06-14
distinguishing identifier	information which unambiguously distinguishes an entity ■	ISO/IEC FDIS 11770-1: 2010-07-26
Distinguishing Identifier	Information which unambiguously distinguishes an entity in the context of an authentication exchange. ■	N8810: 1st CD 29115 | X.eaa: 2010-06-10

Term	Definition	ISO/IEC JTC 1/SC 27 Document
distinguishing identifier	information which unambiguously distinguishes an entity ■	ISO/IEC 11770-2: 2008-06-15 (2nd ed.)
distinguishing identifier	information which unambiguously distinguishes an entity [ISO/IEC 11770-1:1996] ■	ISO/IEC 11770-3: 2008-07-15 (2nd ed.)
diversification	deliberate creation of multiple, independent transformed biometric references from one or more biometric samples obtained from one data subject for the purposes of security and privacy enhancement NOTE 1 The diversification process should be irreversible. NOTE 2 The transformed biometric references should not be uniquely linkable. ■	N8802: FCD 24745: 2010-05-19
domain	collection of entities operating under a single security policy NOTE For example, public key certificates created either by a single certification authority, or by a collection of certification authorities using the same security policy. ■	ISO/IEC 9798-5: 2009-12-15 (3rd ed.)
domain	set of entities operating under a single security policy EXAMPLE public key certificates created by a single authority or by a set of authorities using the same security policy. [ISO/IEC 14888-1] ■	N8760: 1st WD 20008-1: 2010-06-14
domain	set of entities operating under a single security policy EXAMPLE public key certificates created by a single authority or by a set of authorities using the same security policy [ISO/IEC 14888-1] ■	N8763: 1st WD 20009-2: 2010-06-20
domain	collection of entities operating under a single security policy, e.g., public key certificates created either by a single certification authority, or by a collection of certification authorities using the same security policy ■	N8759: 2nd WD 29192-4: 2010-06-15
domain	set of entities operating under a single security policy [ISO/IEC 14888-1] ■	N8751: FCD 29150: 2010-06-10
domain	set of entities operating under a single security policy EXAMPLES public key certificates created by a single authority or by a set of authorities using the same security policy ■	ISO/IEC 14888-1: 2008-04-15 (2nd ed.)
domain of applicability context DA	environment where an entity (3.1.1) can use a set of attributes (3.1.3) for identification (3.2.1) and other purposes NOTE ITU-T X1252[[9]] uses the term context, this document prefers the term domain. EXAMPLE An IT system deployed by an organization that allows login to users is the domain for the user's login name. ■	N8804: 3rd CD 24760-1: 2010-06-11

Term	Definition	ISO/IEC JTC 1/SC 27 Document
domain of origin	property of an attribute (3.1.3) that specifies the domain where the attribute value has been created NOTE 1 The domain of origin typically specifies the meaning and format of the attribute value. Such specification may be based on international standards. NOTE 2 An attribute may contain an explicit value to reference its domain of origin, e.g. an ISO country code for a passport number. EXAMPLE The domain of origin of a club-membership number is the specific club that assigned the number. ■	N8804: 3rd CD 24760-1: 2010-06-11
domain parameter	data item which is common to and known by or accessible to all entities within the domain [ISO/IEC 14888-1:1998] NOTE The set of domain parameters may contain data items such as hash-function identifier, length of the hashtoken, maximum length of the recoverable part of the message, finite field parameters, elliptic curve parameters, or other parameters specifying the security policy in the domain. ■	ISO/IEC 9796-3: 2006-09-15 (2nd ed.)
domain parameter	public key, or function, agreed and used by all entities within the domain ■	ISO/IEC 9798-5: 2009-12-15 (3rd ed.)
domain parameter	data item which is common to and known by or accessible to all entities within the domain NOTE The set of domain parameters may contain data items such as hash-function identifier, length of the hash-token, length of the recoverable part of the message, finite field parameters, elliptic curve parameters, or other parameters specifying the security policy in the domain. [ISO/IEC 9796-3:2000] ■	ISO/IEC 11770-4: 2006-05-01 (1st ed.)
domain parameter	data element which is common to and known by or accessible to all entities within the domain [ISO/IEC 14888-1] ■	N8760: 1st WD 20008-1: 2010-06-14
domain parameter	data element which is common to and known by or accessible to all entities within the domain [ISO/IEC 14888-1] ■	N8763: 1st WD 20009-2: 2010-06-20
domain parameter	public key, or function, agreed and used by all entities within the domain ■	N8759: 2nd WD 29192-4: 2010-06-15
domain parameter	data element which is common to and known by or accessible to all entities within the domain [ISO/IEC 14888-1] ■	N8751: FCD 29150: 2010-06-10
domain parameter	data element which is common to and known by or accessible to all entities within the domain ■	ISO/IEC 14888-1: 2008-04-15 (2nd ed.)
domain separation	security architecture property whereby the TSF defines separate security domains for each user and for the TSF and ensures that no user process can affect the contents of a security domain of another user or of the TSF ■	ISO/IEC 15408-1: 2009-12-15 (3rd ed.)

Term	Definition	ISO/IEC JTC 1/SC 27 Document
DoS (Denial-of-Service) attack	prevention of authorized access to a system resource or the delaying of system operations and functions [ISO/IEC 18028-1] ■	ISO/IEC 18043: 2006-06-15 (1st ed.)
Dynamic Host Control Protocol - DHCP	an Internet protocol that dynamically provides IP addresses at start up (RFC 2131). ■	ISO/IEC 18028-4: 2005-04-01 (1st ed.)
effectiveness	extent to which planned activities are realized and planned results achieved [ISO 9000:2005] ■	N8718: 1st WD 27000: 2010-05-27
effectiveness	property of a system or product representing how well it provides security in the context of its proposed or actual operational use ■	ISO/IEC 21827: 2008-10-15 (2nd ed.)
efficiency	relationship between the results achieved and how well the resources have been used [ISO 9000:2005] ■	N8718: 1st WD 27000: 2010-05-27
electromagnetic emanations - EME	intelligence-bearing signal, which, if intercepted and analyzed, potentially discloses the information that is transmitted, received, handled, or otherwise processed by any information-processing equipment ■	N8776: 2nd WD 19790: 2010-07-16
electronic entry	the entry of SSPs or key components into a cryptographic module using electronic methods such key loader NOTE The operator of the key may have no knowledge of the value of the key being entered ■	N8776: 2nd WD 19790: 2010-07-16
element	indivisible statement of a security need ■	ISO/IEC 15408-1: 2009-12-15 (3rd ed.)
elliptic curve	set of points $P = (x, y)$, where x and y are elements of an explicitly given finite field, that satisfy a cubic equation without any singular point, together with the "point at infinity" denoted by O [ISO/IEC 15946-1:2002] NOTE For a mathematical definition of an elliptic curve over an explicitly given finite field, see Clause A.4. ■	ISO/IEC 9796-3: 2006-09-15 (2nd ed.)
elliptic curve	cubic curve without a singular point NOTE 1 A definition of a cubic curve is given in [29]. NOTE 2 The set of points of E under a certain addition law forms an abelian group. In this part of ISO/IEC 15946, we only deal with finite fields F as the definition field. When we describe the definition field F of an elliptic curve E explicitly, we denote the curve as E/F. NOTE 3 A detailed definition of an elliptic curve is given in Clause 4. [ISO/IEC 15946-1:2008] ■	ISO/IEC 15946-5: 2009-12-15 (1st ed.)

Term	Definition	ISO/IEC JTC 1/SC 27 Document
elliptic curve	any cubic curve *E* without any singular point NOTE 1 The set of points of *E* is an abelian group. The field that includes all coefficients of the equation describing *E* is called the definition field of *E*. In this part of ISO/IEC 15946, we deal with only finite fields *F* as the definition field. When we describe the definition field *F* of *E* explicitly, we denote the curve as *E*/*F*. NOTE 2 A definition of a cubic curve is given [16]. (N6693rev1: 15946-1:2008/DCOR1 2008-07-17) ■	ISO/IEC 15946-1: 2008-04-15 (2nd ed.)
empty string	string of symbols of length zero ■	N8734: 3rd CD 9797-3: 2010-06-16
Encapsulating Security Payload - ESP	an IP-based protocol providing confidentiality services for data. Specifically, ESP provides encryption as a security service to protect the data content of the IP packet. ESP is an Internet standard (RFC 2406). ■	ISO/IEC 18028-4: 2005-04-01 (1st ed.)
encipherment	alternative term for encryption. ■	ISO/IEC 18033-1: 2005-02-01 (1st ed.)
encipherment	(reversible) transformation of data by a cryptographic algorithm to produce ciphertext, i.e. to hide the information content of the data [ISO/IEC 9797-1:1999, ISO/IEC 11770-1:1996, ISO/IEC 18033-1:2005] ■	ISO/IEC 11770-3: 2008-07-15 (2nd ed.)
encipherment algorithm	alternative term for encryption algorithm. ■	ISO/IEC 18033-1: 2005-02-01 (1st ed.)
encipherment system	alternative term for encryption system. ■	ISO/IEC 18033-1: 2005-02-01 (1st ed.)
encompassing signature	single signature for an entire set of code ■	N8776: 2nd WD 19790: 2010-07-16
encountered potential vulnerabilities	potential weakness in the TOE identified by the evaluator while performing evaluation activities that could be used to violate the SFRs ■	ISO/IEC 15408-1: 2009-12-15 (3rd ed.)
encountered potential vulnerabilities	potential weakness in the TOE identified by the evaluator while performing evaluation activities that could be used to violate the SFRs ■	N8784: 1st WD 20004: 2010-08-06
encrypted key	a cryptographic key that has been encrypted using an approved security function with a key encryption key. Considered protected ■	N8776: 2nd WD 19790: 2010-07-16
encryption	(reversible) transformation of data by a cryptographic algorithm to produce ciphertext, i.e., to hide the information content of the data. [ISO/IEC 18033-1] ■	ISO/IEC 10116: 2006-02-01 (3rd ed.)
encryption	reversible operation by a cryptographic algorithm converting data into ciphertext, so as to hide the information content of the data NOTE Encryption [30] and encipherment [24] are equivalent terms. ■	ISO/IEC 9798-5: 2009-12-15 (3rd ed.)

Term	Definition	ISO/IEC JTC 1/SC 27 Document
encryption	reversible operation by a cryptographic algorithm converting data into ciphertext so as to hide the information content of the data ■	ISO/IEC 9798-1: 2010-07-01 (3rd ed.)
encryption	(reversible) transformation of data by a cryptographic algorithm to produce ciphertext, i.e., to hide the information content of the data [ISO/IEC 9797-1]. ■	ISO/IEC 18033-1: 2005-02-01 (1st ed.)
encryption	(reversible) transformation of data by a cryptographic algorithm to produce cipher text, i.e., to hide the information content of the data [ISO/IEC 9797-1] ■	ISO/IEC 18033-2: 2006-05-01 (1st ed.)
encryption	(reversible) transformation of data by a cryptographic algorithm to produce ciphertext, i.e., to hide the information content of the data [ISO/IEC 18033-1] ■	ISO/IEC 19772: 2009-02-15 (1st ed.)
encryption	(reversible) transformation of data by a cryptographic algorithm to produce ciphertext, i.e., to hide the information content of the data [ISO/IEC 9797-1:1996] ■	N8749: 2nd CD 18033-4: 2010-05-19
encryption	(reversible) transformation of data by a cryptographic algorithm to produce ciphertext, i.e., to hide the information content of the data [ISO/IEC 9797-1: 1996] ■	N8757: 2nd WD 29192-3: 2010-07-01
encryption	(reversible) transformation of data by a cryptographic algorithm to produce a ciphertext, i.e., to hide the information content of the data [ISO/IEC 9797-1] ■	N8751: FCD 29150: 2010-06-10
encryption	(reversible) transformation of data by a cryptographic algorithm to produce ciphertext, i.e., to hide the information content of the data NOTE Encryption [ISO/IEC 18033-1] and encipherment [ISO/IEC 9798-1] are equivalent terms. ■	ISO/IEC FDIS 11770-1: 2010-07-26
encryption	reversible operation by a cryptographic algorithm converting data into ciphertext so as to hide the information content of the data [ISO/IEC 9798-1:2010] ■	N8861: PreFDIS 9797-1: 2010-09-03
encryption algorithm	process which transforms plaintext into ciphertext. ■	ISO/IEC 18033-1: 2005-02-01 (1st ed.)
encryption algorithm	process which transforms plaintext into cipher text [ISO/IEC 18033-1] ■	ISO/IEC 18033-2: 2006-05-01 (1st ed.)
encryption algorithm	process which transforms a plaintext into a ciphertext [ISO/IEC 18033-1] ■	N8751: FCD 29150: 2010-06-10
encryption option	option that may be passed to the encryption algorithm of an asymmetric cipher, or of a key encapsulation mechanism, to control the formatting of the output cipher text NOTE See Clauses 7, 8.1. ■	ISO/IEC 18033-2: 2006-05-01 (1st ed.)
encryption system	cryptographic technique used to protect the confidentiality of data, and which consists of three component processes: an encryption algorithm, a decryption algorithm, and a method for generating keys. ■	ISO/IEC 18033-1: 2005-02-01 (1st ed.)

Term	Definition	ISO/IEC JTC 1/SC 27 Document
encryption system	cryptographic technique used to protect the confidentiality of data, and which consists of three component processes: an encryption algorithm, a decryption algorithm, and a method for generating keys [ISO/IEC 18033-1] ■	ISO/IEC 19772: 2009-02-15 (1st ed.)
encryption system	cryptographic technique used to protect the confidentiality of data, and which consists of three component processes: a method for generating keys, an encryption algorithm and a decryption algorithm ■	N8751: FCD 29150: 2010-06-10
energy consumption	power consumption over a certain time period NOTE In ISO/IEC 29192, energy consumption during the cryptographic process is evaluated. ■	N8753: 1st CD 29192-1: 2010-06-22
engineering group	collection of individuals (both managers and technical staff) which is responsible for project or organizational activities related to a particular engineering discipline NOTE Engineering disciplines include the following: hardware, software, software configuration management, software quality assurance, systems, system test, system security. ■	ISO/IEC 21827: 2008-10-15 (2nd ed.)
enrol	create and store an enrolment data record for a biometric capture subject in accordance with an enrolment policy NOTE Definition from [2]. ■	ISO/IEC 19792: 2009-08-01 (1st ed.)
enrol	collect one or more biometric samples from an individual, and subsequently construct one or more biometric reference templates which can then be used to verify or determine the individual's identity ■	ISO/IEC 24761: 2009-05-15 (1st ed.)
enrolment	action of enrolling or being enrolled NOTE Definition from [2]. ■	ISO/IEC 19792: 2009-08-01 (1st ed.)
enrolment	process of collecting one or more biometric samples from an individual, and the subsequent construction of a biometric reference template which can then be used to verify or determine the individual's identity ■	ISO/IEC 24761: 2009-05-15 (1st ed.)

Term	Definition	ISO/IEC JTC 1/SC 27 Document
enrolment	process to make an entity (3.1.1) to be known within a particular domain (3.2.3) NOTE 1 Enrolment involves identity registration typically preceded by identity proofing NOTE 2 In general enrolment collates and creates identity information for storage in an identity register to be used in subsequent identification of the entity in the domain. It is the start of the lifecycle of an identity in the domain for an entity. ■	N8804: 3rd CD 24760-1: 2010-06-11
enrolment data record	record created upon enrolment, associated with an individual and including biometric reference(s) and typically non-biometric data NOTE Definition from [2]. ■	ISO/IEC 19792: 2009-08-01 (1st ed.)
enrolment organization	organization which handles enrolment and creates and stores biometric reference templates ■	ISO/IEC 24761: 2009-05-15 (1st ed.)
ensure	guarantee a strong causal relationship between an action and its consequences NOTE When this term is preceded by the word “help” it indicates that the consequence is not fully certain, on the basis of that action alone. ■	ISO/IEC 15408-1: 2009-12-15 (3rd ed.)
entitlement	least privilege or "need to know" ■	N8812: 3rd WD 29146: 2010-07-14
entity	person, a group, a device or a process ■	N8776: 2nd WD 19790: 2010-07-16
entity	item of interest, inside or outside an ICT system, such as a person, an organization, a device, a subsystem, or a group of such items that has recognizably distinct existence EXAMPLE A human subscriber to a telecom service, a government agency, a network interface card, a website. ■	N8804: 3rd CD 24760-1: 2010-06-11
entity	Editors' note: *** To copy here the last definition from 24760 ** ■	N8812: 3rd WD 29146: 2010-07-14
entity	natural or legal person, a public authority or agency or any other body NOTE In the context outside the scope of this International Standard, an entity may refer to a natural person, animal, organisation, active or passive object, device or group of such items that has an identity. ■	N8806: 4th CD 29100: 2010-06-10
entity authentication	corroboration that an entity is the one claimed [ISO/IEC 9798-1:1997, definition 3.3.11] ■	ISO/IEC 9798-5: 2009-12-15 (3rd ed.)
entity authentication	corroboration that an entity is the one claimed ■	ISO/IEC 9798-1: 2010-07-01 (3rd ed.)
entity authentication	corroboration that an entity is the one claimed [ISO/IEC 9798-1:1997] ■	ISO/IEC 18014-1: 2008-09-01 (2nd ed.)
entity authentication	corroboration that an entity is the one claimed [ISO/IEC 9798-1] ■	N8762: 1st WD 20009-1: 2010-07-13
entity authentication	corroboration that an entity is the one claimed [ISO/IEC 9798-1:1997] ■	N8759: 2nd WD 29192-4: 2010-06-15

Term	Definition	ISO/IEC JTC 1/SC 27 Document
entity authentication	corroboration that an entity is the one claimed [ISO/IEC 9798-1:1997] ■	ISO/IEC FDIS 11770-1: 2010-07-26
entity authentication	corroboration that an entity is the one claimed [ISO/IEC 9798-1] ■	ISO/IEC 11770-2: 2008-06-15 (2nd ed.)
entity authentication	corroboration that an entity is the one claimed [ISO/IEC 9798-1:1997] ■	ISO/IEC 11770-3: 2008-07-15 (2nd ed.)
Entity Authentication Assurance	Confidence that the entity asserting a particular identity is in fact the entity to which the identity has been assigned. ■	N8810: 1st CD 29115 | X.eaa: 2010-06-10
entity authentication of entity *A* to entity *B*	assurance of the identity of entity *A* for entity *B* ■	ISO/IEC 11770-3: 2008-07-15 (2nd ed.)
entropy	total amount of information yielded by a set of bits, representative of the work effort required for an adversary to be able to reproduce the same set of bits [ISO/IEC 18032] ■	ISO/IEC FDIS 9797-2: 2009-09-18
entropy	Total amount of information yielded by a set of bits. It is representative of the work effort required for an adversary to be able to reproduce the same set of bits. ■	ISO/IEC 18032: 2005-01-15 (1st ed.)
entropy	measure of the disorder, randomness or variability in a closed system NOTE The entropy of a random variable *X* is a mathematical measure of the amount of information provided by an observation of *X*. ■	N8745: FCD 18031: 2010-05-18
entropy	measure of the disorder, randomness or variability in a closed system. The entropy of a random variable X is a mathematical measure of the amount of information provided by an observation of X ■	N8776: 2nd WD 19790: 2010-07-16
entropy source	component, device or event which produces outputs which, when captured and processed in some way, produces a bit string containing entropy ■	N8745: FCD 18031: 2010-05-18
entry label	the naming information that identifies a registered PP or package uniquely ■	ISO/IEC 15292: 2001-12-15 (1st ed.)
environment	environment of life cycle process execution (i.e. people, facilities and other resources) and associated environment assurance characteristics (e.g. reputation, certification) NOTE In ISO/IEC TR 15443 environment assurance contrasts with product assurance and process assurance. ■	ISO/IEC TR 15443-3: 2007-12-15 (1st ed.)
environment	business, regulatory and technological contexts inside which an application will be used, including all processes, products, information and actors involved in the application ■	N8632: FCD 27034-1: 2010-05-27
environmental failure protection - EFP	use of features to protect against a compromise of the security of a cryptographic module due to environmental conditions or fluctuations outside of the module's normal operating range ■	N8776: 2nd WD 19790: 2010-07-16

Term	Definition	ISO/IEC JTC 1/SC 27 Document
environmental failure testing - EFT	use of specific methods to provide reasonable assurance that the security of a cryptographic module will not be compromised by environmental conditions or fluctuations outside of the module's normal operating range ■	N8776: 2nd WD 19790: 2010-07-16
error	(1) a deviation of one of the software's states from correct to incorrect, or the discrepancy between the condition or value actually computed, observed, or measured by the software, and the true, specified, or theoretically correct value or condition-these are errors on the part of the software itself, during its operation; (2) A human action that results in software containing a development fault. Examples include omission or misinterpretation of user requirements in a software specification, or incorrect translation or omission of a requirement in the design specification-these are errors on the part of the developer, and to avoid confusion, the term "mistake" is preferred for this type of developer error. An error is that part of the system state which is liable to lead to subsequent failure: an error affecting the service is an indication that a failure occurs or has occurred. An error escalates into a failure when it propagates beyond the ability of the software to continue operating through (or in spite) of that error. An error is sometimes referred to as a "bug". Just as "mistake" as used to indicate an error committed by a human, an "error" can be used to indicate a mistake committed by executing software. [IEEE Std 610.12-1990, NIST SP 500-209] ■	N8732: 3rd WD 29193: 2010-08-06
error detection code EDC	value computed from data and comprised of redundant bits of information designed to detect, but not correct, unintentional changes in the data ■	N8776: 2nd WD 19790: 2010-07-16
escrow agent	authority who can identify the signer from the signed message. Note that an excrow agent may be appointed by the signer to each message the signer signs. ■	N8816: 3rd WD 29191: 2010-06-01
essential communications	Communications whose contents are necessary for the prevention of or relief from calamities, for maintaining transportation, communications or electric power supply, or for the maintenance of public order. {ITU-T format} ■	ISO/IEC 27011/x.1051: 2008-12-15 (1st ed)
evaluation	assessment of a deliverable against defined criteria NOTE 1 Definition from [1]. NOTE 2 In this context, a deliverable is a biometric system. ■	ISO/IEC 19792: 2009-08-01 (1st ed.)
evaluation	assessment of a deliverable against defined criteria (adapted from ISO/IEC 15408–1). a) Systematic examination (quality evaluation) of the extent to which an entity is capable of fulfilling specified requirements [ISO/IEC 14598-1]. ■	ISO/IEC TR 15443-1: 2005-02-01 (1st ed.)

Term	Definition	ISO/IEC JTC 1/SC 27 Document
evaluation	assessment of a PP, an ST or a TOE, against defined criteria ■	ISO/IEC 15408-1: 2009-12-15 (3rd ed.)
evaluation	assessment of a PP, an ST or a TOE, against defined criteria ■	N8784: 1st WD 20004: 2010-08-06
evaluation assurance level	set of assurance requirements drawn from ISO/IEC 15408-3, representing a point on the ISO/IEC 15408 predefined assurance scale, that form an assurance package ■	ISO/IEC 15408-1: 2009-12-15 (3rd ed.)
evaluation authority	body that sets the standards and monitors the quality of evaluations conducted by bodies within a specific community and implements ISO/IEC 15408 for that community by means of an evaluation scheme ■	ISO/IEC 15408-1: 2009-12-15 (3rd ed.)
evaluation deliverable	any resource required from the sponsor or developer by the evaluator or evaluation authority to perform one or more evaluation or evaluation oversight activities ■	N8912: Corrected 18045: 2010-09-15
evaluation evidence	tangible evaluation deliverable ■	N8912: Corrected 18045: 2010-09-15
evaluation organization	organization which evaluates biometric processing unit function or security ■	ISO/IEC 24761: 2009-05-15 (1st ed.)
evaluation pass statement	statement issued by an organisation that performs evaluations against ISO/IEC 15408 confirming that a PP has successfully passed assessment against the evaluation criteria given in clause 4 of Part 3 of that International Standard ■	ISO/IEC 15292: 2001-12-15 (1st ed.)
evaluation scheme	administrative and regulatory framework under which ISO/IEC 15408 is applied by an evaluation authority within a specific community ■	ISO/IEC 15408-1: 2009-12-15 (3rd ed.)
evaluation technical report	report that documents the overall verdict and its justification, produced by the evaluator and submitted to an evaluation authority ■	N8912: Corrected 18045: 2010-09-15
evaluator	person or party responsible for performing a security evaluation of a biometric product ■	ISO/IEC 19792: 2009-08-01 (1st ed.)
event	occurrence or change of a particular set of circumstances [ISO Guide 73:2009] ■	N8718: 1st WD 27000: 2010-05-27
event	occurrence or change of a particular set of circumstances [ISO 31000:2009] NOTE 'Information security event' means an identified occurrence of a system, service or network state indicating a possible breach of information security policy or failure of safeguards, or a previously unknown situation that may be security relevant (see ISO/IEC 27000:2009) ■	N8923: FCD 27005: 2010-06-02
evidence	information which is used, either by itself or in conjunction with other information, to establish proof about an event or action NOTE Evidence does not necessarily prove the truth or existence of something (see proof) but can contribute to the establishment of such a proof. ■	ISO/IEC 13888-1: 2009-07-15 (3rd ed)

Term	Definition	ISO/IEC JTC 1/SC 27 Document
evidence	directly measurable characteristics of a process and/or product that represent objective, demonstrable proof that a specific activity satisfies a specified requirement ■	ISO/IEC 21827: 2008-10-15 (2nd ed.)
evidence	information either by itself, or in conjunction with other information, is used to establish proof about an event or action NOTE Evidence does not necessarily prove truth or existence of something (see proof) but contributes to establish proof. [ISO/IEC 13888-1:2009] ■	N8642: 2nd PDTR 29149: 2010-06-22
evidence generator	entity that produces non-repudiation evidence [ISO/IEC 10181-4] ■	ISO/IEC 13888-1: 2009-07-15 (3rd ed)
evidence generator	entity that produces non-repudiation evidence [ISO/IEC 10181-4] ■	ISO/IEC FDIS 13888-2: 2010-08-06
evidence generator	entity that produces non-repudiation evidence [ISO/IEC 13888-1:2009] ■	N8642: 2nd PDTR 29149: 2010-06-22
evidence requester	entity requesting evidence to be generated either by another entity or by a trusted third party ■	ISO/IEC 13888-1: 2009-07-15 (3rd ed)
evidence requester	entity requesting evidence to be generated either by another entity or by a trusted third party [ISO/IEC 13888-1:2009] ■	N8642: 2nd PDTR 29149: 2010-06-22
evidence subject	entity responsible for the action, or associated with the event, with regard to which evidence is generated ■	ISO/IEC 13888-1: 2009-07-15 (3rd ed)
evidence user	entity that uses non-repudiation evidence [ISO/IEC 10181-4] ■	ISO/IEC 13888-1: 2009-07-15 (3rd ed)
evidence user	entity that uses non-repudiation evidence [ISO/IEC 13888-1:2009] ■	N8642: 2nd PDTR 29149: 2010-06-22
evidence verifier	entity that verifies non-repudiation evidence [ISO/IEC 10181-4] ■	ISO/IEC 13888-1: 2009-07-15 (3rd ed)
examine	generate a verdict by analysis using evaluator expertise NOTE The statement that uses this verb identifies what is analysed and the properties for which it is analysed. ■	N8912: Corrected 18045: 2010-09-15
exchange multiplicity parameter	number of exchanges of information involved in one instance of an authentication mechanism ■	ISO/IEC 9798-5: 2009-12-15 (3rd ed.)
exchange multiplicity parameter	number of exchanges of information involved in one instance of an authentication mechanism ■	N8759: 2nd WD 29192-4: 2010-06-15
executable form	form of the code in which the software or firmware is managed and controlled completely by the operational environment of the module and does not require compilation (e.g. no source code, object code or just-in-time compiled code) ■	N8776: 2nd WD 19790: 2010-07-16

Term	Definition	ISO/IEC JTC 1/SC 27 Document
exhaustive	characteristic of a methodical approach taken to perform an analysis or activity according to an unambiguous plan NOTE This term is used in ISO/IEC 15408 with respect to conducting an analysis or other activity. It is related to "systematic" but is considerably stronger, in that it indicates not only that a methodical approach has been taken to perform the analysis or activity according to an unambiguous plan, but that the plan that was followed is sufficient to ensure that all possible avenues have been exercised. ■	ISO/IEC 15408-1: 2009-12-15 (3rd ed.)
explain	give argument accounting for the reason for taking a course of action NOTE This term differs from both "describe" and "demonstrate". It is intended to answer the question "Why?" without actually attempting to argue that the course of action that was taken was necessarily optimal. ■	ISO/IEC 15408-1: 2009-12-15 (3rd ed.)
explicit key authentication from *A* to *B*	assurance for entity *B* that *A* is the only other entity that is in possession of the correct key NOTE - Implicit key authentication from *A* to *B* and key confirmation from *A* to *B* together imply explicit key authentication from *A* to *B*. [ISO/IEC 11770-3:1999] ■	ISO/IEC 11770-4: 2006-05-01 (1st ed.)
explicit key authentication from entity *A* to entity *B*	assurance for entity *B* that entity *A* is the only other entity that is in possession of the correct key [ISO/IEC 11770-3] NOTE Implicit key authentication from *A* to *B* and key confirmation from *A* to *B* together imply explicit key authentication from *A* to *B*. ■	ISO/IEC 11770-2: 2008-06-15 (2nd ed.)
explicit key authentication from entity *A* to entity *B*	assurance for entity *B* that entity *A* is the only other entity that is in possession of the correct key NOTE Implicit key authentication from entity *A* to entity *B* and key confirmation from entity *A* to entity *B* together imply explicit key authentication from entity *A* to entity *B*. ■	ISO/IEC 11770-3: 2008-07-15 (2nd ed.)
explicitly given finite field	set of all *e*-tuples over [0, *p* – 1], where p is prime and *e* ≥ 1, along with a "multiplication table" NOTE 1 For a mathematical definition of an explicitly given finite field, see Clause A.3. NOTE 2 For more detailed information on finite fields, see ISO/IEC 15946-1:2002. ■	ISO/IEC 9796-3: 2006-09-15 (2nd ed.)
explicitly given finite field	finite field that is represented explicitly in terms of its characteristic and a multiplication table for a basis of the field over the underlying prime field NOTE See Clause 5.3. ■	ISO/IEC 18033-2: 2006-05-01 (1st ed.)
exploit	defined way to breach the security of an Information System through vulnerability ■	ISO/IEC 18043: 2006-06-15 (1st ed.)

Term	Definition	ISO/IEC JTC 1/SC 27 Document
exploitable vulnerability	weakness in the TOE that can be used to violate the SFRs in the operational environment for the TOE ■	ISO/IEC 15408-1: 2009-12-15 (3rd ed.)
exploitable vulnerability	weakness in the TOE that can be used to violate the SFRs in the operational environment for the TOE ■	N8784: 1st WD 20004: 2010-08-06
exploit; exploited	An exploit is the use of a vulnerability discovered on system, to fire an attack on the system. to A zero-day exploit is one that takes advantage of a security vulnerability on the same day that the vulnerability becomes known, generally by official publication of the editor of the system ; To be completed ■	N8732: 3rd WD 29193: 2010-08-06
Extensible Authentication Protocol - EAP	an authentication protocol supported by RADIUS and standardised by the IETF in RFC 2284. ■	ISO/IEC 18028-4: 2005-04-01 (1st ed.)
extension	addition to an ST or PP of functional requirements not contained in ISO/IEC 15408-2 and/or assurance requirements not contained in ISO/IEC 15408-3 ■	ISO/IEC 15408-1: 2009-12-15 (3rd ed.)
external context	external environment in which the organization seeks to achieve its objectives NOTE External context can include: - the cultural, social, political, legal, regulatory, financial, technological, economic, natural and competitive environment, whether international, national, regional or local; - key drivers and trends having impact on the objectives of the organization; and - relationships with, and perceptions and values of, external stakeholders. [ISO 31000:2009] ■	N8923: FCD 27005: 2010-06-02
external entity	human or IT entity possibly interacting with the TOE from outside of the TOE boundary NOTE An external entity can also be referred to as a user. ■	ISO/IEC 15408-1: 2009-12-15 (3rd ed.)
external operational system	separate operational system which interfaces to the operational system that is the subject of evaluation ■	ISO/IEC TR 19791: 2010-04-01 (2nd ed.)
extranet	extension of an organization's Intranet, especially over the public network infrastructure, enabling resource sharing between the organization and other organizations and individuals that it deals with by providing limited access to its Intranet NOTE For example, an organization's customers can be provided access to some part of its Intranet, creating an extranet, but the customers cannot be considered "trusted" from a security standpoint. ■	ISO/IEC 27033-1: 2009-12-15 (1st ed.)

Term	Definition	ISO/IEC JTC 1/SC 27 Document
failure	Termination of the ability of a functional unit to perform a required function [61508-4] The inability of a system or component to perform, or the non-performance by the system or component, of an intended function or service; or (2) a deviation of a function or service from its specified, expected performance, resulting in its incorrect performance. Failures fall into two general categories: - Value failures: the functionality or service no fulfills its specified/expected purpose, i.e., it no longer delivers its specified/expected value; - Timing failures: the timing of the functionality or service no longer falls within its specified/expected temporal constraints. ■	N8732: 3rd WD 29193: 2010-08-06
failure mode	manner by which a failure is observed; it generally describes the way the failure occurs and its impact on the operation of the system ■	N8622: PreFDIS 27031: 2010-08-18
failure-to-enrol rate - FTE	proportion of the population for whom the system fails to complete the enrolment process NOTE The observed failure-to-enrol rate is measured on test crew enrolments. The predicted/expected failure-toenrol- rate will apply to the entire target population. ■	ISO/IEC 19792: 2009-08-01 (1st ed.)
false accept rate - FAR	proportion of verification transactions with wrongful claims of identity that are incorrectly confirmed ■	ISO/IEC 19792: 2009-08-01 (1st ed.)
false match rate - FMR	proportion of zero-effort impostor attempt samples falsely declared to match the compared non-self template NOTE The measured/observed false match rate is distinct from the predicted/expected false match rate (the former may be used to estimate the latter). ■	ISO/IEC 19792: 2009-08-01 (1st ed.)
false negative	no IDS alert when there is an attack ■	ISO/IEC 18043: 2006-06-15 (1st ed.)
false non-match rate - FNMR	proportion of genuine attempt samples falsely declared not to match the template of the same characteristic from the same user supplying the sample NOTE The measured/observed false non-match rate is distinct from the predicted/expected false non-match rate (the former may be used to estimate the latter). ■	ISO/IEC 19792: 2009-08-01 (1st ed.)
false positive	IDS alert when there is no attack ■	ISO/IEC 18043: 2006-06-15 (1st ed.)
false reject rate - FRR	proportion of verification transactions with truthful claims of identity that are incorrectly denied ■	ISO/IEC 19792: 2009-08-01 (1st ed.)
family	set of components that share a similar goal but differ in emphasis or rigour ■	ISO/IEC 15408-1: 2009-12-15 (3rd ed.)

Term	Definition	ISO/IEC JTC 1/SC 27 Document
fault	Abnormal condition that may cause in reduction, or loss, of the capability of the functional unit to perform a required function [61508-4] The adjudged or hypothesized cause of an error. A fault is considered active when it causes an error orfailure; otherwise it is considered dormant. Some dormant faults never become active. In common usage, "bug" or "error" are used to express the same meaning. Software faults include incorrect steps, processes, and data definitions in computer programs. Faults fall into three basic categories: 1. Development faults: introduced into the software during some stage of its development; developmental faults include incorrect steps, processes, and data definitions that cause the software to perform in an unintended or unanticipated manner; 2. Physical faults: originate from defects in the hardware on which the software runs (hardware faults include such defects as short circuits or broken wires); 3. External faults: originate in the interactions between the software and external entities (users, other software). ■	N8732: 3rd WD 29193: 2010-08-06
federated identity	identity (3.1.2) with attributes (3.1.3) for use in multiple domains (3.2.3), which together form an identity federation (3.5.2) NOTE 1 A federated identity may be jointly managed by identity information providers of the federated domains. NOTE 2 The shared attributes used in the federated domains may in particular be used for identification, e.g. to support single sign-on (SSO). NOTE 3 The federated identity may persist or may be a temporary one e.g. as single-sign-on identity. ■	N8804: 3rd CD 24760-1: 2010-06-11
feedback buffer (*FB*)	variable used to store input data for the encryption process. At the starting point *FB* has the value of *SV*. ■	ISO/IEC 10116: 2006-02-01 (3rd ed.)
field	mathematical notion of a field, i.e., a set of elements, together with binary operations for addition and multiplication on this set, such that the usual field axioms apply ■	ISO/IEC 18033-2: 2006-05-01 (1st ed.)
File Transfer Protocol - FTP	an internet standard (RFC 959) for transferring files between a client and a server. ■	ISO/IEC 18028-4: 2005-04-01 (1st ed.)
filtering	process of accepting or rejecting data flows through a network, according to specified criteria ■	ISO/IEC 27033-1: 2009-12-15 (1st ed.)
finder	individual or organization that finds a potential vulnerability in a product or online service NOTE Subgroups include researchers, security companies, users, governments, and coordinators. ■	N8780: 1st CD 29147: 2010-06-10
finite abelian group	group such that the underlying set of elements is finite, and such that the underlying binary operation is commutative ■	ISO/IEC 18033-2: 2006-05-01 (1st ed.)

Term	Definition	ISO/IEC JTC 1/SC 27 Document
finite commutative group	finite set E with the binary operation "*" such that - for all $a, b, c \in E$, $(a * b) * c = a * (b * c)$; - there exists $e \in E$ with $e * a = a$ for all $a \in E$; - for all $a \in E$ there exists $b \in E$ with $b * a = e$; - for all $a, b \in E$, $a * b = b * a$. NOTE 1 - If $a^0 = e$, and $a^{n+1} = a * a^n$ (for $n \geq 0$) is defined recursively, the order of $a \in E$ is the least positive integer n such that $a^n = e$. NOTE 2 - In some cases, such as when E is the set of points on an elliptic curve, arithmetic in the finite set E is described with additive notation. ■	ISO/IEC 14888-3: 2006-11-15 (2nd ed.)
finite field	field such that the underlying set of elements is finite ■	ISO/IEC 18033-2: 2006-05-01 (1st ed.)
finite field	field containing a finite number of elements NOTE 1 A definition of field is given in [29]. NOTE 2 For any positive integer m and a prime p, there exists a finite field containing exactly p^m elements. This field is unique up to isomorphism and is denoted by $F(p^m)$, where p is called the characteristic of $F(p^m)$. [ISO/IEC 15946-1:2008] ■	ISO/IEC 15946-5: 2009-12-15 (1st ed.)
finite field	cryptographic bilinear map e_n satisfying the non-degeneracy, bilinearity, and computability ■	ISO/IEC 15946-1: 2008-04-15 (2nd ed.)
finite state model - FSM	a mathematical model of a sequential machine that is comprised of a finite set of input events, a finite set of output events, a finite set of states, a function that maps states and input to output, a function that maps states and inputs to states (a state transition function), and a specification that describes the initial state ■	N8776: 2nd WD 19790: 2010-07-16
firewall	type of security gateway or barrier placed between network environments - consisting of a dedicated device or a composite of several components and techniques - through which all traffic from one network environment to another, and vice versa, traverses and only authorized traffic is allowed to pass [ISO/IEC 18028-1] ■	ISO/IEC 18043: 2006-06-15 (1st ed.)
firewall	type of security barrier placed between network environments -- consisting of a dedicated device or a composite of several components and techniques -- through which all traffic from one network environment traverses to another, and vice versa, and only authorized traffic, as defined by the local security policy, is allowed to pass ■	ISO/IEC 27033-1: 2009-12-15 (1st ed.)

Term	Definition	ISO/IEC JTC 1/SC 27 Document
firmware	programs and data components of a cryptographic module that are stored in hardware within the cryptographic boundary and cannot be dynamically written or modified during execution [ISO/IEC 19790:2006, 3.31] EXAMPLE Storage hardware may include but is not limited to ROM, PROM, EEPROM, or FLASH. ■	ISO/IEC 24759: 2008-07-01 (1st ed.)
firmware	executable code of a cryptographic module that is stored in hardware within the cryptographic boundary and cannot be dynamically written or modified during execution while operating in a non-modifiable or limited operational environment EXAMPLE Storage hardware may include but not limited to PROM, EEPROM, FLASH, solid state memory, hard drives, etc ■	N8776: 2nd WD 19790: 2010-07-16
firmware module	module that is composed solely of firmware ■	N8776: 2nd WD 19790: 2010-07-16
formal	expressed in a restricted syntax language with defined semantics based on well-established mathematical concepts ■	ISO/IEC 15408-1: 2009-12-15 (3rd ed.)
formal description	description whose syntax and semantics are defined on the basis of well-established mathematical concepts ■	N8778: 3rd CD 29128: 2010-06-11
formal language	language for modelling, calculation, and predication in the specification, design, analysis, construction, and assurance of hardware and software systems whose syntax and semantics are defined on the basis of well-established mathematical concepts ■	N8778: 3rd CD 29128: 2010-06-11
formal methods	techniques based on well-established mathematical concepts for modelling, calculation, and predication in the specification, design, analysis, construction, and assurance of hardware and software systems ■	N8778: 3rd CD 29128: 2010-06-11
forward secrecy	assurance that subsequent (future) values cannot be determined from current or previous values ■	N8745: FCD 18031: 2010-05-18
forward secrecy with respect to both entity *A* and entity *B* individually	property that knowledge of entity *A*'s long-term private key subsequent to a key agreement operation does not enable an opponent to recompute previously derived keys ■	ISO/IEC 11770-3: 2008-07-15 (2nd ed.)
forward secrecy with respect to entity *A*	property that knowledge of entity *A*'s long-term private key or knowledge of entity *B*'s long-term private key subsequent to a key agreement operation does not enable an opponent to recompute previously derived keys NOTE This differs from mutual forward secrecy in which knowledge of both entity *A*'s and entity *B*'s long-term private keys do not enable recomputation of previously derived keys. ■	ISO/IEC 11770-3: 2008-07-15 (2nd ed.)

Term	Definition	ISO/IEC JTC 1/SC 27 Document
forward security with interval T	security condition in which an entity leaving at time $t = t_0$ cannot obtain any subsequent *shared secret keys* at time $t > t_0 + T$ ■	N8743: 2nd CD 11770-5: 2010-07-29
full domain cryptographic hash function	function that maps strings of bits to integers in a fixed range, satisfying the properties of (1) for a given output, it is computationally infeasible to find an input which maps to this output, and (2) for a given input, it is computationally infeasible to find a second input which maps to the same output NOTE A full domain cryptographic hash function is similar to a standard cryptographic hash function with the exception that the former outputs an integer rather than a bit string; see 7.2.2. ■	N8751: FCD 29150: 2010-06-10
functional cohesion	functional property of a module which performs activities related to a single purpose [IEEE Std 610.12-1990] NOTE A functionally cohesive module transforms a single type of input into a single type of output, such as a stack manager or a queue manager. See also cohesion (3.2.3). ■	ISO/IEC 15408-1: 2009-12-15 (3rd ed.)
functional interface	external interface providing a user with access to functionality of the TOE which is not directly involved in enforcing security functional requirements NOTE In a composed TOE these are the interfaces provided by the base component that are required by the dependent component to support the operation of the composed TOE. ■	ISO/IEC 15408-1: 2009-12-15 (3rd ed.)
Functional Role	functional roles reflect the essential business functions that need to be performed. Functional roles are defined by a set of standard tasks [Neumann/Strembeck] ■	N8812: 3rd WD 29146: 2010-07-14
functional specification	high-level description of the ports and interfaces visible to the operator and a high-level description of the behaviour of the cryptographic module ■	N8776: 2nd WD 19790: 2010-07-16
functional testing	testing of the cryptographic module functionality as defined by the functional specification ■	N8776: 2nd WD 19790: 2010-07-16
gate equivalent	unit of measure which allows to specify manufacturing-technology-independent complexity of digital electronic circuits, commonly the silicon area of a two-input drive-strength-one NAND gate NOTE In order to get the gate equivalent for the different gates, one divides the area of the particular gate by the area of the two-input NAND gate in the appropriate technology. ■	N8753: 1st CD 29192-1: 2010-06-22
Generic SIO Class	SIO Class in which the data types for one or more of the components are not fully specified. ■	ISO/IEC 15816: 2002-02-01 (1st ed.)

Term	Definition	ISO/IEC JTC 1/SC 27 Document
glass box	idealized mechanism that accepts inputs and produces outputs and is designed such that an observer can see inside and determine exactly what is going on NOTE This term can be contrasted to black box. ■	N8745: FCD 18031: 2010-05-18
group	mathematical notion of a group, i.e., a set of elements, together with a binary operation on this set, such that the usual group axioms apply ■	ISO/IEC 18033-2: 2006-05-01 (1st ed.)
group	set of entities operating under a single membership management policy EXAMPLE - Each member has a membership credential which is created by a group issuing authority in the group issuing process. ■	N8760: 1st WD 20008-1: 2010-06-14
group	set of entities operating under a single membership management policy EXAMPLE Each member has a membership credential which is created by a single authority or by a set of authorities using the same membership management policy. ■	N8763: 1st WD 20009-2: 2010-06-20
group issuing authority	entity who is able to create group membership credentials ■	N8760: 1st WD 20008-1: 2010-06-14
group issuing authority	entity who is able to create group membership credentials ■	N8763: 1st WD 20009-2: 2010-06-20
group issuing key	set of private data elements specific to a group issuing authority and usable only by this entity in the group issuing process ■	N8760: 1st WD 20008-1: 2010-06-14
group issuing process	process which takes as inputs the group member signature key, the group issuing key and the group public parameters, and which gives as output the group membership credential ■	N8760: 1st WD 20008-1: 2010-06-14
group member	entity who has a group membership credential and can create a group signature on the behalf of the group ■	N8760: 1st WD 20008-1: 2010-06-14
group member	entity who has a group membership credential and can create a group signature on the behalf of the group ■	N8763: 1st WD 20009-2: 2010-06-20
group member signature key	set of private data elements specific to a group member and usable only by this entity in the group issuing process and the group signature process ■	N8760: 1st WD 20008-1: 2010-06-14
group membership credential	data element which is specific to the group member and is rendered unforgeable with the private key of a group issuing authority, and which is usable by the group member in the group signature process ■	N8760: 1st WD 20008-1: 2010-06-14
group membership credential	data element which is specific to the group member and is rendered unforgeable with the private key of a group issuing authority ■	N8763: 1st WD 20009-2: 2010-06-20
group public parameter	data element which is accessible to all entities within the group or involved in the group signature verification process ■	N8760: 1st WD 20008-1: 2010-06-14

Term	Definition	ISO/IEC JTC 1/SC 27 Document
group public parameter	data element which is accessible to all entities within the group or involved in the group signature verification process ■	N8763: 1st WD 20009-2: 2010-06-20
group signature	data element resulting from the group signature process NOTE Part 2 of ISO/IEC 20008 specifies a number of types of group signatures, some of them with the tracing process and some of them with the linking process. ■	N8760: 1st WD 20008-1: 2010-06-14
group signature	data element resulting from the group signature process ■	N8763: 1st WD 20009-2: 2010-06-20
group signature process	process which takes as inputs the message, the group member signature key, the group membership credential and the group public parameters, and which gives as output the signature ■	N8760: 1st WD 20008-1: 2010-06-14
group signature process	process which takes as inputs the message, the group member private key, the group membership credential and the group public parameters, and which gives as output the signature ■	N8763: 1st WD 20009-2: 2010-06-20
group signature verification process	process which takes as inputs the signed message, the group verification key and the group public parameters, and which gives as output the result of the group signature verification: valid or invalid ■	N8760: 1st WD 20008-1: 2010-06-14
group signature verification process	process which takes as inputs the signed message, the group verification key and the group public parameters, and which gives as output the result of the group signature verification: valid or invalid ■	N8763: 1st WD 20009-2: 2010-06-20
group tracing authority	entity who enables to trace a group signature to its signer's identifier ■	N8760: 1st WD 20008-1: 2010-06-14
group tracing authority	entity who enables to trace a group signature to its signer ■	N8763: 1st WD 20009-2: 2010-06-20
group tracing key	set of private data elements specific to a group tracing authority and usable only by this entity in the group tracing process ■	N8760: 1st WD 20008-1: 2010-06-14
group tracing process	process which takes as inputs the group signature, the group tracing key and the group public parameters, and which gives as output the signer identifier ■	N8760: 1st WD 20008-1: 2010-06-14
group verification key	data element which is mathematically related to a group authority's private key and which is used by the verifier in the group verification process ■	N8760: 1st WD 20008-1: 2010-06-14
group verification key	data element which is mathematically related to a group authority's private key and which is used by the verifier in the group verification process ■	N8763: 1st WD 20009-2: 2010-06-20
guarantee	Refer to the definition for warranty ISO/IEC TR 15443-1: 2004 ■	ISO/IEC TR 15443-1: 2005-02-01 (1st ed.)
guidance documentation	documentation that describes the delivery, preparation, operation, management and/or use of the TOE ■	ISO/IEC 15408-1: 2009-12-15 (3rd ed.)
guideline	recommendation of what is expected to be done to achieve an objective ■	N8718: 1st WD 27000: 2010-05-27

Term	Definition	ISO/IEC JTC 1/SC 27 Document
hacking	accessing a computer system without the authorization of the user or the owner ■	N8624: 2nd CD 27032: 2010-06-15
hactivism	hacking for a politically or socially motivated purpose ■	N8624: 2nd CD 27032: 2010-06-15
half-block	a string of bits of length $L_\Phi/2$ EXAMPLE Half the length of the block H_j. ■	ISO/IEC 10118-4: 1998-12-15 (1st ed.)
hard / hardness	the relative resistance of a metal or other material to denting, scratching, or bending; physically toughened; rugged, and durable. The relative resistances of the material to be penetrated by another object ■	N8776: 2nd WD 19790: 2010-07-16
hardware	the physical equipment/components within the cryptographic boundary used to process programs and data ■	N8776: 2nd WD 19790: 2010-07-16
Hardware Cryptographic Credential: A credential that is comprised of a hardware device that contains	a protected cryptographic key. NOTE - It is also referred to as a hard credential or hard cryptographic credential. ■	N8810: 1st CD 29115 | X.eaa: 2010-06-10
hardware module	a module composed primarily of hardware, which may also contain firmware ■	N8776: 2nd WD 19790: 2010-07-16
hardware module interface HMI	the total set of commands used to request the services of the hardware module, including parameters that enter or leave the module's cryptographic boundary as part of the requested service ■	N8776: 2nd WD 19790: 2010-07-16
hash value	function which maps strings of bits to fixed-length strings of bits, satisfying the following two properties: - it is computationally infeasible to find for a given output, an input which maps to this output; - it is computationally infeasible to find for a given input, a second input which maps to the same output NOTE Computational feasibility depends on the specific security requirements and environment. [ISO/IEC 10118-1:2000] ■	ISO/IEC 18014-1: 2008-09-01 (2nd ed.)
hash value	string of bits which is the output of a hash-function NOTE See ISO/IEC 10118-1:2000, 3.4. ■	ISO/IEC 18014-3: 2009-12-15 (2nd ed.)
hash value	the output of a cryptographic hash function ■	N8776: 2nd WD 19790: 2010-07-16
hash value	string of bits which is the output of a hash-function [ISO/IEC 10118-1: 2000] ■	N8640: 3rd WD 27037: 2010-05-31
hash-code	the string of bits which is the output of a hash-function NOTE – The literature on this subject contains a variety of terms that have the same or similar meaning as hash-code. Modification Detection Code, Manipulation Detection Code, digest, hash-result, hash-value and imprint are some examples. ■	ISO/IEC 10118-1: 2000-06-15 (2nd ed.)
hash-code	string of bits that is the output of a hash-function [ISO/IEC 10118-1] ■	ISO/IEC 13888-1: 2009-07-15 (3rd ed)

Term	Definition	ISO/IEC JTC 1/SC 27 Document
hash-code	string of octets which is the output of a hash-function NOTE Adapted from ISO/IEC 10118-1:2000. ■	ISO/IEC 9796-3: 2006-09-15 (2nd ed.)
hash-code	string of bits which is the input to a hash-function ■	ISO/IEC FDIS 9797-2: 2009-09-18
hash-code	string of bits which is the output of a hash-function [ISO/IEC 10118-1] ■	ISO/IEC FDIS 9796-2: 2010-09-10
hash-code	string of bits which is the output of a hash-function NOTE The literature on this subject contains a variety of terms that have the same or similar meaning as hash-code. Modification Detection Code, Manipulation Detection Code, digest, hash-result, hash-value and imprint are some examples. [ISO/IEC 10118-1] ■	N8760: 1st WD 20008-1: 2010-06-14
hash-code	string of bits which is the output of a hash-function NOTE The literature on this subject contains a variety of terms that have the same or similar meaning as hash-code. Modification Detection Code, Manipulation Detection Code, digest, hash-result, hash-value and imprint are some examples. [ISO/IEC 10118-1] ■	N8763: 1st WD 20009-2: 2010-06-20
hash-code	string of bits which is the output of a hash-function [ISO/IEC 10118-1] ■	ISO/IEC 14888-1: 2008-04-15 (2nd ed.)
hashed password	function which maps strings of bits to fixed-length strings of bits, satisfying the following two properties. - It is computationally infeasible to find for a given output, an input which maps to this output. - It is computationally infeasible to find for a given input, a second input which maps to the same output. NOTE - Computational feasibility depends on the specific security requirements and environment. [ISO/IEC 10118-1:2000] ■	ISO/IEC 11770-4: 2006-05-01 (1st ed.)
hash-function	a function which maps strings of bits to fixed-length strings of bits, satisfying the following two properties: -- it is computationally infeasible to find for a given output, an input which maps to this output; -- it is computationally infeasible to find for a given input, a second input which maps to the same output NOTE – Computational feasibility depends on the specific security requirements and environment. ■	ISO/IEC 10118-1: 2000-06-15 (2nd ed.)
hash-function	function which maps strings of bits to fixed-length strings of bits, satisfying the following two properties: - it is computationally infeasible to find for a given output an input which maps to this output; - it is computationally infeasible to find for a given input a second input which maps to the same output [ISO/IEC 10118-1] ■	ISO/IEC 13888-1: 2009-07-15 (3rd ed)

Term	Definition	ISO/IEC JTC 1/SC 27 Document
hash-function	function which maps strings of octets to fixed-length strings of octets, satisfying the following two properties: -- for a given output, it is computationally infeasible to find an input which maps to this output; -- for a given input, it is computationally infeasible to find a second input which maps to the same output. NOTE 1 Adapted from ISO/IEC 10118-1:2000. NOTE 2 Computational feasibility depends on the specific security requirements and environment. NOTE 3 For the purposes of this part of ISO/IEC 9796, the allowable hash-functions are those described in ISO/IEC 10118-2 and ISO/IEC 10118-3, with the following proviso: -- The hash-functions described in ISO/IEC 10118 map bit strings to bit strings, whereas in this part of ISO/IEC 9796, they map octet strings to octet strings. Therefore, a hash-function in ISO/IEC 10118-2 or ISO/IEC 10118-3 is allowed in this part of ISO/IEC 9796 only if the length in bits of the output is a multiple of 8, in which case the mapping between octet strings and bit strings is affected by the functions OS2BSP and BS2OSP. ■	ISO/IEC 9796-3: 2006-09-15 (2nd ed.)
hash-function	string of bits which is the output of a hash-function [ISO/IEC 10118-1] ■	ISO/IEC FDIS 9797-2: 2009-09-18
hash-function	function that maps strings of bits to fixed-length strings of bits, satisfying the following two properties: - for a given output, it is computationally infeasible to find an input that maps to this output; - it is computationally infeasible to find two distinct inputs that map to the same output [ISO/IEC 10118-1:2000, definition 3.5] ■	ISO/IEC 9798-5: 2009-12-15 (3rd ed.)
hash-function	function which maps strings of bits to fixed-length strings of bits, satisfying the following two properties: - for a given output, it is computationally infeasible to find an input which maps to this output; - for a given input, it is computationally infeasible to find a second input which maps to the same output [ISO/IEC 9797-2] ■	ISO/IEC FDIS 9796-2: 2010-09-10
hash-function	function which maps strings of bits to fixed-length strings of bits, satisfying the following two properties: - it is computationally infeasible to find for a given output an input which maps to this output; - it is computationally infeasible to find for a given input a second input which maps to the same output. [ISO/IEC 10118-1] ■	ISO/IEC FDIS 9798-6: 2010-08-05

Term	Definition	ISO/IEC JTC 1/SC 27 Document
hash-function	function which maps strings of bits to fixed-length strings of bits, satisfying the following two properties: - it is computationally infeasible to find for a given output an input which maps to this output; - it is computationally infeasible to find for a given input a second input which maps to the same output [ISO/IEC 10118-1] ■	ISO/IEC FDIS 13888-2: 2010-08-06
hash-function	result of applying a hash-function to a password ■	ISO/IEC 11770-4: 2006-05-01 (1st ed.)
hash-function	string of bits which is the output of a hash-function NOTE Identical to the definition of hash-code in ISO/IEC 10118-1:2000. ■	ISO/IEC 18014-1: 2008-09-01 (2nd ed.)
hash-function	function which maps strings of bits to fixed-length strings of bits, satisfying the following two properties: - for a given output, it is computationally infeasible to find an input which maps to this output; - for a given input, it is computationally infeasible to find a second input which maps to the same output. [ISO/IEC 10118-1] NOTE 1 Computational feasibility depends on the specific security requirements and environment. NOTE 2 For the purposes of this document, the recommended hash-functions are those defined in ISO/IEC 10118-2 and ISO/IEC 10118-3. ■	ISO/IEC 15946-5: 2009-12-15 (1st ed.)
hash-function	function which maps strings of bits to fixed-length strings of bits, satisfying the following two properties: - it is computationally infeasible to find for a given output, an input which maps to this output - it is computationally infeasible to find for a given input, a second input which maps to the same output NOTE Computational feasibility depends on the specific security requirements and environment. [ISO/IEC 10118-1:2000, definition 3.5] ■	ISO/IEC 18014-2: 2009-12-15 (2nd ed.)
hash-function	function which maps strings of bits to fixed-length strings of bits, satisfying the following two properties: it is computationally infeasible to find for a given output, an input which maps to this output; it is computationally infeasible to find for a given input, a second input which maps to the same output [ISO/IEC 10118-1:2000, definition 3.5] ■	ISO/IEC 18014-3: 2009-12-15 (2nd ed.)

Term	Definition	ISO/IEC JTC 1/SC 27 Document
hash-function	function which maps strings of bits to fixed-length strings of bits, satisfying the following two properties: - for a given output, it is computationally infeasible to find an input which maps to this output; - for a given input, it is computationally infeasible to find a second input which maps to the same output NOTE Computational feasibility depends on the specific security requirements and environment. [ISO/IEC 10118-1] ■	N8760: 1st WD 20008-1: 2010-06-14
hash-function	function which maps strings of bits to fixed-length strings of bits, satisfying the following two properties: - for a given output, it is computationally infeasible to find an input which maps to this output; - for a given input, it is computationally infeasible to find a second input which maps to the same output NOTE Computational feasibility depends on the specific security requirements and environment. [ISO/IEC 10118-1] ■	N8763: 1st WD 20009-2: 2010-06-20
hash-function	function that maps strings of bits to fixed-length strings of bits, satisfying the following two properties: - for a given output, it is computationally infeasible to find an input that maps to this output; - it is computationally infeasible to find two distinct inputs that map to the same output [ISO/IEC 10118-1:2000] ■	N8759: 2nd WD 29192-4: 2010-06-15
hash-function	function, which maps strings of bits to fixed-length, strings of bits, satisfying the following two properties. - It is computationally infeasible to find for a given output, an input that maps to this output. - It is computationally infeasible to find for a given input, a second input, which maps to the same output. NOTE Computational feasibility depends on the specific security requirements and environment. [ISO/IEC 10118-1] ■	N8745: FCD 18031: 2010-05-18
hash-function	function which maps strings of bits to fixed-length strings of bits, satisfying the following two properties: - It is computationally infeasible to find for a given output, an input which maps to this output. - It is computationally infeasible to find for a given input, a second input which maps to the same output. NOTE Computational feasibility depends on the specific security requirements and environment. [ISO/IEC 10118-1:2000] ■	N8642: 2nd PDTR 29149: 2010-06-22

Term	Definition	ISO/IEC JTC 1/SC 27 Document
hash-function	function which maps strings of bits to fixed-length strings of bits, satisfying the following two properties: - it is computationally infeasible to find for a given output, an input which maps to this output - it is computationally infeasible to find for a given input, a second input which maps to the same output NOTE Computational feasibility depends on the specific security requirements and environment. [ISO/IEC 10118-1:2000] ■	N8640: 3rd WD 27037: 2010-05-31
hash-function	function which maps strings of bits to fixed-length strings of bits, satisfying the following two properties: - for a given output, it is computationally infeasible to find an input which maps to this output; - for a given input, it is computationally infeasible to find a second input which maps to the same output NOTE 1 Computational feasibility depends on the specific security requirements and environment. NOTE 2 This definition of hash-function is referred to as one-way hash-function. [ISO/IEC 10118-1] ■	ISO/IEC 14888-1: 2008-04-15 (2nd ed.)
hash-function	function which maps strings of bits to fixed-length strings of bits, satisfying two properties: 1) it is computationally infeasible to find for a given output, an input which maps to this output; 2) it is computationally infeasible to find for a given input, a second input which maps to the same output NOTE 1 The literature on this subject contains a variety of terms which have the same or similar meaning as hashfunction. Compressed encoding and condensing function are some examples. NOTE 2 Computational feasibility depends on the user's specific security requirements and environment. ■	ISO/IEC 11770-3: 2008-07-15 (2nd ed.)
hash-function identifier	byte identifying a specific hash-function ■	ISO/IEC 10118-1: 2000-06-15 (2nd ed.)
hash-function identifier	byte identifying a specific hash-function ■	ISO/IEC 10118-4: 1998-12-15 (1st ed.)
hash-function identifier	Identifiers are defined for each of the two MASH hash-functions specified in this standard. The hash-function identifiers for the hash-functions specified in clause 8.1 and 8.2 are equal to 41 and 42 (hexadecimal) respectively. The range of values from 43 to 4f (hexadecimal) are reserved for future use as hash-function identifiers by this part of ISO/IEC 10118. ■	ISO/IEC 10118-4: 1998-12-15 (1st ed.)

Term	Definition	ISO/IEC JTC 1/SC 27 Document
hash-token	concatenation of a hash-code and an optional control field which can be used to identify the hash-function and the padding method [ISO/IEC 14888-1:1998] NOTE The control field with the hash-function identifier is mandatory unless the hash-function is uniquely determined by the signature mechanism or by the domain parameters. ■	ISO/IEC 9796-3: 2006-09-15 (2nd ed.)
hash-value	string of bits which is the output of a hash-function NOTE Adapted from hash-code as defined in ISO/IEC 10118-1. ■	ISO/IEC 18014-2: 2009-12-15 (2nd ed.)
hash-value	string of bits which is the output of a hash-function [ISO/IEC 10118-1: 2000] ■	N8642: 2nd PDTR 29149: 2010-06-22
honeypot	generic term for a decoy system used to deceive, distract, divert and to encourage the attacker to spend time on information that appears to be very valuable, but actually is fabricated and would not be of interest to a legitimate user ■	ISO/IEC 18043: 2006-06-15 (1st ed.)
host	addressable system or computer in TCP/IP based networks like the Internet ■	ISO/IEC 18043: 2006-06-15 (1st ed.)
host protected area HPA	an area of a storage media that is normally not visible to the machine's operating system ■	N8640: 3rd WD 27037: 2010-05-31
hub	network device that functions at layer 1 of the OSI reference model NOTE There is no real intelligence in network hubs; they only provide physical attachment points for networked systems or resources. ■	ISO/IEC 27033-1: 2009-12-15 (1st ed.)
human behaviour	understanding of interactions among humans and other elements of a system with the intent to ensure well being and systems performance NOTE 1 Human behaviour includes culture, needs and aspirations of people as individuals and as groups. NOTE 2 In respect of information technology (IT), there are numerous groups or communities of humans, each with their own needs, aspirations and behaviours. For example, people who use information systems might exhibit needs relating to accessibility and ergonomics, as well as availability and performance. People whose job roles are changing because of the use of IT might exhibit needs relating to communication, training, and reassurance. People involved in building and operating IT capabilities might exhibit needs relating to working conditions and development of skills. [ISO/IEC 38500:2008] ■	N8712: 3rd WD 27014: 2010-05-28
human entropy source	entropy source that has some kind of random human component ■	N8745: FCD 18031: 2010-05-18
hybrid cipher	asymmetric cipher that combines both asymmetric and symmetric cryptographic techniques ■	ISO/IEC 18033-2: 2006-05-01 (1st ed.)

Term	Definition	ISO/IEC JTC 1/SC 27 Document
hybrid DRBG	DRBG that uses a non-deterministic entropy source as an additional entropy source ■	N8745: FCD 18031: 2010-05-18
hybrid firmware module interface HFMI	the total set of commands used to request the services of the hybrid firmware module, including parameters that enter or leave the module's cryptographic boundary as part of the requested service ■	N8776: 2nd WD 19790: 2010-07-16
hybrid module	module whose cryptographic boundary delimits the composite of a software or firmware, component and a disjoint hardware component ■	N8776: 2nd WD 19790: 2010-07-16
hybrid NRBG	(physical or non-physical) NRBG that takes a seed value as an additional entropy source ■	N8745: FCD 18031: 2010-05-18
hybrid software module interface HSMI	the total set of commands used to request the services of the hybrid software module, including parameters that enter or leave the module's cryptographic boundary as part of the requested service ■	N8776: 2nd WD 19790: 2010-07-16
ICT disaster recovery	ability of the ICT elements of an organisation to support its critical business functions to acceptable level within a predetermined period of time following a disruption ■	N8622: PreFDIS 27031: 2010-08-18
ICT disaster recovery plan ICT DRP	clearly defined and documented plan which recovers ICT capabilities when a disruption occurs NOTE it is called ICT continuity plan in some organizations. ■	N8622: PreFDIS 27031: 2010-08-18
ICT readiness for business continuity IRBC	capability of an organization to support its business operations by prevention, detection and response to disruption and recovery of ICT services ■	N8622: PreFDIS 27031: 2010-08-18
ICT systems	hardware, software and firmware of computers, telecommunications and network equipment or other electronic information handling systems and associated equipment NOTE ICT systems include any equipment or interconnected systems or subsystems of equipment that are used in the acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission or reception of data/information. ■	ISO/IEC 24762: 2008-02-01 (1st ed.)
identifiability	ability of personal characteristics such as name/identity, location, contact or others to be associated to a natural person ■	N8806: 4th CD 29100: 2010-06-10

Term	Definition	ISO/IEC JTC 1/SC 27 Document
identification	process involving the search for, recognition and documentation of potential digital evidence 3.14 imaging process of creating a bitwise copy of storage media, commonly adopted by digital forensic practitioners NOTE Some storage media have an area inaccessible via an interface such as invalid block of a flash memory. EXAMPLE When imaging a hard disk, the DEFR would also copy data that has been deleted but not overwritten. ■	N8640: 3rd WD 27037: 2010-05-31
identification	recognition of an entity (3.1.1) in a particular domain (3.2.3) NOTE 1 The process of identification uses claimed, observed or assigned attributes. NOTE 2 Recognition is a process to determine that presented identity information associated with a particular entity meets all the requirements for the entity to be recognized as distinct from other entities in a particular domain. NOTE 3 Identification is usually an authentication process to obtain a specific level of confidence in the result. ■	N8804: 3rd CD 24760-1: 2010-06-11
identification	recognition of a person in a particular domain by a set of his or her attributes ■	N8806: 4th CD 29100: 2010-06-10
identification (biometrics)	process of performing a biometric search against an enrolment database to find and return the identity reference attributable to a single individual ■	N8802: FCD 24745: 2010-05-19
identification data	set of public data items (an account number, an expiry date and time, a serial number, etc.) assigned to an entity and used to identify it ■	ISO/IEC 9798-5: 2009-12-15 (3rd ed.)
identification data	sequence of data elements, including the distinguishing identifier for an entity, assigned to an entity and used to identify it NOTE The identification data may additionally contain data elements such as identifier of the signature process, identifier of the signature key, validity period of the signature key, restrictions on key usage, associated security policy parameters, key serial number, or domain parameters. [ISO/IEC 14888-1] ■	N8763: 1st WD 20009-2: 2010-06-20
identification data	sequence of data elements, including the distinguishing identifier for an entity, assigned to an entity and used to identify it NOTE The identification data may additionally contain data elements such as identifier of the signature process, identifier of the signature key, validity period of the signature key, restrictions on key usage, associated security policy parameters, key serial number, or domain parameters. [ISO/IEC 14888-1] ■	N8751: FCD 29150: 2010-06-10

Term	Definition	ISO/IEC JTC 1/SC 27 Document
identification data	sequence of data elements, including the distinguishing identifier for an entity, assigned to an entity and used to identify it NOTE The identification data may additionally contain data elements such as identifier of the signature process, identifier of the signature key, validity period of the signature key, restrictions on key usage, associated security policy parameters, key serial number, or domain parameters. ■	ISO/IEC 14888-1: 2008-04-15 (2nd ed.)
identification rank	smallest value k for which a user's correct identifier is in the top k identifiers returned by an identification system NOTE The Identification rank is dependent on the size of the enrolment database, and should be quoted "rank k out of n". ■	ISO/IEC 19792: 2009-08-01 (1st ed.)
identifier	one or more attributes (3.1.3) that uniquely characterize an entity in a specific domain (3.2.3) NOTE An identifier may be suitable for use outside the domain. EXAMPLE A name of a club with a club-membership number, a health insurance card number together with a name of the insurance company, an IP address, or a Universal Unique Identifier (UUID) can all be used as identifiers. ■	N8804: 3rd CD 24760-1: 2010-06-11
identifier	one or more attributes that uniquely characterize an entity in a specific domain EXAMPLE A name of a club with a club-membership number, a health insurance card number together with a name of the insurance company, an IP address, or an UUID can all be used as identifiers ■	N8802: FCD 24745: 2010-05-19
identity	representation uniquely identifying entities (e.g. a user, a process or a disk) within the context of the TOE NOTE An example of such a representation is a string. For a human user, the representation can be the full or abbreviated name or a (still unique) pseudonym. ■	ISO/IEC 15408-1: 2009-12-15 (3rd ed.)
identity	set of attributes which make it possible to recognize, contact or locate the PII principal ■	N8806: 4th CD 29100: 2010-06-10
identity	structured collection of an entity's attributes allowing this entity to be recognized and distinguished from other entities within a given domain ■	N8802: FCD 24745: 2010-05-19

Term	Definition	ISO/IEC JTC 1/SC 27 Document
identity partial identity ID	set of attributes (3.1.3) related to an entity (3.1.1) NOTE 1 An entity can have more than one identity. NOTE 2 Usually an identity allows entities to be distinguished within a domain of applicability. NOTE 3 ITU-T X1252[[9]] specifies the unique distinguishing use of an identity, in this document the term identifier implies this aspect. ■	N8804: 3rd CD 24760-1: 2010-06-11
identity assertion	statement by an identity information authority (3.3.4) used by a relying party (3.3.8) for authentication (3.3.2) of an identity (3.1.2) NOTE An identity assertion may be the cryptographic proof of a successful authentication, created with algorithms and keys agreed in the identity federation. ■	N8804: 3rd CD 24760-1: 2010-06-11
identity evidence evidence of identity	identity information (3.2.5) for an entity (3.1.1) required for authentication(3.3.2) of an entity ■	N8804: 3rd CD 24760-1: 2010-06-11
identity federation	agreement between two or more domains (3.2.3) specifying how identity information (3.2.5) will be exchanged and managed for cross-domain identification (3.2.1) purposes NOTE 1 Establishing an identity federation typically includes an agreement on the use of common protocols and procedures for privacy control, data protection and auditing and the use of standardized data formats and cryptographic techniques NOTE 2 The federation agreement can be the basis for identity authorities in each of the domains of applicability to mutually recognize credentials for authorization ■	N8804: 3rd CD 24760-1: 2010-06-11
identity information	set of values of attributes (3.1.3) in an identity (3.1.2) ■	N8804: 3rd CD 24760-1: 2010-06-11
identity information authority - IIA	entity (3.1.1) related to a particular domain (3.2.3) that can make assertions on the validity and/or correctness of one or more attribute (3.1.3) values in an identity (3.1.2) NOTE 1 An identity information authority is typically associated with a domain in which the attributes it can make assertions on have a particular significance, for instance the domain of origin. NOTE 2 The activity of an identity information authority may be subject to a policy on privacy protection. ■	N8804: 3rd CD 24760-1: 2010-06-11

Term	Definition	ISO/IEC JTC 1/SC 27 Document
identity information provider - IIP	entity (3.1.1) that makes available identity information (3.2.5) NOTE Typical operations performed by an identity information provider are to create and maintain identity information for entities known in a particular domain. An identity information provider and an identity information authority may be the same entity. ■	N8804: 3rd CD 24760-1: 2010-06-11
identity management IM	processes and policies involved in managing the value and life cycle of attributes (3.1.3) of identities (3.1.2) known in a particular domain NOTE Processes and policies in identity management support the functions of an identity information authority where applicable, in particular to handle the interaction between an entity for which an identity is managed and the identity information authority. ■	N8804: 3rd CD 24760-1: 2010-06-11
identity management system IdMS	system controlling entity identity information throughout the information lifecycle in one domain ■	N8802: FCD 24745: 2010-05-19
identity proofing initial entity authentication	particular form of authentication (3.3.2) based on identity evidence (3.4.4) that is performed as the condition for enrolment (3.4.3) ■	N8804: 3rd CD 24760-1: 2010-06-11
identity reference IR	non-biometric attribute that is an identifier with a value that remains the same for the duration of the existence of the entity in a domain ■	N8802: FCD 24745: 2010-05-19
identity register IMS register	repository of identities (3.1.2) for different entities (3.1.1) NOTE 1 A typical identity register is indexed by reference identifier NOTE 2 The identity information authority in a particular domain typically uses its own identity register. However, an identity register may be shared between related domains, e.g. within the same commercial entity. NOTE 3 The quality of the identity information in an identity register is determined by the authentication policies used during enrolment. ■	N8804: 3rd CD 24760-1: 2010-06-11
identity registration	process of recording an entity(3.1.1) in an identity register(3.4.5) ■	N8804: 3rd CD 24760-1: 2010-06-11
impact	adverse change to the level of business objectives achieved ■	N8718: 1st WD 27000: 2010-05-27
impact	adverse change to the level of business objectives achieved ■	N8923: FCD 27005: 2010-06-02

Term	Definition	ISO/IEC JTC 1/SC 27 Document
implementation representation	least abstract representation of the TSF, specifically the one that is used to create the TSF itself without further design refinement NOTE Source code that is then compiled or a hardware drawing that is used to build the actual hardware are examples of parts of an implementation representation. ■	ISO/IEC 15408-1: 2009-12-15 (3rd ed.)
implicit key authentication from *A* to *B*	assurance for entity *B* that *A* is the only other entity that can possibly be in possession of the correct key [ISO/IEC 11770-3:1999] ■	ISO/IEC 11770-4: 2006-05-01 (1st ed.)
implicit key authentication from entity *A* to entity *B*	assurance for entity *B* that entity *A* is the only other entity that can possibly be in possession of the correct key [ISO/IEC 11770-3] ■	ISO/IEC 11770-2: 2008-06-15 (2nd ed.)
implicit key authentication from entity *A* to entity *B*	assurance for entity *B* that entity *A* is the only other entity that can possibly be in possession of the correct key ■	ISO/IEC 11770-3: 2008-07-15 (2nd ed.)
imprint	string of bits, either the hash-code of a data string or the data string itself ■	ISO/IEC 13888-1: 2009-07-15 (3rd ed)
imprint	string of bits, either the hash-value of a data string or the data string itself [ISO/IEC 13888-1:2009] ■	N8642: 2nd PDTR 29149: 2010-06-22
inactive	state of an entity, in which the entity can not obtain the *shared secret key* ■	N8743: 2nd CD 11770-5: 2010-07-29
indicator	measure that provides an estimate or evaluation of specified attributes derived from an analytical model with respect to defined information needs ■	ISO/IEC 27004: 2009-12-15 (1st ed.)
indirect identifier	attribute (3.1.3) associated with in an entity (3.1.1) in a domain (3.2.3 that is based on an unique values in an identifier (3.1.4) for the same entity (3.1.1) from a different domain EXAMPLE The number of a driver's license in a membership record. ■	N8804: 3rd CD 24760-1: 2010-06-11
individual key	*key* shared between the *key distribution centre* and each entity NOTE *Key* meant to be used for encrypting other keys and shared between an entity and the *key distribution centre*. *Individual keys* are unique per entity. ■	N8743: 2nd CD 11770-5: 2010-07-29
individual rekeying	*rekeying* method in which the *shared secret key*, and optionally, *key encryption keys* are updated when an entity j*oins* or *leaves* ■	N8743: 2nd CD 11770-5: 2010-07-29
industry sector	organisational grouping based on economic or societal similarities ■	N8708: 3rd WD 27010: 2010-05-27
informal	expressed in natural language ■	ISO/IEC 15408-1: 2009-12-15 (3rd ed.)
information asset	knowledge or data that has a distinct value to the organization ■	N8718: 1st WD 27000: 2010-05-27

Term	Definition	ISO/IEC JTC 1/SC 27 Document
information asset	knowledge or data that has value to the individual or organization NOTE Adapted from ISO/IEC 27000:2009 ■	N8624: 2nd CD 27032: 2010-06-15
information need	insight necessary to manage objectives, goals, risks and problems [ISO/IEC 15939:2007] ■	ISO/IEC 27004: 2009-12-15 (1st ed.)
information security	preservation of confidentiality (2.10), integrity (2.30) and availability (2.8) of information NOTE In addition, other properties, such as authenticity (2.7), accountability (2.2), nonrepudiation (2.36), and reliability (2.42) can also be involved. ■	N8718: 1st WD 27000: 2010-05-27
information security	preservation of confidentiality, integrity and availability of information NOTE 1 In addition, other properties such as authenticity, accountability, non-repudiation and reliability can also be involved. NOTE 2 Adapted from ISO/IEC 27002:2005. ■	ISO/IEC 24762: 2008-02-01 (1st ed.)
information security event	identified occurrence relating to information security (2.22) ■	N8718: 1st WD 27000: 2010-05-27
information security forensics	application of investigation and analysis techniques to capture, record and analyze information security incidents; to discover the source of attacks or other types of incident and, if necessary, to gather evidence suitable for presentation in disciplinary proceedings or a court of law, or for other purposes NOTE The goal of information security forensics is to perform a structured investigation while maintaining a documented and appropriate chain of evidence to help determine what happened and who was responsible for it. For further information on information security forensics, refer to ISO/IEC 27037. ■	N8636: FCD 27035: 2010-05-19
information security incident	information security events (2.23) that have compromised information security (2.22) ■	N8718: 1st WD 27000: 2010-05-27
information security incident management	processes (2.40) for detecting, reporting, assessing, responding to, dealing with, and learning from information security incidents (2.24) ■	N8718: 1st WD 27000: 2010-05-27

Term	Definition	ISO/IEC JTC 1/SC 27 Document
information security incident response team - ISIRT	team of appropriately skilled and trusted members of the organization that handles information security incidents during their lifecycle NOTE 1 Where the focus of activity of an ISIRT is on Information and Communication Technology (ICT) systems, in some communities such a team is typically referred to as a Computer Security Incident Response Team (CSIRT) or Computer Emergency Response Team (CERT). NOTE 2 The ISIRT as described in this Standard is an organizational function that covers the process for information security incidents, while other common functions (with similar abbreviations) within the incident handling may have slightly different scope and purpose and mainly focusing on IT related incidents only. Some common used abbreviations are: - CERT: Computer Emergency Response Team mainly focuses on ICT incidents. There may be other specific national definitions for CERT. - CSIRT: A Computer Security Incident Response Team is a service organization that is responsible for receiving, reviewing, and responding to computer security incident reports and activity. Their services are usually performed for a defined constituency that could be a parent entity such as a corporation, governmental, or educational organization; a region or country; a research network; or a paid client. ■	N8636: FCD 27035: 2010-05-19
information security management	business risk-based approach, to establishing, implementing, operating, monitoring, reviewing, maintaining and improving information security (2.22) ■	N8718: 1st WD 27000: 2010-05-27
information security management system - ISMS	part of the overall management system (2.34) which applies information security management (2.26) principles and practices ■	N8718: 1st WD 27000: 2010-05-27
information security management system - ISMS	part of the overall management system based on business risk approach, to establish, implement, operate, monitor, review, maintain and improve information security [ISO/IEC 27001:2005, definition 3.7] ■	ISO/IEC TR 15443-3: 2007-12-15 (1st ed.)
information security risk	effect of uncertainty on information security (2.22) objectives ■	N8718: 1st WD 27000: 2010-05-27
information security risk	potential that a given threat will exploit vulnerabilities of an asset or group of assets and thereby cause harm to the organization NOTE 1 In general terms, a risk is an effect of uncertainty on objectives (see ISO 31000:2009) NOTE 2 It is measured in terms of a combination of the likelihood of an event and its consequence. ■	N8923: FCD 27005: 2010-06-02

Term	Definition	ISO/IEC JTC 1/SC 27 Document
information sharing community	group of organisations that agree to share information ■	N8708: 3rd WD 27010: 2010-05-27
information system	application, service, information technology asset, or any other information handling component ■	N8718: 1st WD 27000: 2010-05-27
infrastructure	facilities and equipments to enable the ICT DR services, including but not limited to power supply, telecommunications connections and environmental controls ■	ISO/IEC 24762: 2008-02-01 (1st ed.)
Initial provisioning	The initial provisioning of a ICT account must provide the entity with appropriate credentials for access authentication to required systems and services (see also subclause 9.5). ■	N8812: 3rd WD 29146: 2010-07-14
initialisation value	value used in defining the starting point of a cryptographic algorithm (e.g., a hash-function or an encryption algorithm) ■	N8745: FCD 18031: 2010-05-18
initialization value	value used in defining the starting point of an encipherment process [ISO 8372:1987] ■	N8749: 2nd CD 18033-4: 2010-05-19
initialization value	value used in defining the starting point of an encipherment process [ISO 8372: 1987] ■	N8757: 2nd WD 29192-3: 2010-07-01
initialization vector	a vector used in defining the starting point of a cryptographic process within a cryptographic algorithm ■	N8776: 2nd WD 19790: 2010-07-16
initializing value	a value used in defining the starting point of a hash-function ■	ISO/IEC 10118-1: 2000-06-15 (2nd ed.)
initializing value	function which maps strings of bits to fixed-length strings of bits, satisfying the following two properties: - for a given output, it is computationally infeasible to find an input which maps to this output; - for a given input, it is computationally infeasible to find a second input which maps to the same output [ISO/IEC 10118-1] ■	ISO/IEC FDIS 9797-2: 2009-09-18
input data	information that is entered into a cryptographic module and may be used for the purposes of transformation or computation using an approved security function [ISO/IEC 19790:2006, 3.33] ■	ISO/IEC 24759: 2008-07-01 (1st ed.)
input data	information that is entered into a cryptographic module may be used for the purposes of transformation or computation using an approved security function ■	N8776: 2nd WD 19790: 2010-07-16
input data string	value used in defining the starting point of a hash-function [ISO/IEC 10118-1] ■	ISO/IEC FDIS 9797-2: 2009-09-18

Term	Definition	ISO/IEC JTC 1/SC 27 Document
installation	procedure performed by a human user embedding the TOE in its operational environment and putting it into an operational state NOTE This operation is normally performed only once, after receipt and acceptance of the TOE. The TOE is expected to be progressed to a configuration allowed by the ST. If similar processes have to be performed by the developer they are denoted as "generation" throughout ALC: Life-cycle support. If the TOE requires an initial start-up that does not need to be repeated regularly, this process would be classified as installation. ■	ISO/IEC 15408-1: 2009-12-15 (3rd ed.)
integrity	property of protecting the accuracy and completeness of assets (2.3) ■	N8718: 1st WD 27000: 2010-05-27
integrity	property of safeguarding the accuracy and completeness of information and processing methods ■	ISO/IEC 21827: 2008-10-15 (2nd ed.)
integrity	property that sensitive data has not been modified or deleted in an unauthorised and undetected manner ■	N8776: 2nd WD 19790: 2010-07-16
integrity	quality of a system or component that reflects its logical correctness and reliability, completeness, and consistency. In security terms, integrity generates the requirement for the system or component to be protected against either intentional or accidental attempts to (1) alter, modify, or destroy it in an improper or unauthorized manner, or (2) prevent it from performing its intended function(s) in an unimpaired manner, free from improper or unauthorized manipulation. [CNSSI 4009, NIST SP 800-27-Rev.A] ■	N8732: 3rd WD 29193: 2010-08-06
inter TSF transfers	communicating data between the TOE and the security functionality of other trusted IT products ■	ISO/IEC 15408-1: 2009-12-15 (3rd ed.)
interaction	general communication-based activity between entities ■	ISO/IEC 15408-1: 2009-12-15 (3rd ed.)
interface	means of interaction with a component or module ■	ISO/IEC 15408-1: 2009-12-15 (3rd ed.)
interface	logical entry or exit point of a cryptographic module that provides access to the module for logical information flows ■	N8776: 2nd WD 19790: 2010-07-16
interleaving attack	masquerade which involves use of information derived from one or more ongoing or previous authentication exchanges ■	ISO/IEC 9798-1: 2010-07-01 (3rd ed.)
intermediate biometric reference template	intermediate biometric sample or combination of intermediate biometric samples used as a biometric reference template ■	ISO/IEC 24761: 2009-05-15 (1st ed.)
intermediate biometric sample	biometric sample obtained by processing a raw biometric sample, intended for further processing ■	ISO/IEC 24761: 2009-05-15 (1st ed.)

Term	Definition	ISO/IEC JTC 1/SC 27 Document
internal communication channel	communication channel between separated parts of the TOE ■	ISO/IEC 15408-1: 2009-12-15 (3rd ed.)
internal context	internal environment in which the organization seeks to achieve its objectives NOTE Internal context can include: - governance, organizational structure, roles and accountabilities; - policies, objectives, and the strategies that are in place to achieve them; - the capabilities, understood in terms of resources and knowledge (e.g. capital, time, people, processes, systems and technologies); - perceptions and values of internal stakeholders; - information systems, information flows and decision-making processes (both formal and informal); - relationships with, and perceptions and values of, internal stakeholders; - the organization's culture; - standards, guidelines and models adopted by the organization; and - form and extent of contractual relationships. [ISO Guide 31000:2009] ■	N8923: FCD 27005: 2010-06-02
internal TOE transfer	communicating data between separated parts of the TOE ■	ISO/IEC 15408-1: 2009-12-15 (3rd ed.)
internally consistent	no apparent contradictions exist between any aspects of an entity NOTE In terms of documentation, this means that there can be no statements within the documentation that can be taken to contradict each other. ■	ISO/IEC 15408-1: 2009-12-15 (3rd ed.)
internet	collection of interconnected networks called an internetwork or just an internet ■	ISO/IEC 27033-1: 2009-12-15 (1st ed.)
internet	global system of inter-connected networks in the public domain ■	ISO/IEC 27033-1: 2009-12-15 (1st ed.)
internet	the global system of inter-connected networks in the public domain [ISO/IEC 27033-1:2009] NOTE There is a difference between the definition of "an internet" and "the Internet". ■	N8624: 2nd CD 27032: 2010-06-15
internet internetwork	collection of interconnected networks NOTE 1 Adapted from ISO/IEC 27033-1:2009 NOTE 2 In this context, reference would be made to "an internet". There is a difference between the definition of "an internet" and "the Internet". ■	N8624: 2nd CD 27032: 2010-06-15
Internet Engineering Task Force - IETF	the group responsible for proposing and developing technical Internet standards. ■	ISO/IEC 18028-4: 2005-04-01 (1st ed.)
Internet Message Access Protocol v4 - IMAP4	an email protocol which allows accessing and administering emails and mailboxes located on a remote email server (defined in RFC 2060). ■	ISO/IEC 18028-4: 2005-04-01 (1st ed.)

Term	Definition	ISO/IEC JTC 1/SC 27 Document
Internet service provider	company that provides Internet services to a user and enables its customers access to the Internet Note 1: Usually in return for a fee. Note 2: Also sometimes referred to as an Internet access provider (IAP). ■	N8624: 2nd CD 27032: 2010-06-15
Internet services	services delivered to a user to enable access the Internet via an assigned IP address and typically includes authentication, authorisation and DNS services ■	N8624: 2nd CD 27032: 2010-06-15
interpretation	clarification or amplification of an ISO/IEC 15408, ISO/IEC 18045 or scheme requirement ■	N8912: Corrected 18045: 2010-09-15
intranet	private computer network that uses Internet protocols and network connectivity to securely share part of an organization's information or operations with its employees ■	ISO/IEC 27033-1: 2009-12-15 (1st ed.)
intruder	individual who is conducting, or has conducted, an intrusion or attack against a victim's host, site, network, or organization ■	ISO/IEC 18043: 2006-06-15 (1st ed.)
intrusion	unauthorized access to a network or a network-connected system, i.e. deliberate or accidental unauthorized access to an information system, to include malicious activity against an information system, or unauthorized use of resources within an information system ■	ISO/IEC 18043: 2006-06-15 (1st ed.)
intrusion	unauthorized access to a network or a network-connected system, i.e. deliberate or accidental unauthorized access to an information system, to include malicious activity against an information system, or unauthorized use of resources within an information system ■	ISO/IEC 27033-1: 2009-12-15 (1st ed.)
intrusion detection	formal process of detecting intrusions, generally characterized by gathering knowledge about abnormal usage patterns as well as what, how, and which vulnerability has been exploited to include how and when it occurred ■	ISO/IEC 18043: 2006-06-15 (1st ed.)
intrusion detection	formal process of detecting intrusions, generally characterized by gathering knowledge about abnormal usage patterns as well as what, how, and which vulnerability has been exploited so as to include how and when it occurred NOTE See ISO/IEC 18043. ■	ISO/IEC 27033-1: 2009-12-15 (1st ed.)
intrusion detection system IDS	technical system that is used to identify that an intrusion has been attempted, is occurring, or has occurred and possibly respond to intrusions in information systems and networks NOTE See ISO/IEC 18043. ■	ISO/IEC 27033-1: 2009-12-15 (1st ed.)
intrusion detection system, IDS	information system used to identify that an intrusion has been attempted, is occurring, or has occurred and possibly respond to intrusions in Information Systems and networks ■	ISO/IEC 18043: 2006-06-15 (1st ed.)

Term	Definition	ISO/IEC JTC 1/SC 27 Document
intrusion prevention	formal process of actively responding to prevent intrusions ■	ISO/IEC 27033-1: 2009-12-15 (1st ed.)
intrusion prevention system IPS	variant on intrusion detection systems that are specifically designed to provide an active response capability NOTE See ISO/IEC 18043. ■	ISO/IEC 27033-1: 2009-12-15 (1st ed.)
intrusion prevention system, IPS	variant on intrusion detection systems that are specifically designed to provide an active response capability ■	ISO/IEC 18043: 2006-06-15 (1st ed.)
Irreversibility	property of a transform that creates a biometric reference from a biometric sample(s) or features such that knowledge of the transformed biometric reference cannot be used to determine any information about the generating biometric sample(s) or features ■	N8802: FCD 24745: 2010-05-19
ISMS project	structured activities undertaken by an organization to implement an ISMS ■	ISO/IEC 27003: 2010-02-01 (1st ed.)
ISO/IEC approved	security function that is either - specified in an ISO/IEC standard, or - adopted/recommended in an ISO/IEC standard and specified either in an annex of the ISO/IEC standard or in a document normatively referenced by the ISO/IEC standard ■	ISO/IEC 24759: 2008-07-01 (1st ed.)
ISO/IEC approved	security function that is either: - specified in an ISO/IEC standard; or - adopted/recommended in an ISO/IEC standard and specified either in an annex of the ISO/IEC standard or in a document referenced by the ISO/IEC standard cryptographic module that has been tested and validated by a validation authority ■	N8776: 2nd WD 19790: 2010-07-16
issue key	set of private data elements specific to an entity and usable only by this entity in the issue process NOTE Issue key is only available to an authorized entity with issue privilege. [ISO/IEC 14888-1] ■	N8763: 1st WD 20009-2: 2010-06-20
issue process	process which takes as input a user's public data, the issue key and the domain parameters, and which gives as output a user signature key ■	N8763: 1st WD 20009-2: 2010-06-20
IT security product	A package of IT software, firmware and/or hardware, providing functionality designed for use or incorporation within a multiplicity of systems [ISO/IEC 15408–1]. ■	ISO/IEC TR 15443-1: 2005-02-01 (1st ed.)
iteration	use of the same component to express two or more distinct requirements ■	ISO/IEC 15408-1: 2009-12-15 (3rd ed.)
Jacobi symbol	Jacobi symbol of *a* with respect to an odd number *n* is the product of the Legendre symbols of *a* with respect to the prime factors of *n* (repeating the Legendre symbols for repeated prime factors). NOTE Defined in Annex A of ISO/IEC 9796-2. ■	ISO/IEC 18032: 2005-01-15 (1st ed.)

Term	Definition	ISO/IEC JTC 1/SC 27 Document
join	change of an entity state from *inactive* to *active* ■	N8743: 2nd CD 11770-5: 2010-07-29
JTC 1 Registration Authority	organisation appointed by the ISO and IEC councils to register objects in accordance with a JTC 1 procedural Standard ■	ISO/IEC 15292: 2001-12-15 (1st ed.)
justification	analysis leading to a conclusion NOTE "Justification" is more rigorous than a demonstration. This term requires significant rigour in terms of very carefully and thoroughly explaining every step of a logical argument. ■	ISO/IEC 15408-1: 2009-12-15 (3rd ed.)
Kerckhoffs box	idealized cryptosystem where the design and public keys are known to an adversary, but in which there are secret keys and/or other private information that is not known to an adversary NOTE A Kerckhoffs Box lies between a black box and a glass box in terms of the knowledge of an adversary. ■	N8745: FCD 18031: 2010-05-18
key	sequence of symbols that controls the operation of a cryptographic transformation (e.g. encryption, decryption). [ISO/IEC 18033-1] ■	ISO/IEC 10116: 2006-02-01 (3rd ed.)
key	sequence of symbols that controls the operations of a cryptographic transformation (e.g. encipherment, decipherment, cryptographic check-function computation, signature calculation, or signature verification) [ISO/IEC 11770-3] ■	ISO/IEC 13888-1: 2009-07-15 (3rd ed)
key	sequence of symbols that controls the operations of a cryptographic transformation (e.g. encipherment, decipherment, cryptographic check-function computation, signature calculation, or signature verification) [ISO/IEC 11770-1] ■	ISO/IEC FDIS 13888-2: 2010-08-06
key	sequence of symbols that controls the operation of a cryptographic transformation NOTE Examples are encryption, decryption, cryptographic check function computation, signature generation, or signature verification. ■	ISO/IEC 9798-1: 2010-07-01 (3rd ed.)
key	sequence of symbols that controls the operation of a cryptographic transformation (e.g. encipherment, decipherment, cryptographic check function computation, signature calculation, or signature verification) [ISO/IEC 11770-3:1999] ■	ISO/IEC 11770-4: 2006-05-01 (1st ed.)
key	sequence of symbols that controls the operation of a cryptographic transformation (e.g. encipherment, decipherment) [ISO/IEC 11770-1:1996]. ■	ISO/IEC 18033-1: 2005-02-01 (1st ed.)
key	sequence of symbols that controls the operation of a cryptographic transformation (e.g., encryption, decryption) [ISO/IEC 11770-1:1996] ■	ISO/IEC 18033-2: 2006-05-01 (1st ed.)

Term	Definition	ISO/IEC JTC 1/SC 27 Document
key	sequence of symbols that controls the operation of a cryptographic transformation (e.g. encipherment, decipherment) [ISO/IEC 18033-1] ■	ISO/IEC 19772: 2009-02-15 (1st ed.)
key	sequence of symbols that controls the operation of a cryptographic transformation (e.g. encipherment, decipherment) [ISO/IEC 11770-1:1996] ■	N8755: 1st CD 29192-2: 2010-06-22
key	sequence of symbols that controls the operations of a cryptographic transformation ■	N8743: 2nd CD 11770-5: 2010-07-29
key	sequence of symbols that controls the operation of a cryptographic transformation EXAMPLE Encipherment, decipherment. [ISO/IEC 11770-1:1996] ■	N8749: 2nd CD 18033-4: 2010-05-19
key	sequence of symbols that controls the operation of a cryptographic transformation (e.g. encipherment, decipherment) [ISO/IEC 11770-1: 1996] ■	N8757: 2nd WD 29192-3: 2010-07-01
key	sequence of symbols that controls the operation of a cryptographic transformation (e.g. encryption, decryption) [ISO/IEC 11770-1:1996] ■	N8751: FCD 29150: 2010-06-10
key	sequence of symbols that controls the operation of a cryptographic transformation (e.g., encryption, decryption, cryptographic check function computation, signature generation, or signature verification) ■	ISO/IEC FDIS 11770-1: 2010-07-26
key	sequence of symbols that controls the operation of a cryptographic transformation (e.g. encipherment, decipherment) NOTE In all the ciphers specified in this part of ISO/IEC18033, keys consist of a sequence of bits. [ISO/IEC 11770-1:1996] ■	ISO/IEC FDIS 18033-3: 2010-07-12
key	sequence of symbols that controls the operation of a cryptographic transformation e.g. encryption, decryption, cryptographic check function computation, signature generation, or signature verification [ISO/IEC 9798-1:2010] ■	N8861: PreFDIS 9797-1: 2010-09-03
key	sequence of symbols that controls the operation of a cryptographic transformation (e.g. encipherment, decipherment, *MAC* function computation, signature calculation, or signature verification) [ISO/IEC 11770-1:1996] ■	ISO/IEC 11770-3: 2008-07-15 (2nd ed.)
key (cryptographic key)	sequence of symbols that controls the operation of a cryptographic transformation [ISO/IEC 9798-1] ■	N8762: 1st WD 20009-1: 2010-07-13

Term	Definition	ISO/IEC JTC 1/SC 27 Document
key agreement	key agreement process of establishing a shared secret key between entities in such a way that neither of them can predetermine the value of that key NOTE By "predetermine" it is meant that neither entity *A* nor entity *B* can, in a computationally efficient way, choose a smaller key space and force the computed key in the protocol to fall into that key space. ■	ISO/IEC 11770-3: 2008-07-15 (2nd ed.)
key agreement	process of establishing a shared secret key between entities in such a way that neither of them can predetermine the value of that key [ISO/IEC 11770-1:1996] ■	ISO/IEC 11770-4: 2006-05-01 (1st ed.)
key agreement	process of establishing a shared secret key between entities in such a way that neither of them can predetermine the value of that key ■	ISO/IEC FDIS 11770-1: 2010-07-26
key agreement	key establishment procedure where the resultant key is a function of information by two or more participants, so that no party can predetermine the value of the key independently of the other party's contribution using automated methods ■	N8776: 2nd WD 19790: 2010-07-16
key archiving	service which provides a secure, long-term storage of keys after normal use ■	ISO/IEC FDIS 11770-1: 2010-07-26
key certification	service which assures the association of a public key with an entity ■	ISO/IEC FDIS 11770-1: 2010-07-26
key chain	set of cryptographic *keys* which are not necessarily independent ■	N8743: 2nd CD 11770-5: 2010-07-29
key commitment	process of committing to use specific keys in the operation of a key agreement scheme before revealing the specified keys ■	ISO/IEC 11770-3: 2008-07-15 (2nd ed.)
key confirmation	assurance for one entity that another identified entity is in possession of the correct key ■	ISO/IEC FDIS 11770-1: 2010-07-26
key confirmation from *A* to *B*	assurance for entity *B* that entity *A* is in possession of the correct key [ISO/IEC 11770-3:1999] ■	ISO/IEC 11770-4: 2006-05-01 (1st ed.)
key confirmation from entity *A* to entity *B*	assurance for entity *B* that entity *A* is in possession of the correct key [ISO/IEC 11770-3] ■	ISO/IEC 11770-2: 2008-06-15 (2nd ed.)
key confirmation from entity *A* to entity *B*	assurance for entity *B* that entity *A* is in possession of the correct key ■	ISO/IEC 11770-3: 2008-07-15 (2nd ed.)
key control	ability to choose the key, or the parameters used in the key computation [ISO/IEC 11770-1:1996] ■	ISO/IEC 11770-4: 2006-05-01 (1st ed.)
key control	ability to choose the key, or the parameters used in the key computation ■	ISO/IEC FDIS 11770-1: 2010-07-26
key control	ability to choose the key, or the parameters used in the key computation ■	ISO/IEC 11770-2: 2008-06-15 (2nd ed.)
key control	ability to choose the key or the parameters used in the key computation ■	ISO/IEC 11770-3: 2008-07-15 (2nd ed.)

Term	Definition	ISO/IEC JTC 1/SC 27 Document
key deregistration	procedure provided by a key registration authority that removes the association of a key with an entity ■	ISO/IEC FDIS 11770-1: 2010-07-26
key derivation	service which forms a potentially large number of keys using a secret original key called the derivation key, non-secret variable data and a secure transformation process ■	ISO/IEC FDIS 11770-1: 2010-07-26
key derivation function	function that utilizes shared secrets and other mutually known parameters as inputs, and outputs one or more shared secrets, which can be used as keys ■	ISO/IEC 11770-4: 2006-05-01 (1st ed.)
key derivation function	function that maps octet strings of any length to octet strings of an arbitrary, specified length, such that it is computationally infeasible to find correlations between inputs and outputs, and such that given one part of the output, but not the input, it is computationally infeasible to predict any bit of the remaining output. The precise security requirements depend on the application. NOTE See Clause 6.2. ■	ISO/IEC 18033-2: 2006-05-01 (1st ed.)
key derivation function	function that outputs one or more shared secrets, used as keys, given shared secrets and other mutually known parameters as input ■	ISO/IEC 11770-3: 2008-07-15 (2nd ed.)
key destruction	service for the secure destruction of keys that are no longer needed ■	ISO/IEC FDIS 11770-1: 2010-07-26
key distribution	service which securely provides key management information objects to authorized entities ■	ISO/IEC FDIS 11770-1: 2010-07-26
key distribution centre	entity trusted to generate or acquire, and distribute *keys* to entities ■	N8743: 2nd CD 11770-5: 2010-07-29
key distribution centre	entity that is trusted to generate or acquire keys and to distribute the keys to communicating parties and that shares a unique symmetric key with each of the parties ■	ISO/IEC FDIS 11770-1: 2010-07-26
key distribution service	service of distributing keys securely to authorized entities performed by a Key Distribution Center and described in ISO/IEC 11770-1. ■	ISO/IEC 15945: 2002-02-01 (1st ed.)
key encapsulation mechanism	similar to an asymmetric cipher, but the encryption algorithm takes as input a public key and generates a secret key and an encryption of this secret key NOTE See Clause 8.1. ■	ISO/IEC 18033-2: 2006-05-01 (1st ed.)
key encryption key	optional key shared with some entities to reduce communication overhead in a key establishment mechanism for multiple entities NOTE This key may be updated. ■	N8743: 2nd CD 11770-5: 2010-07-29
key encryption key KEK	a cryptographic key that is used for the encryption or decryption of other keys ■	N8776: 2nd WD 19790: 2010-07-16

Term	Definition	ISO/IEC JTC 1/SC 27 Document
key establishment	process of making available a shared secret key to one or more entities; key establishment includes key agreement, key transport and key retrieval ■	ISO/IEC 11770-4: 2006-05-01 (1st ed.)
key establishment	process of making available a shared key to one or more entities, where the process includes key agreement or key transport [ISO/IEC 11770-3:2008] ■	ISO/IEC FDIS 11770-1: 2010-07-26
key establishment	the process of making available a shared secret key to one or more entities NOTE Key establishment includes key agreement and key transport ■	N8776: 2nd WD 19790: 2010-07-16
key establishment	process of making available a shared secret key to one or more entities, where the process includes key agreement and key transport ■	ISO/IEC 11770-3: 2008-07-15 (2nd ed.)
key generating function	function which takes as input a number of parameters, at least one of which shall be secret, and which gives as output keys appropriate for the intended algorithm and application, and which has the property that it is computationally infeasible to deduce the output without prior knowledge of the secret input ■	ISO/IEC 11770-2: 2008-06-15 (2nd ed.)
key generation	process of generating a key ■	ISO/IEC FDIS 11770-1: 2010-07-26
key generation algorithm	method for generating asymmetric key pairs NOTE See Clauses 7, 8.1. ■	ISO/IEC 18033-2: 2006-05-01 (1st ed.)
key generator	entity responsible for generation of an asymmetric key pair ■	ISO/IEC FDIS 11770-1: 2010-07-26
key installation	service which securely establishes a key within a key management facility in a manner that protects it from compromise ■	ISO/IEC FDIS 11770-1: 2010-07-26
key loader	self-contained device that is capable of storing at least one plaintext or encrypted SSP or key component that can be transferred, upon request, into a cryptographic module. The use of a key loader requires human manipulation ■	N8776: 2nd WD 19790: 2010-07-16
key management	administration and use of the generation, registration, certification, deregistration, distribution, installation, storage, archiving, revocation, derivation and destruction of keying material in accordance with a security policy [ISO/IEC 11770-1:1996] ■	ISO/IEC 11770-4: 2006-05-01 (1st ed.)
key management	administration and use of generation, registration, certification, deregistration, distribution, installation, storage, archiving, revocation, derivation and destruction of keying material in accordance with a security policy ■	ISO/IEC FDIS 11770-1: 2010-07-26
key management	administration and use of the generation, registration, certification, deregistration, distribution, installation, storage, archiving, revocation, derivation and destruction of keying material in accordance with a security policy ■	N8776: 2nd WD 19790: 2010-07-16

Term	Definition	ISO/IEC JTC 1/SC 27 Document
key pair	pair consisting of a signature key and a verification key, i.e., - a set of data elements that shall be totally or partially kept secret, to be used only by the signer; - a set of data elements that can be totally made public, to be used by any verifier [ISO/IEC 14888-1] ■	N8760: 1st WD 20008-1: 2010-06-14
key pair	pair consisting of a signature key and a verification key, i.e., - a set of data elements that shall be totally or partially kept secret, to be used only by the signer; - a set of data elements that can be totally made public, to be used by any verifier [ISO/IEC 14888-1] ■	N8763: 1st WD 20009-2: 2010-06-20
key pair	pair consisting of a public key and a private key associated with an asymmetric cipher ■	N8751: FCD 29150: 2010-06-10
key pair	pair consisting of a signature key and a verification key, i.e., - a set of data elements that shall be totally or partially kept secret, to be used only by the signer; - a set of data elements that can be totally made public, to be used by any verifier ■	ISO/IEC 14888-1: 2008-04-15 (2nd ed.)
key registration	service which associates a key with an entity ■	ISO/IEC FDIS 11770-1: 2010-07-26
key retrieval	process of establishing a key for one or more entities known as the retrieving entities with the involvement of one or more other entities who are not necessarily able to access the key after the process, and which normally requires authentication of the retrieving entity/entities by the other entity/entities ■	ISO/IEC 11770-4: 2006-05-01 (1st ed.)
key revocation	service which assures the secure deactivation of a key ■	ISO/IEC FDIS 11770-1: 2010-07-26
key storage	service which provides secure storage of keys intended for current or near-term use or for backup ■	ISO/IEC FDIS 11770-1: 2010-07-26
key token	key establishment message sent from one entity to another entity during the execution of a key establishment mechanism ■	ISO/IEC 11770-4: 2006-05-01 (1st ed.)
key token	key management message sent from one entity to another entity during the execution of a key management mechanism ■	ISO/IEC 11770-3: 2008-07-15 (2nd ed.)
key token check function	function that utilizes a key token and other publicly known parameters as input, and outputs a Boolean value during the execution of a key establishment mechanism ■	ISO/IEC 11770-4: 2006-05-01 (1st ed.)
key token factor	value that is kept secret and that is used, possibly in conjunction with a weak secret, to create a key token ■	ISO/IEC 11770-4: 2006-05-01 (1st ed.)
key token generation function	function that utilizes a key token factor and other parameters as input, and outputs a key token during the execution of a key establishment mechanism ■	ISO/IEC 11770-4: 2006-05-01 (1st ed.)

Term	Definition	ISO/IEC JTC 1/SC 27 Document
key translation centre	entity trusted to decrypt a key that was generated and encrypted by one party and re-encrypt it for another party ■	ISO/IEC FDIS 11770-1: 2010-07-26
key transport	process of transferring a key from one entity to another entity, suitably protected [ISO/IEC 11770-3:2008] ■	ISO/IEC FDIS 11770-1: 2010-07-26
key transport	the process of transferring a key from one entity to another entity using automated methods ■	N8776: 2nd WD 19790: 2010-07-16
key transport	process of transferring a key from one entity to another entity, suitably protected ■	ISO/IEC 11770-3: 2008-07-15 (2nd ed.)
keying material	data necessary to establish and maintain cryptographic keying relationships EXAMPLES Keys, initialization values. ■	ISO/IEC FDIS 11770-1: 2010-07-26
keystream	pseudorandom sequence of symbols, intended to be secret, used by the encryption and decryption algorithms of a stream cipher. If a portion of the keystream is known by an attacker, then it shall be computationally infeasible for the attacker to deduce any information about the remainder of the keystream. ■	ISO/IEC 18033-1: 2005-02-01 (1st ed.)
keystream	pseudorandom sequence of symbols, intended to be secret, used by the encryption and decryption algorithms of a stream cipher NOTE If a portion of the keystream is known by an attacker, then it shall be computationally infeasible for the attacker to deduce any information about the remainder of the keystream. ■	N8751: FCD 29150: 2010-06-10
keystream function	function that takes as input the current state of the keystream generator and (optionally) part of the previously output ciphertext, and gives as output the next part of the keystream ■	N8749: 2nd CD 18033-4: 2010-05-19
keystream function	function that takes as input the current state of the keystream generator and (optionally) part of the previously output ciphertext, and gives as output the next part of the keystream ■	N8757: 2nd WD 29192-3: 2010-07-01
keystream generator	state-based process (i.e. a finite state machine) that takes as inputs a key, an initialization vector, and if necessary the ciphertext, and that outputs a keystream, i.e. a sequence of bits or blocks of bits, of arbitrary length ■	N8749: 2nd CD 18033-4: 2010-05-19
keystream generator	state-based process (i.e. a finite state machine) that takes as inputs a key, an initialization vector, and if necessary the ciphertext, and that outputs a keystream, i.e. a sequence of bits or blocks of bits, of arbitrary length ■	N8757: 2nd WD 29192-3: 2010-07-01

Term	Definition	ISO/IEC JTC 1/SC 27 Document
known-answer test	method of testing a deterministic mechanism where a given input is processed by the mechanism and the resulting output is then compared to a corresponding known value NOTE Known-answer testing of a deterministic mechanism may also include testing the integrity of the software which implements the deterministic mechanism. For example, if the software implementing the deterministic mechanism is digitally signed, then the signature can be recalculated and compared to the known signature value. ■	N8745: FCD 18031: 2010-05-18
label	octet string that is input to both the encryption and decryption algorithms of an asymmetric cipher, and of a data encapsulation mechanism. A label is public information that is bound to the cipher text in a nonmalleable way NOTE See Clauses 7, 8.2. ■	ISO/IEC 18033-2: 2006-05-01 (1st ed.)
lamb	biometric reference that results in higher than normal similarity scores on a particular biometric system when compared to biometric samples or references from other subjects ■	ISO/IEC 19792: 2009-08-01 (1st ed.)
layer 2 switching	technology that uses internal switching mechanisms to establish and control connections between devices using layer 2 protocols NOTE It is typically used to simulate a LAN environment to upper layer protocols. ■	ISO/IEC 18028-5: 2006-07-01 (1st ed.)
layer 2 VPN	virtual private network used to provide a simulated LAN environment over a network infrastructure NOTE Sites linked by a layer 2 VPN can operate as though they are on the same LAN. ■	ISO/IEC 18028-5: 2006-07-01 (1st ed.)
layer 3 switching	technology that uses internal switching mechanisms in combination with standard routing mechanisms, or which employs MPLS techniques, in order to establish and control connections between networks ■	ISO/IEC 18028-5: 2006-07-01 (1st ed.)
layer 3 VPN	virtual private network used to provide a simulated WAN environment over a network infrastructure NOTE Sites linked by a layer 3 VPN can operate as though they are on a private WAN. ■	ISO/IEC 18028-5: 2006-07-01 (1st ed.)

Term	Definition	ISO/IEC JTC 1/SC 27 Document
layering	design technique where separate groups of modules (the layers) are hierarchically organized to have separate responsibilities such that one layer depends only on layers below it in the hierarchy for services, and provides its services only to the layers above it NOTE Strict layering adds the constraint that each layer receives services only from the layer immediately beneath it, and provides services only to the layer immediately above it. ■	ISO/IEC 15408-1: 2009-12-15 (3rd ed.)
leaf node	node in a *tree* which is not a parent of any other node, i.e. has no child nodes ■	N8743: 2nd CD 11770-5: 2010-07-29
leave	change of an entity state from active to inactive ■	N8743: 2nd CD 11770-5: 2010-07-29
Legendre symbol	Let p be an odd prime, and let a be a positive integer. The Legendre symbol of a with respect to p is defined as $a^{(p-1)/2} \bmod p$. NOTE Defined in Annex A of ISO/IEC 9796-2. ■	ISO/IEC 18032: 2005-01-15 (1st ed.)
length	length of a string of digits or the representation of an integer Specifically: (1) length of a bit string is the number of bits in the string NOTE 1 See Clause 5.2.1. (2) length of an octet string is the number of octets in the string NOTE 2 See Clause 5.2.2. (3) bit length of a non-negative integer n is the number of bits in its binary representation, i.e., $\mathrm{dlog}_2(n + 1)$ NOTE 3 See Clause 5.2.4. (4) octet length of a non-negative integer n is the number of digits in its representation base 256, i.e., $\mathrm{dlog}_{256}(n + 1)$ NOTE 4 See Clause 5.2.4. ■	ISO/IEC 18033-2: 2006-05-01 (1st ed.)
level of risk	magnitude of a risk (2.45) expressed in terms of the combination of consequences (2.12) and their likelihood (2.32) [ISO Guide 73:2009] ■	N8718: 1st WD 27000: 2010-05-27
level of risk	magnitude of a risk, expressed in terms of the combination of consequences and their likelihood [ISO 31000:2009] ■	N8923: FCD 27005: 2010-06-02
life cycle stage	instance within the deliverable life cycle that relates to the state of the deliverable. a) A period within the system life cycle that relates to the state of the system description and/or the system itself [ISO/IEC 15288]. ■	ISO/IEC TR 15443-1: 2005-02-01 (1st ed.)
life-cycle	sequence of stages of existence of an object (for example a product or a system) in time ■	ISO/IEC 15408-1: 2009-12-15 (3rd ed.)
life-cycle definition	definition of the life-cycle model ■	ISO/IEC 15408-1: 2009-12-15 (3rd ed.)

Term	Definition	ISO/IEC JTC 1/SC 27 Document
life-cycle model	description of the stages and their relations to each other that are used in the management of the life-cycle of a certain object, how the sequence of stages looks and which high level characteristics the stages have NOTE See also Figure 1. ■	ISO/IEC 15408-1: 2009-12-15 (3rd ed.)
lightweight cryptography	cryptography tailored to be implemented in constrained environments NOTE The constraints can be aspects such as chip area, energy consumption, memory size, or communication bandwidth. ■	N8753: 1st CD 29192-1: 2010-06-22
likelihood	chance of something happening [ISO Guide 73:2009] ■	N8718: 1st WD 27000: 2010-05-27
likelihood	chance of something happening NOTE 1 In risk management terminology, t he word "likelihood" is used to refer to the chance of something happening, whether defined, measured or determined objectively or subjectively, qualitatively or quantitatively, and described using general terms or mathematically (such as a probability or a frequency over a given time period). NOTE 2 The English term "likelihood" does not have a direct equivalent in some languages; instead, the equivalent of the term "probability" is often used. However, in English, "probability" is often narrowly interpreted as a mathematical term. Therefore, in risk management terminology, "likelihood" is used with the intent that it should have the same broad interpretation as the term "probability" has in many languages other than English. [ISO 31000:2009] ■	N8923: FCD 27005: 2010-06-02
limited operational environment	an operational environment that is designed to accept only controlled functional changes that successfully pass the software/firmware load test ■	N8776: 2nd WD 19790: 2010-07-16
link	data item attesting to the existence of at least two other data items through the use of collision-resistant hash functions ■	ISO/IEC 18014-3: 2009-12-15 (2nd ed.)
link key	set of private data elements specific to an entity and usable only by this entity in the link process NOTE Link key is only available to authorized entities with link privilege. ■	N8763: 1st WD 20009-2: 2010-06-20
link process	process which takes as input two anonymous signatures, the link key and the domain parameters, and which gives as output yes/no according to whether the two signatures have been generated from the same signer or not ■	N8763: 1st WD 20009-2: 2010-06-20
linking authority	entity who is able to find whether two anonymous signatures are linked or not ■	N8760: 1st WD 20008-1: 2010-06-14

Term	Definition	ISO/IEC JTC 1/SC 27 Document
linking base	set of public data elements, optionally specific to a linking authority, and usable by any linking authority in the linking process NOTE The linking base is also called the name base in the literature and used in direct anonymous attestation, which is specified in Part 2 of ISO/IEC 20008. ■	N8760: 1st WD 20008-1: 2010-06-14
linking key	set of private data elements specific to a linking authority and usable only by this entity in the linking process ■	N8760: 1st WD 20008-1: 2010-06-14
linking process	process which takes as inputs two anonymous signatures, the domain public parameters and optionally the linking base and/or the linking key, and which gives as output the result of the signature linkage: linked or unlinked ■	N8760: 1st WD 20008-1: 2010-06-14
Local Area Network - LAN	local network, usually within a building. ■	ISO/IEC 18028-4: 2005-04-01 (1st ed.)
local linkability	linkability with a feature that two or more signatures from a same anonymous user are linked only by a specific linking authority but other linking authorities or other entities cannot link the signatures ■	N8763: 1st WD 20009-2: 2010-06-20
logical cohesion	procedural cohesion; characteristics of a module performing similar activities on different data structures NOTE A module exhibits logical cohesion if its functions perform related, but different, operations on different inputs. See also cohesion (3.2.3). ■	ISO/IEC 15408-1: 2009-12-15 (3rd ed.)
logical key hierarchy	*tree* used for managing the *shared secret key* and *key encryption keys* ■	N8743: 2nd CD 11770-5: 2010-07-29
logical key structure	logical structure to manage *keys* NOTE This structure has no correlation with the network topology. ■	N8743: 2nd CD 11770-5: 2010-07-29
logical protection	protection against unauthorised access (including unauthorised use, modification, substitution, and, in the case of CSPs, disclosure) by means of the Module Software Interface under operating system control. Logical protection of software SSPs does not protect against physical tampering ■	N8776: 2nd WD 19790: 2010-07-16
low-level testing	testing of the individual components or group of components of the cryptographic module and their physical ports and logical interfaces ■	N8776: 2nd WD 19790: 2010-07-16

Term	Definition	ISO/IEC JTC 1/SC 27 Document
MAC algorithm	algorithm for computing a function which maps strings of bits and a secret key to fixed-length strings of bits, satisfying the following properties: - for any key and any input string the function can be computed efficiently; - for any fixed key, and given no prior knowledge of the key, it is computationally infeasible to compute the function value on any new input string, even given knowledge of the set of input strings and corresponding function values, where the value of the *i*th input string may have been chosen after observing the value of the first *i*-1 function values [ISO/IEC 9797-1] ■	ISO/IEC FDIS 13888-2: 2010-08-06
MAC algorithm	algorithm for computing a function which maps strings of bits and a secret key to fixed-length strings of bits, satisfying the following two properties: - for any key and any input string, the function can be computed efficiently; - for any fixed key, and given no prior knowledge of the key, it is computationally infeasible to compute the function value on any new input string, even given knowledge of the set of input strings and corresponding function values, where the value of the ith input string may have been chosen after observing the value of the first i - 1 function values. [ISO/IEC 9797-1] NOTE 1 See Clause 6.3. NOTE 2 In this part of ISO/IEC 18033, the input and output strings of a MAC algorithm will be restricted to be octet strings (interpreted in a natural way as bit strings). ■	ISO/IEC 18033-2: 2006-05-01 (1st ed.)
MAC algorithm key	key that controls the operation of a MAC algorithm [ISO/IEC 9797-1] ■	ISO/IEC FDIS 9797-2: 2009-09-18
MAC algorithm key	key that controls the operation of a MAC algorithm ■	N8861: PreFDIS 9797-1: 2010-09-03
maintainer	individual or organization that performs maintenance activities on a product or online service NOTE Adapted from ISO/IEC 12207:2008 ■	N8780: 1st CD 29147: 2010-06-10
maintenance	process of modifying a system or component after delivery to correct flaws, improve performance or other attributes, or adapt to a changed environment [IEEE-Std. 610] ■	ISO/IEC 21827: 2008-10-15 (2nd ed.)
maintenance process	any change performed on an application after its delivery. EXAMPLE Correction of faults, addition of functionality, steps taken to improve performance, ensuring that the application is functional. ■	N8632: FCD 27034-1: 2010-05-27

Term	Definition	ISO/IEC JTC 1/SC 27 Document
maintenance role	role assumed to perform physical maintenance and/or logical maintenance services [ISO/IEC 19790:2006, 3.41] EXAMPLE Maintenance services may include but are not limited to hardware and/or software diagnostics. ■	ISO/IEC 24759: 2008-07-01 (1st ed.)
maintenance role	role assumed to perform physical maintenance and/or logical maintenance services EXAMPLE Maintenance services may include but not limited to hardware and/or software diagnostics. ■	N8776: 2nd WD 19790: 2010-07-16
malicious contents	applications, documents, files, data or other resources that have malicious features or capabilities embedded, disguised or hidden in them ■	N8624: 2nd CD 27032: 2010-06-15
malware	software designed to infiltrate a computer system without the computer owner's informed consent NOTE 1 This definition was adapted from Wikipedia http://en.wikipedia.org/wiki/Malware. NOTE 2 The term originated from the combination of two words "malicious" and "software". NOTE 3 The term is a general term used by computer professionals to mean a variety of forms of damaging, intrusive, or annoying software or program code. EXAMPLE A maliciously crafted document that contains hidden vulnerability exploit code would be called malware. ■	N8780: 1st CD 29147: 2010-06-10
malware	malicious software designed specifically to damage or disrupt a system, attacking confidentiality, integrity and/or availability NOTE Viruses and Trojan horses are examples of malware. ■	ISO/IEC 27033-1: 2009-12-15 (1st ed.)
malware malicious software	software designed with malicious intent containing features or capabilities that can potentially cause harm directly or indirectly to the user and/or the user's computer system EXAMPLES Viruses, worms, trojans ■	N8624: 2nd CD 27032: 2010-06-15
malware malicious software	category of software that is designed with a malicious intent, containing features or capabilities that could potentially cause harm directly or indirectly to the user and/or the user's computer system NOTE See ISO/IEC 27032. ■	ISO/IEC FDIS 27033-3: 2010-09-10
management	coordinated activities to direct and control an organization ■	N8718: 1st WD 27000: 2010-05-27
management controls	security controls (i.e., safeguards and countermeasures) for an information system that focus on the management of risk and the management of information system security [NIST SP 800-53] ■	ISO/IEC TR 19791: 2010-04-01 (2nd ed.)

Term	Definition	ISO/IEC JTC 1/SC 27 Document
management system	framework of guidelines (2.19), policies (2.37), procedures (2.39) and processes (2.40) associated resources aimed at ensuring an organization meets its objectives ■	N8718: 1st WD 27000: 2010-05-27
Mandatory Access Controls	Mandatory Access Controls enforce policy over subjects and storage objects being controlled (e.g., processes, files, segments, devices). These subjects and objects are assigned sensitivity labels that are a combination of hierarchical classification levels and non-hierarchical categories, and the labels are used as the basis for mandatory access control decisions. (Adapted from DOD 5200.28-STD (para 3.1.1.4)) ■	N8812: 3rd WD 29146: 2010-07-14
Man-in-the-middle Attack	attack in which an attacker is able to read, insert, and modify messages between two parties without their knowledge. ■	N8810: 1st CD 29115 | X.eaa: 2010-06-10
manual	requiring human operator manipulation ■	N8776: 2nd WD 19790: 2010-07-16
manual authentication certificate	combination of a secret key and a check-value, generated by one of the two devices engaging in manual authentication, with the property that, when entered into the other device, this pair of values can be used to complete the manual authentication process at some later time ■	ISO/IEC FDIS 9798-6: 2010-08-05
manual entity authentication	process achieving entity authentication between two devices using a combination of message exchanges via a (potentially insecure) communications channel and the manual transfer of limited amounts of data between the devices ■	ISO/IEC FDIS 9798-6: 2010-08-05
mark	legally registered trade mark or otherwise protected symbol which is issued under the rules of an accreditation body or of a certification body, indicating that adequate confidence in the systems operated by a body has been demonstrated or that relevant products or individuals conform to the requirements of a specified standard ■	ISO/IEC 27006: 2007-03-01 (1st ed.)
mask generation function	function which maps strings of bits to strings of bits of arbitrary specified length, satisfying the following property: - it is computationally infeasible to predict, given one part of an output but not the input, another part of the output ■	ISO/IEC FDIS 9796-2: 2010-09-10
masquerade	pretence by an entity to be a different entity ■	ISO/IEC 9798-1: 2010-07-01 (3rd ed.)
Masquerade	pretence by an entity to be a different entity. ■	N8810: 1st CD 29115 | X.eaa: 2010-06-10
master secret key	data item that shall be kept secret and should only be used by the trusted server in accordance with the process of generation of signer private data ■	N8759: 2nd WD 29192-4: 2010-06-15
match	decision that the recognition biometric sample(s) and the biometric reference template are from the same individual ■	ISO/IEC 24761: 2009-05-15 (1st ed.)

Term	Definition	ISO/IEC JTC 1/SC 27 Document
matrix	an 8 by 8 matrix in which each entry is a string of 8 bits used in dedicated hash-function 7 of Clause 13 ■	ISO/IEC 10118-3: 2004-03-01 (3rd ed.)
measure	variable to which a value is assigned as the result of measurement [ISO/IEC 15939:2007] NOTE The term "measures" is used to refer collectively to base measures, derived measures, and indicators. EXAMPLE A comparison of a measured defect rate to planned defect rate along with an assessment of whether or not the difference indicates a problem. ■	ISO/IEC 27004: 2009-12-15 (1st ed.)
measurement	process of obtaining information about the effectiveness of ISMS and controls using a measurement method, a measurement function, an analytical model, and decision criteria ■	ISO/IEC 27004: 2009-12-15 (1st ed.)
measurement function	algorithm or calculation performed to combine two or more base measures [ISO/IEC 15939:2007] ■	ISO/IEC 27004: 2009-12-15 (1st ed.)
measurement method	logical sequence of operations, described generically, used in quantifying an attribute with respect to a specified scale [ISO/IEC 15939:2007] NOTE The type of measurement method depends on the nature of the operations used to quantify an attribute. Two types can be distinguished: - subjective: quantification involving human judgment; - objective: quantification based on numerical rules. ■	ISO/IEC 27004: 2009-12-15 (1st ed.)
measurement results	one or more indicators and their associated interpretations that address an information need ■	ISO/IEC 27004: 2009-12-15 (1st ed.)
message	string of octets of any length ■	ISO/IEC 9796-3: 2006-09-15 (2nd ed.)
message	string of bits of any length [ISO/IEC 14888-1] ■	ISO/IEC FDIS 9796-2: 2010-09-10
message	string of bits of any length [ISO/IEC 14888-1] ■	N8760: 1st WD 20008-1: 2010-06-14
message	string of bits of any length [ISO/IEC 14888-1] ■	N8763: 1st WD 20009-2: 2010-06-20
message	string of bits of any length ■	N8751: FCD 29150: 2010-06-10
message	string of bits of any length ■	ISO/IEC 14888-1: 2008-04-15 (2nd ed.)
message authentication code - MAC	string of bits which is the output of a *MAC* algorithm NOTE A *MAC* is sometimes called a cryptographic check value (see, for example, ISO 7498-2). ■	ISO/IEC 11770-3: 2008-07-15 (2nd ed.)
message authentication code - MAC	string of bits which is the output of a MAC algorithm [ISO/IEC 9797-1] NOTE A MAC is sometimes called a cryptographic check value (see for example ISO 7498-2). ■	ISO/IEC 13888-1: 2009-07-15 (3rd ed)

Term	Definition	ISO/IEC JTC 1/SC 27 Document
message authentication code – MAC	string of bits which is the output of a MAC algorithm NOTE A MAC is sometimes called a cryptographic check value. [ISO/IEC 9797-1:1999] ■	ISO/IEC 9798-2: 2008-12-15 (3rd ed.)
message authentication code – MAC	string of bits which is the output of a MAC algorithm [ISO/IEC 9797-1] ■	ISO/IEC FDIS 9798-6: 2010-08-05
message authentication code – MAC	string of bits which is the output of a MAC algorithm [ISO/IEC 9797-1] NOTE A MAC is sometimes called a cryptographic check value (see for example ISO/IEC 7498-2). ■	ISO/IEC FDIS 13888-2: 2010-08-06
message authentication code – MAC	string of bits which is the output of a MAC algorithm NOTE A MAC is sometimes called a cryptographic check value (see for example ISO 7498-2). [ISO/IEC 9797-1:1999, definition 3.2.4] ■	ISO/IEC 18014-2: 2009-12-15 (2nd ed.)
message authentication code – MAC	cryptographic checksum on data that uses a symmetric key to detect both accidental and intentional modifications of data EXAMPLE A Hash Based Message Authentication Code ■	N8776: 2nd WD 19790: 2010-07-16
message authentication code – MAC	string of bits which is the output of a MAC algorithm NOTE A MAC is sometimes called a cryptographic check value (see for example ISO 7498-2). [ISO/IEC 9797-1:1999] ■	N8642: 2nd PDTR 29149: 2010-06-22
message authentication code - MAC	string of bits which is the output of a MAC algorithm NOTE A MAC is sometimes called a cryptographic check value (see for example ISO 7498-2 [1]). ■	N8861: PreFDIS 9797-1: 2010-09-03
message authentication code - MAC	string of bits which is the output of a MAC algorithm NOTE A MAC is sometimes called a cryptographic check value (see for example ISO 7498-2 [1]). [ISO/IEC 9797-1] ■	ISO/IEC FDIS 9797-2: 2009-09-18
message authentication code - MAC	string of bits which is the output of a MAC algorithm [ISO/IEC 9797-1] NOTE 1 See Clause 6.3. NOTE 2 In this part of ISO/IEC 18033, a MAC will be restricted to be an octet string (interpreted in a natural way as a bit string). ■	ISO/IEC 18033-2: 2006-05-01 (1st ed.)
message authentication code - MAC	string of bits which is the output of a MAC algorithm [ISO/IEC 9797-1] ■	ISO/IEC 19772: 2009-02-15 (1st ed.)

Term	Definition	ISO/IEC JTC 1/SC 27 Document
message authentication code (MAC) algorithm	algorithm for computing a function which maps strings of bits and a secret key to fixed-length strings of bits, satisfying the following two properties: - for any key and any input string the function can be computed efficiently; - for any fixed key, and given no prior knowledge of the key, it is computationally infeasible to compute the function value on any new input string, even given knowledge of the set of input strings and corresponding function values, where the value of the *i*th input string may have been chosen after observing the value of the first *i* - 1 function values. NOTE 1 A MAC algorithm is sometimes called a cryptographic check function (see for example ISO 7498-2). NOTE 2 Computational feasibility depends on the user's specific security requirements and environment. [ISO/IEC 9797-1:1999] ■	ISO/IEC 9798-2: 2008-12-15 (3rd ed.)
message muthentication code (MAC) algorithm	algorithm for computing a function which maps strings of bits and a secret key to fixed-length strings of bits, satisfying the following two properties: - for any key and any input string, the function can be computed efficiently; - for any fixed key, and given no prior knowledge of the key, it is computationally infeasible to compute the function value on any new input string, even given knowledge of the set of input strings and corresponding function values, where the value of the *i*th input string may have been chosen after observing the value of the first *i*-1 function values (for integer *i* > 1) NOTE 1 A MAC algorithm is sometimes called a cryptographic check function (see for example ISO 7498-2 [1]). NOTE 2 Computational feasibility depends on the user's specific security requirements and environment. [ISO/IEC 9797-1] ■	ISO/IEC FDIS 9797-2: 2009-09-18

Term	Definition	ISO/IEC JTC 1/SC 27 Document
message authentication code (MAC) algorithm	algorithm for computing a function which maps strings of bits and a secret key to fixed-length strings of bits, satisfying the following two properties: - for any key and any input string the function can be computed efficiently - for any fixed key, and given no prior knowledge of the key, it is computationally infeasible to compute the function value on any new input string, even given knowledge of the set of input strings and corresponding function values, where the value of the ith input string may have been chosen after observing the value of the first i-1 function values NOTE 1 A MAC algorithm is sometimes called a cryptographic check function (see for example ISO 7498-2). NOTE 2 Computational feasibility depends on the user's specific security requirements and environment. [ISO/IEC 9797-1:1999, definition 3.2.6] ■	ISO/IEC 18014-2: 2009-12-15 (2nd ed.)
message authentication code (MAC) algorithm	algorithm for computing a function which maps strings of bits and a secret key to fixed-length strings of bits, satisfying the following two properties: 1) for any key and any input string the function can be computed efficiently; 2) for any fixed key, and given no prior knowledge of the key, it is computationally infeasible to compute the function value on any new input string, even given knowledge of the set of input strings and corresponding function values, where the value of the *i*-th input string may have been chosen after observing the value of the first *i*-1 function values ■	ISO/IEC 11770-3: 2008-07-15 (2nd ed.)
message authentication code (MAC) algorithm	algorithm for computing a function that maps strings of bits and a secret key to fixed-length strings of bits, satisfying the following two properties: - for any key and any input string the function can be computed efficiently; - for any fixed key, and given no prior knowledge of the key, it is computationally infeasible to compute the function value on any new input string, even given knowledge of the set of input strings and corresponding function values, where the value of the *i*th input string may have been chosen after observing the value of the first *i* - 1 function values NOTE 1 A MAC algorithm is sometimes called a cryptographic check function (see for example ISO 7498-2). NOTE 2 Computational feasibility depends on the user's specific security requirements and environment. [ISO/IEC 9797-1] ■	ISO/IEC 13888-1: 2009-07-15 (3rd ed)

Term	Definition	ISO/IEC JTC 1/SC 27 Document
message authentication code (MAC) algorithm	algorithm for computing a function which maps strings of bits and a secret key to fixed-length strings of bits, satisfying the following properties: - for any key and any input string the function can be computed efficiently; - for any fixed key, and given no prior knowledge of the key, it is computationally infeasible to compute the function value on any new input string, even given knowledge of the set of input strings and corresponding function values, where the value of the *i*th input string may have been chosen after observing the value of the first *i*-1 function values. [ISO/IEC 9797-1] ■	ISO/IEC FDIS 9798-6: 2010-08-05
message authentication code (MAC) algorithm	algorithm for computing a function which maps strings of bits and a secret key to fixed-length strings of bits, satisfying the following two properties: - for any key and any input string, the function can be computed efficiently; - for any fixed key, and given no prior knowledge of the key, it is computationally infeasible to compute the function value on any new input string, even given knowledge of a set of input strings and corresponding function values, where the value of the *i*th input string may have been chosen after observing the value of the first *i*-1 function values (for integers $i > 1$) NOTE 1 A MAC algorithm is sometimes called a cryptographic check function (see for example ISO 7498-2 [1]). NOTE 2 Computational feasibility depends on the user's specific security requirements and environment. ■	N8861: PreFDIS 9797-1: 2010-09-03
message representative	bit string derived as a function of the message and which is combined with the private signature key to yield the signature ■	ISO/IEC FDIS 9796-2: 2010-09-10
method	a way of performing something according to a plan to obtain reproducible results in a systematic and traceable manner ■	ISO/IEC TR 15443-3: 2007-12-15 (1st ed.)
methodology	collection of standards, procedures and supporting methods that define the complete approach to the development of a product or system ■	ISO/IEC 21827: 2008-10-15 (2nd ed.)
methodology	system of principles, procedures and processes applied to IT security evaluations ■	N8912: Corrected 18045: 2010-09-15
metric	quantitative scale and method, which can be used for measurement ■	ISO/IEC TR 15443-3: 2007-12-15 (1st ed.)
microcode	processor instructions that correspond to an executable program instruction EXAMPLE Assembler code ■	N8776: 2nd WD 19790: 2010-07-16

Term	Definition	ISO/IEC JTC 1/SC 27 Document
min-entropy	lower bound of entropy that is useful in determining a worst-case estimate of sampled entropy NOTE The bit string *X* (or more precisely, the corresponding random variable that models random bit strings of this type) has min-entropy *k* if k is the largest value such that **Pr** [*X* = *x*] ≤ 2^{-k}. That is, *X* contains *k* bits of min-entropy or randomness. ■	N8745: FCD 18031: 2010-05-18
minimal disclosure	principle of identity management (3.4.1) to restrict the transfer of identity information (3.2.5) to the minimal number of attributes strictly required for a particular purpose ■	N8804: 3rd CD 24760-1: 2010-06-11
minimum business continuity objective MBCO	minimum level of services and/or products that is acceptable to the organization to achieve its business objectives during a disruption ■	N8622: PreFDIS 27031: 2010-08-18
minimum entropy	a lower bound of entropy that is useful in determining a worst-case estimate of sample entropy ■	N8776: 2nd WD 19790: 2010-07-16
modem	hardware or software that modulates digital signals into analogue ones and vice versa (demodulation) for the purpose of using telephone protocols as a computer protocol. ■	ISO/IEC 18028-4: 2005-04-01 (1st ed.)
modifiable operational environment	an operational environment that is designed to accept functional changes that may contain non-controlled software (i.e. untrusted) ■	N8776: 2nd WD 19790: 2010-07-16
modular decomposition	process of breaking a system into components to facilitate design, development and evaluation [IEEE Std 610.12-1990] ■	ISO/IEC 15408-1: 2009-12-15 (3rd ed.)
modulus	a parameter which is a positive integer and a product of two distinct prime numbers ■	ISO/IEC 10118-4: 1998-12-15 (1st ed.)
modulus	Integer used as a divisor of an integer dividend in order to obtain an integer remainder. ■	ISO/IEC 7064: 2003-02-15 (2nd ed.)
modulus	integer whose factorization shall be kept secret and whose factors shall be infeasible to compute ■	ISO/IEC 14888-2: 2008-04-15 (2nd ed.)
monitoring attacks	generic category of attack methods that includes passive analysis techniques aiming at disclosure of sensitive internal data of the TOE by operating the TOE in the way that corresponds to the guidance documents ■	ISO/IEC 15408-1: 2009-12-15 (3rd ed.)
monitoring authority monitor	trusted third party monitoring actions and events, and that is trusted to provide evidence about what has been monitored ■	ISO/IEC 13888-1: 2009-07-15 (3rd ed)

Term	Definition	ISO/IEC JTC 1/SC 27 Document
multi protocol label switching - MPLS	technique, developed for use in inter-network routing, whereby labels are assigned to individual data paths or flows, and used to switch connections, underneath and in addition to normal routing protocol mechanisms NOTE Label switching can be used as one method of creating tunnels. ■	ISO/IEC 27033-1: 2009-12-15 (1st ed.)
multi-factor authentication	authentication with at least two independent authentication factors. An authentication factor is a piece of information and process used to authenticate or verify the identity of a entity. Independent authentication factor categories are: something you know, something you have, and something you are ■	N8776: 2nd WD 19790: 2010-07-16
multiple-chip embedded cryptographic module	physical embodiment in which two or more integrated circuit chips are interconnected and are embedded within an enclosure or a product that may not be physically protected EXAMPLE Adapters and expansion boards ■	N8776: 2nd WD 19790: 2010-07-16
multiple-chip standalone cryptographic module	physical embodiment in which two or more integrated circuit chips are interconnected and the entire enclosure is physically protected EXAMPLE Encrypting routers or secure radios ■	N8776: 2nd WD 19790: 2010-07-16
Multipurpose Internet Mail Extensions - MIME	method allowing the transfer of multimedia and binary data via email; it is specified in RFC 2045 to RFC 2049. ■	ISO/IEC 18028-4: 2005-04-01 (1st ed.)
mutual authentication	entity authentication that provides both entities with assurance of each other's identity [ISO/IEC 9798-1:1997, definition 3.3.14] ■	ISO/IEC 9798-5: 2009-12-15 (3rd ed.)
mutual authentication	entity authentication which provides both entities with assurance of each other's identity ■	ISO/IEC 9798-1: 2010-07-01 (3rd ed.)
mutual authentication	entity authentication which provides both entities with assurance of each other's identity [ISO/IEC 9798-1] ■	N8762: 1st WD 20009-1: 2010-07-13
mutual authentication	entity authentication which provides both entities with assurance of each other's identity ■	N8810: 1st CD 29115 | X.eaa: 2010-06-10
mutual entity authentication	entity authentication which provides both entities with assurance of each other's identity ■	ISO/IEC 11770-3: 2008-07-15 (2nd ed.)
mutual forward secrecy	property that knowledge of both entity *A*'s and entity *B*'s long-term private keys subsequent to a key agreement operation does not enable an opponent to recompute previously derived keys ■	ISO/IEC 11770-3: 2008-07-15 (2nd ed.)
mutual key authentication	assurance for two entities that only the other entity can possibly be in possession of the correct key ■	ISO/IEC 11770-4: 2006-05-01 (1st ed.)

Term	Definition	ISO/IEC JTC 1/SC 27 Document
***n*-bit block cipher**	block cipher with the property that plaintext blocks and ciphertext blocks are *n* bits in length. ■	ISO/IEC 10116: 2006-02-01 (3rd ed.)
***n*-bit block cipher**	block cipher with the property that plaintext blocks and ciphertext blocks are *n* bits in length [ISO/IEC 18033-3:2005] ■	ISO/IEC FDIS 10118-2: 2010-03-10
***n*-bit block cipher**	block cipher with the property that plaintext blocks and ciphertext blocks are n bits in length [ISO/IEC 10116:1997]. ■	ISO/IEC 18033-1: 2005-02-01 (1st ed.)
***n*-bit block cipher**	block cipher with the property that plaintext blocks and ciphertext blocks are *n* bits in length [ISO/IEC 10116:2006] ■	N8755: 1st CD 29192-2: 2010-06-22
***n*-bit block cipher**	block cipher with the property that plaintext blocks and ciphertext blocks are *n* bits in length [ISO/IEC 10116:1997] ■	N8749: 2nd CD 18033-4: 2010-05-19
***n*-bit block cipher**	block cipher with the property that plaintext blocks and ciphertext blocks are *n* bits in length [ISO/IEC 10116:2006] ■	N8751: FCD 29150: 2010-06-10
***n*-bit block cipher**	block cipher with the property that plaintext blocks and ciphertext blocks are *n* bits in length [ISO/IEC 10116:2006] ■	ISO/IEC FDIS 18033-3: 2010-07-12
***n*-bit block cipher**	block cipher with the property that plaintext blocks and ciphertext blocks are *n* bits in length [ISO/IEC 10116] 3.12 output transformation function that is applied at the end of the MAC algorithm, before the truncation operation ■	N8861: PreFDIS 9797-1: 2010-09-03
nearly prime number	positive integer $n = m \cdot r$, where m is a large prime number and r is a small smooth integer NOTE The meaning of the terms large and small prime numbers is dependent on the application, and is based on bounds determined by the designer. ■	ISO/IEC 15946-5: 2009-12-15 (1st ed.)
Network Access Server - NAS	a system, normally a computer, which provides access to an infrastructure for remote clients. ■	ISO/IEC 18028-4: 2005-04-01 (1st ed.)
network administration	day-to-day operation and management of network processes, and assets using networks ■	ISO/IEC 27033-1: 2009-12-15 (1st ed.)
network analyzer	device or software used to observe and analyze information flowing in networks NOTE Prior to the information flow analysis, information should be gathered in a specific way such as by using a network sniffer. ■	ISO/IEC 27033-1: 2009-12-15 (1st ed.)
network element	information system that is connected to a network ■	ISO/IEC 27033-1: 2009-12-15 (1st ed.)
network management	process of planning, designing, implementing, operating, monitoring and maintaining a network ■	ISO/IEC 27033-1: 2009-12-15 (1st ed.)
network monitoring	process of continuously observing and reviewing data recorded on network activity and operations, including audit logs and alerts, and related analysis ■	ISO/IEC 27033-1: 2009-12-15 (1st ed.)

Term	Definition	ISO/IEC JTC 1/SC 27 Document
network security policy	set of statements, rules and practices that explain an organization's approach to the use of its network resources, and specify how its network infrastructure and services should be protected ■	ISO/IEC 27033-1: 2009-12-15 (1st ed.)
network sniffer	device or software used to capture information flowing in networks ■	ISO/IEC 27033-1: 2009-12-15 (1st ed.)
next-state function	function that takes as input the current state of the keystream generator and (optionally) part of the previously output ciphertext, and gives as output a new state for the keystream generator ■	N8749: 2nd CD 18033-4: 2010-05-19
next-state function	function that takes as input the current state of the keystream generator and (optionally) part of the previously output ciphertext, and gives as output a new state for the keystream generator ■	N8757: 2nd WD 29192-3: 2010-07-01
nibble	block of four consecutive bits (half an octet) ■	ISO/IEC FDIS 9796-2: 2010-09-10
non-administrator guidance	written material that is used by the User and/or other non-administrative roles for operating the cryptographic module in an approved mode of operation. The non-administrator guidance describes the security functions of the cryptographic module and contains information and procedures for the secure use of the cryptographic module, including instructions, guidelines, and warnings ■	N8776: 2nd WD 19790: 2010-07-16
non-bypassability	<of the TSF> security architecture property whereby all SFR-related actions are mediated by the TSF ■	ISO/IEC 15408-1: 2009-12-15 (3rd ed.)
nonce	number used once ■	N8734: 3rd CD 9797-3: 2010-06-16
non-conformity	non-fulfilment of a requirement [ISO 9000:2005] ■	N8718: 1st WD 27000: 2010-05-27
non-deterministic random bit generator - NRBG	RBG whose security depends upon sampling an entropy source NOTE The entropy source shall be sampled whenever the RBG produces output, and possibly more often. ■	N8745: FCD 18031: 2010-05-18
non-disclosure of communications	properties of communications being handled by the persons engaged in the telecommunications organization should not be disclosed in terms of the existence, the content, the source, the destination and the date and time of communicated information. {ITU-T format} ■	ISO/IEC 27011/x.1051: 2008-12-15 (1st ed)
non-invasive attack	attack that can be performed on a cryptographic module without direct physical contact with components within the cryptographic boundary of the module. An attack that does not alter or change the state of the cryptographic module ■	N8776: 2nd WD 19790: 2010-07-16
non-match	decision that the recognition biometric sample(s) and the biometric reference template are not from the same individual ■	ISO/IEC 24761: 2009-05-15 (1st ed.)
non-modifiable operational environment	operational environment that is designed to not accept functional changes ■	N8776: 2nd WD 19790: 2010-07-16

Term	Definition	ISO/IEC JTC 1/SC 27 Document
non-recoverable part	part of the message stored or transmitted along with the signature; empty when message recovery is total ■	ISO/IEC FDIS 9796-2: 2010-09-10
non-repudiation	ability to prove the occurrence of a claimed event (2.18) or action and its originating entities ■	N8718: 1st WD 27000: 2010-05-27
non-repudiation	ability to prove an action or event has taken place, so that this event or action cannot be repudiated later [ISO/IEC 7498-2:1989] ■	N8642: 2nd PDTR 29149: 2010-06-22
Non-repudiation	security objective aimed at preventing the denial of previous commitments or actions. ■	N8810: 1st CD 29115 | X.eaa: 2010-06-10
non-repudiation exchange	sequence of one or more transfers of non-repudiation information (NRI) for the purpose of non-repudiation ■	ISO/IEC 13888-1: 2009-07-15 (3rd ed)
non-repudiation information	set of information that may contain information about an event or action for which evidence is to be generated and verified, the evidence itself, and the non-repudiation policy in effect ■	ISO/IEC 13888-1: 2009-07-15 (3rd ed)
non-repudiation of creation	service intended to protect against an entity's false denial of having created the content of a message (i.e. being responsible for the content of a message) ■	ISO/IEC 13888-1: 2009-07-15 (3rd ed)
non-repudiation of creation	Protection against an entity's false denial of having created the content of a message (i.e. being responsible for the content of a message). ■	ISO/IEC 15945: 2002-02-01 (1st ed.)
non-repudiation of delivery	service intended to protect against a recipient's false denial of having received a message and recognised the content of a message ■	ISO/IEC 13888-1: 2009-07-15 (3rd ed)
non-repudiation of delivery token	data item which allows the originator to establish non-repudiation of delivery for a message ■	ISO/IEC 13888-1: 2009-07-15 (3rd ed)
non-repudiation of knowledge	service intended to protect against a recipient's false denial of having taken notice of the content of a received message ■	ISO/IEC 13888-1: 2009-07-15 (3rd ed)
non-repudiation of origin	service intended to protect against the originator's false denial of having created the content of a message and of having sent a message ■	ISO/IEC 13888-1: 2009-07-15 (3rd ed)
non-repudiation of origin token	data item which allows recipients to establish non-repudiation of origin for a message ■	ISO/IEC 13888-1: 2009-07-15 (3rd ed)
non-repudiation of receipt	service intended to protect against a recipient's false denial of having received a message ■	ISO/IEC 13888-1: 2009-07-15 (3rd ed)
non-repudiation of sending	service intended to protect against the sender's false denial of having sent a message ■	ISO/IEC 13888-1: 2009-07-15 (3rd ed)
non-repudiation of submission	service intended to provide evidence that a delivery authority has accepted a message for transmission ■	ISO/IEC 13888-1: 2009-07-15 (3rd ed)

Term	Definition	ISO/IEC JTC 1/SC 27 Document
non-repudiation of submission token	data item which allows either the originator (sender) or the delivery authority to establish non-repudiation of submission for a message having been submitted for transmission ■	ISO/IEC 13888-1: 2009-07-15 (3rd ed)
non-repudiation of transport	service intended to provide evidence for the message originator that a delivery authority has delivered a message to the intended recipient ■	ISO/IEC 13888-1: 2009-07-15 (3rd ed)
non-repudiation of transport token	data item which allows either the originator or the delivery authority to establish non-repudiation of transport for a message ■	ISO/IEC 13888-1: 2009-07-15 (3rd ed)
non-repudiation policy	set of criteria for the provision of non-repudiation services NOTE More specifically, a set of rules to be applied for the generation and verification of evidence and for adjudication. ■	ISO/IEC 13888-1: 2009-07-15 (3rd ed)
non-repudiation service requester	entity that requests that non-repudiation evidence be generated for a particular event or action ■	ISO/IEC 13888-1: 2009-07-15 (3rd ed)
non-repudiation token	special type of security token as defined in ISO/IEC 10181-1, consisting of evidence, and, optionally, of additional data ■	ISO/IEC 13888-1: 2009-07-15 (3rd ed)
non-repudiation token	special type of security token as defined in ISO/IEC 10181-1, consisting of evidence, and, optionally, of additional data [ISO/IEC 13888-1:2009] ■	N8642: 2nd PDTR 29149: 2010-06-22
non-security relevant	requirements that are not addressed within the scope of this standard ■	N8776: 2nd WD 19790: 2010-07-16
normal mode of operation	the mode where the entire set of algorithms, security functions, services or processes are available and/or configurable ■	N8776: 2nd WD 19790: 2010-07-16
notarization	provision of evidence by a notary about the properties of the entities involved in an action or event, and of the data stored or communicated ■	ISO/IEC 13888-1: 2009-07-15 (3rd ed)
notarization token	non-repudiation token generated by a notary ■	ISO/IEC 13888-1: 2009-07-15 (3rd ed)
notary authority	trusted third party trusted to provide evidence about the properties of the entities involved and of the data stored or communicated, or to extend the lifetime of an existing token beyond its expiry or beyond subsequent revocation ■	ISO/IEC 13888-1: 2009-07-15 (3rd ed)
number	natural number, i.e. a non-negative integer ■	ISO/IEC 9798-5: 2009-12-15 (3rd ed.)
object	item characterized through the measurement of its attributes ■	ISO/IEC 27004: 2009-12-15 (1st ed.)
object	passive entity in the TOE, that contains or receives information, and upon which subjects perform operations ■	ISO/IEC 15408-1: 2009-12-15 (3rd ed.)

Term	Definition	ISO/IEC JTC 1/SC 27 Document
object	entity that contains or receives information. The objects can represent information containers (e.g., files or directories in an operating system, and/or columns, rows, tables, and views within a database management system), or objects can represent exhaustible system resources, such as printers, disk space, and CPU cycles. The set of objects covered by RBAC includes all of the objects listed in the permissions that are assigned to roles. [ANSI-RBAC] ■	N8812: 3rd WD 29146: 2010-07-14
object identifier OID	a value (distinguishable from all other such values) which is associated with an object [ITU X.680:2002} ■	N8642: 2nd PDTR 29149: 2010-06-22
observation report	report written by the evaluator requesting a clarification or identifying a problem during the evaluation ■	N8912: Corrected 18045: 2010-09-15
octet	string of eight bits ■	ISO/IEC FDIS 9796-2: 2010-09-10
octet	a bit string of length 8 NOTE See Clause 5.2.2. ■	ISO/IEC 18033-2: 2006-05-01 (1st ed.)
octet string	sequence of octets NOTE 1 See Clause 5.2.2. NOTE 2 When appropriate, an octet string may be interpreted as a bit string, simply by concatenating all of the component octets. ■	ISO/IEC 18033-2: 2006-05-01 (1st ed.)
on-card matching	performing comparison and decision making on an integrated circuit card where the biometric reference template is retained on-card in order to enhance security and privacy NOTE 3 The term "matching" is deprecated and replaced with the term "comparison" in ISO/IEC JTC 1/SC 37 work. But the term "on card matching" is a term heavily used in ISO/IEC JTC 1/SC 17 work. So this term is used in this International Standard. ■	ISO/IEC 24761: 2009-05-15 (1st ed.)
One-time password - OTP	password only used once thus countering replay attacks. ■	ISO/IEC 18028-4: 2005-04-01 (1st ed.)
one-way function	function with the property that it is easy to compute the output for a given input but it is computationally infeasible to find for a given output an input which maps to this output [ISO/IEC 11770-3:1999]	ISO/IEC 11770-4: 2006-05-01 (1st ed.)
one-way function	function that is known to be "easy to compute but hard to invert" ■	N8743: 2nd CD 11770-5: 2010-07-29
one-way function	function with the property that it is easy to compute the output for a given input but it is computationally infeasible to find for a given output an input, which maps to this output [ISO/IEC 11770-3] ■	N8745: FCD 18031: 2010-05-18
one-way function	function with the property that it is easy to compute the output for a given input, but it is computationally infeasible to find for a given output an input which maps to this output ■	ISO/IEC 11770-3: 2008-07-15 (2nd ed.)

Term	Definition	ISO/IEC JTC 1/SC 27 Document
one-way function with trapdoor	function that is known to be "easy to compute but hard to invert" unless some secret information (trapdoor) is known ■	N8743: 2nd CD 11770-5: 2010-07-29
one-way hash function	function which maps strings of bits to fixed-length strings of bits, satisfying the following two properties: - for a given output, it is computationally infeasible to find an input which maps to this output; - for a given input, it is computationally infeasible to find a second input which maps to the same output [ISO/IEC 10118-1] ■	N8751: FCD 29150: 2010-06-10
online services	service which is implemented by hardware, software or a combination of them, and provided over a communication line or network NOTE The content being hosted can be of a proprietary nature EXAMPLE Search engines, online backup services, Internet-hosted email, and software as a service are considered to be online services ■	N8780: 1st CD 29147: 2010-06-10
opacity	protection of information that might be derived by observing network activities, such as deriving addresses of end-points in a voice-over-Internet-Protocol call NOTE Opacity recognizes the need to protect actions in addition to information. ■	ISO/IEC FDIS 27033-3: 2010-09-10
opaque	impenetrable by light (i.e., light within the visible spectrum of wavelength range of 400nm to 750nm); neither transparent nor translucent within the visible spectrum ■	N8776: 2nd WD 19790: 2010-07-16
operation	<on a component of ISO/IEC 15408> modification or repetition of a component NOTE Allowed operations on components are assignment, iteration, refinement and selection. ■	ISO/IEC 15408-1: 2009-12-15 (3rd ed.)
operation	<on an object> specific type of action performed by a subject on an object ■	ISO/IEC 15408-1: 2009-12-15 (3rd ed.)
operation	usage phase of the TOE including "normal usage", administration and maintenance of the TOE after delivery and preparation ■	ISO/IEC 15408-1: 2009-12-15 (3rd ed.)
operation	executable image of a program, which upon invocation executes some function for the user. Within a file system, operations might include read, write, and execute. Within a database management system, operations might include insert, delete, append, and update. An operation is also known as a privilege. [ANSI-RBAC] ■	N8812: 3rd WD 29146: 2010-07-14
operational controls	security controls (i.e., safeguards and countermeasures) for an information system that primarily are implemented and executed by people (as opposed to systems) [NIST SP 800-53] ■	ISO/IEC TR 19791: 2010-04-01 (2nd ed.)

Term	Definition	ISO/IEC JTC 1/SC 27 Document
operational environment	environment in which the TOE is operated ■	ISO/IEC 15408-1: 2009-12-15 (3rd ed.)
operational environment	set of all software and hardware consisting of an operating system and hardware platform required for the module to operate securely ■	N8776: 2nd WD 19790: 2010-07-16
operational state	the state where services or functions can be requested by an operator and the data results outputted from the cryptographic module's data output interface ■	N8776: 2nd WD 19790: 2010-07-16
operational system	information system, including its non-IT aspects, considered in the context of its operating environment ■	ISO/IEC TR 19791: 2010-04-01 (2nd ed.)
operator	individual or organization that performs the operations of a product or online service NOTE 1 Adapted from ISO/IEC 12207:2008. NOTE 2 The role of operator and the role of user may be vested, simultaneously or sequentially, in the same individual or organization. ■	N8780: 1st CD 29147: 2010-06-10
operator	individual or a process (subject) operating on behalf of the individual, authorised to assume one or more roles ■	N8776: 2nd WD 19790: 2010-07-16
opt-in	process or type of policy whereby the PII principal is required to take a separate action to express specific, explicit, prior consent for a specific type of processing NOTE PII (and an associated opt-in) could also be collected by a PII processor acting on behalf of a PII controller. ■	N8806: 4th CD 29100: 2010-06-10
opt-out	process or type of policy whereby the PII principal is required to take a separate action in order to withhold or withdraw consent for a specific type of processing NOTE In the case of opt-out, implied consent exists for the PII controller to process PII unless the individual explicitly denies or withdraws permission. Opt-out is also a process provided by a PII controller for a PII principal to deny or withdraw permission to perform a specific type of processing. ■	N8806: 4th CD 29100: 2010-06-10
order of an elliptic curve E(F)	number of points on an elliptic curve *E* defined over a finite field *F* ■	ISO/IEC 15946-5: 2009-12-15 (1st ed.)
organisation	group of people and facilities with an arrangement of responsibilities, authorities and relationships EXAMPLE Company, corporation, firm, enterprise, institution, charity, sole trader or association, or parts or combinations thereof. NOTE 1 The arrangement is generally orderly. NOTE 2 An organization can be public, private or not for profit. [ISO 9000:2005] ■	N8712: 3rd WD 27014: 2010-05-28

Term	Definition	ISO/IEC JTC 1/SC 27 Document
organization	company, corporation, firm, enterprise, authority or institution, or part or combination thereof, whether incorporated or not, public or private, that has its own functions and administration and is able to ensure that information security is exercised ■	ISO/IEC 27006: 2007-03-01 (1st ed.)
organization	group of people and facilities with an arrangement of responsibilities, authorities and relationships [ISO 9000:2005] NOTE 1 In the context of this International Standard, an individual is distinct from an organization. NOTE 2 In general, a government is also an organization. In the context of this International Standard, governments can be considered separately from other organizations for clarity. ■	N8624: 2nd CD 27032: 2010-06-15
organization normative framework	organization-wide framework containing a set of processes and elements that are normative inside the organization and relevant to application security ■	N8632: FCD 27034-1: 2010-05-27
organization normative framework committee	organization role responsible for maintaining and approving the application security-related components of the Organization Normative Framework ■	N8632: FCD 27034-1: 2010-05-27
organizational role	Organizational roles correspond to the hierarchical organization in a company in terms of internal structures. [Neumann/Strembeck] ■	N8812: 3rd WD 29146: 2010-07-14
organizational security policy	set of security rules, procedures, or guidelines for an organization NOTE A policy may pertain to a specific operational environment. ■	ISO/IEC 15408-1: 2009-12-15 (3rd ed.)
organizations	entities which utilize ICT DR services ■	ISO/IEC 24762: 2008-02-01 (1st ed.)
originator	entity that sends a message to the recipient or makes available a message for which non-repudiation services are to be provided ■	ISO/IEC 13888-1: 2009-07-15 (3rd ed)
output data	information or computed results produced by a cryptographic module ■	N8776: 2nd WD 19790: 2010-07-16
output function	output function that combines the keystream and the plaintext to produce the ciphertext NOTE This function is often bitwise XOR. ■	N8749: 2nd CD 18033-4: 2010-05-19
output generation function	function in a random bit generator that outputs bits that appear to be random ■	N8745: FCD 18031: 2010-05-18
output transformation	transformation or mapping of the output of the iteration stage to obtain the hash-code ■	ISO/IEC 10118-1: 2000-06-15 (2nd ed.)
output transformation	function that is applied at the end of the MAC algorithm, before the truncation operation [ISO/IEC 9797-1] ■	ISO/IEC FDIS 9797-2: 2009-09-18
outsourced service providers	external service providers of ICT DR services ■	ISO/IEC 24762: 2008-02-01 (1st ed.)

Term	Definition	ISO/IEC JTC 1/SC 27 Document
outsourcing	acquisition of services by an acquirer to perform activities required to support acquirer's business functions ■	N8638: 3rd WD 27036: 2010-08-13
outsourcing agreement	formal agreement between acquirer and supplier that documents conditions for delivery of services to be completed ■	N8638: 3rd WD 27036: 2010-08-13
overall verdict	pass or fail statement issued by an evaluator with respect to the result of an evaluation ■	N8912: Corrected 18045: 2010-09-15
oversight verdict	statement issued by an evaluation authority confirming or rejecting an overall verdict based on the results of evaluation oversight activities ■	N8912: Corrected 18045: 2010-09-15
package	reusable set of either functional or assurance components combined together to satisfy a set of identified security objectives (from ISO/IEC 15408-1) ■	ISO/IEC 15292: 2001-12-15 (1st ed.)
package	named set of either security functional or security assurance requirements NOTE An example of a package is "EAL 3". ■	ISO/IEC 15408-1: 2009-12-15 (3rd ed.)
padding	appending extra bits to a data string ■	ISO/IEC 10118-1: 2000-06-15 (2nd ed.)
padding	appending extra bits to a data string [ISO/IEC 10118-1] ■	ISO/IEC FDIS 9797-2: 2009-09-18
padding	appending extra bits to a data string [ISO/IEC 10118-1:2000] ■	N8749: 2nd CD 18033-4: 2010-05-19
padding	appending extra bits to a data string [ISO/IEC 10118-1: 2000] ■	N8757: 2nd WD 29192-3: 2010-07-01
pair multiplicity parameter	number of asymmetric pairs of numbers involved in one instance of an authentication mechanism ■	ISO/IEC 9798-5: 2009-12-15 (3rd ed.)
pairing	function which takes two elements, P and Q, from an elliptic curve cyclic group over a finite field, G_1, as input, and produces an element from another cyclic group over a finite field, G_2, as output, and which has the following two properties (where we assume that the cyclic groups G_1 and G_2 have order q, for some prime q, and for any two elements P, Q, the output of the pairing function is written as $<P, Q>$). - Bilinearity: If P, P_1, P_2, Q, Q_1, Q_2 are elements of G_1 and a is an integer satisfying $1 \leq a \leq q - 1$, then $<P_1 + P_2, Q> = <P_1, Q> * <P_2, Q>$, $<P, Q_1 + Q_2> = <P, Q_1> * <P, Q_2>$, and $<[a]P, Q> = <P, [a]Q> = <P, Q>^a$. - Non-degeneracy: If P is a non-identity element of G_1, $<P, P> \neq 1$. ■	ISO/IEC 14888-3: 2006-11-15 (2nd ed.)
parameter	integer or bit string or function [ISO/IEC 14888-1] ■	N8760: 1st WD 20008-1: 2010-06-14
parameter	integer or bit string or function [ISO/IEC 14888-1] ■	N8763: 1st WD 20009-2: 2010-06-20
parameter	integer or bit string or function ■	N8751: FCD 29150: 2010-06-10
parameter	integer, bit string or hash-function ■	ISO/IEC 14888-1: 2008-04-15 (2nd ed.)
parameter generation process	process which gives as its output domain parameter and user keys ■	ISO/IEC 9796-3: 2006-09-15 (2nd ed.)

Term	Definition	ISO/IEC JTC 1/SC 27 Document
parent node of node *v*	node on which node *v* hangs ■	N8743: 2nd CD 11770-5: 2010-07-29
Partially anonymous authentication	method of verifying the user's access privilege where user's identity information is not revealed in course of verification but an escrow agent can reveal the identity information. ■	N8816: 3rd WD 29191: 2010-06-01
partition	process of dividing a string of bits of arbitrary length into a sequence of blocks, where the length of each block shall be n bits, except for the final block which shall contain r bits, $0 < r \leq n$ ■	ISO/IEC 19772: 2009-02-15 (1st ed.)
passivation	effect of a reactive process in semiconductor junctions, surfaces or components and integrated circuits constructed to include means of detection and protection NOTE 1 Silicon dioxide and phosphorus glass are examples of passivation material. NOTE 2 Passivation can modify the behaviour of the circuit. Passivation material is technology dependent. ■	ISO/IEC 24759: 2008-07-01 (1st ed.)
passivation	a process in the construction of semiconductor devices in which junctions, surfaces of components and integrated circuits are afforded a means of protection against the modification of circuit behaviour EXAMPLE Silicon dioxide or phosphorus glass NOTE Passivation material is technology dependant ■	N8776: 2nd WD 19790: 2010-07-16
Passive mode - PASV mode	an FTP connection establishment mode. ■	ISO/IEC 18028-4: 2005-04-01 (1st ed.)
password	secret word, phrase, number or character sequence used for entity authentication, which is a memorized weak secret ■	ISO/IEC 11770-4: 2006-05-01 (1st ed.)
password	a string of characters used to authenticate an identity or to verify access authorisation EXAMPLE Letters, numbers, and other symbols ■	N8776: 2nd WD 19790: 2010-07-16
Password Authentication Protocol - PAP	an authentication protocol provided for PPP (RFC 1334). ■	ISO/IEC 18028-4: 2005-04-01 (1st ed.)
password verification data	process of establishing one or more shared secret keys between two entities using prior shared passwordbased information (which means that either both of them have the same shared password or one has the password and the other has password verification data) and neither of them can predetermine the values of the shared secret keys ■	ISO/IEC 11770-4: 2006-05-01 (1st ed.)
password-authenticated key agreement	key retrieval process where one entity *A* has a weak secret derived from a password, and the other entity *B* has a strong secret associated with *A*'s weak secret; these two entities, using their own secrets, negotiate a secret key which is retrievable by *A*, but not (necessarily) derivable by *B* ■	ISO/IEC 11770-4: 2006-05-01 (1st ed.)
password-authenticated key retrieval	key token which is derived from both a weak secret and a key token factor ■	ISO/IEC 11770-4: 2006-05-01 (1st ed.)
password-entangled key token	data that is used to verify an entity's knowledge of a specific password ■	ISO/IEC 11770-4: 2006-05-01 (1st ed.)

Term	Definition	ISO/IEC JTC 1/SC 27 Document
pedigree	Informal recognition of the vendor's consistent repeatability to provide deliverables that satisfy its security policy or to perform as claimed (pedigree is an environmental factor associated with the vendor or deliverable). ■	ISO/IEC TR 15443-1: 2005-02-01 (1st ed.)
penetration	unauthorized act of bypassing the security mechanisms of an Information System ■	ISO/IEC 18043: 2006-06-15 (1st ed.)
penetration profile	definition of the activities required to effect a penetration ■	ISO/IEC 21827: 2008-10-15 (2nd ed.)
perfect backward security	security condition in which a joining entity cannot obtain any former *shared secret keys* ■	N8743: 2nd CD 11770-5: 2010-07-29
perfect forward security	security condition in which a leaving entity cannot obtain any subsequent *shared secret keys* ■	N8743: 2nd CD 11770-5: 2010-07-29
periodic self-tests	a suite of pre-conditional and conditional self-tests executed either upon operator's request or repeated after a maximum operational time and in the conditions specified in the security policy ■	N8776: 2nd WD 19790: 2010-07-16
peripheral	device attached to a digital device in order to expand its functionality ■	N8640: 3rd WD 27037: 2010-05-31
Permission	Permission is an approval to perform an operation on one or more RBAC protected objects. [ANSI-RBAC] ■	N8812: 3rd WD 29146: 2010-07-14
Personal Digital Assistant - PDA	usually a handheld computer (palmtop computer). ■	ISO/IEC 18028-4: 2005-04-01 (1st ed.)
personal firewall	A software application running on a single machine, protecting network traffic into and out of that machine to permit or deny communications based on an end user-defined security policy. ■	N8630: 2nd WD 27033-4: 2010-06-16
personal identification number	secret number sequence used for entity authentication, which is a memorized weak secret ■	ISO/IEC FDIS 11770-1: 2010-07-26
personal identification number PIN	a numeric code used to authenticate an identity ■	N8776: 2nd WD 19790: 2010-07-16
personal information	Information about an individual which can be used to identify that individual. The specific information used for this identification will be that defined by national legislation. {ITU-T format} ■	ISO/IEC 27011/x.1051: 2008-12-15 (1st ed)
personal security environment (PSE)	Secure local storage for an entity's private key, the directly trusted CA key and possibly other data. Depending on the security policy of the entity or the system requirements, this may be, for example, a cryptographically protected file or a tamper resistant hardware token. ■	ISO/IEC 15945: 2002-02-01 (1st ed.)

Term	Definition	ISO/IEC JTC 1/SC 27 Document
personalization service	service of storing cryptographic information (especially private keys) to a PSE. NOTE The organizational and physical security measures for a service like this are not in the scope of this Recommendation | International Standard. For organizational measures, refer to ITU-T Rec. X.842 | ISO/IEC TR 14516 Guidelines on the use and management of Trusted Third Party services. ■	ISO/IEC 15945: 2002-02-01 (1st ed.)
Personally identifiable information - PII	information (a) that uniquely links to an person or (b) can be used to create a unique link, to, contact, or to locate the person to which this information pertains, or (c) from which identification or contact information of a person can be derived, or (d) that is linked with PII, including personal characteristics or preferences NOTE Adapted from ISO/IEC 29100 to conform to the definition of terms in this document. ■	N8804: 3rd CD 24760-1: 2010-06-11
personally identifiable information - PII	any information (a) that identifies or can be used to identify, contact, or locate the person to whom such information pertains, (b) from which identification or contact information of an individual person can be derived, or (c) that is or might be linked to a natural person directly or indirectly [ISO/IEC 29100 - Privacy framework] ■	N8802: FCD 24745: 2010-05-19
personally identifiable information - PII	any information (a) that identifies or can be used to identify, contact, or locate the person to whom such information pertains, (b) from which identification or contact information of an individual person can be derived, or (c) that is or might be directly or indirectly linked to a natural person. NOTE To determine whether a PII principal is identifiable, account should be taken of all the means which can reasonably be used by the entity holding the data, or by any other party, to identify that individual. ■	N8806: 4th CD 29100: 2010-06-10
Pharming	Attack aimed at redirecting a website's traffic to another, bogus website. ■	N8810: 1st CD 29115 | X.eaa: 2010-06-10
phishing	fraudulent process of attempting to acquire private or confidential information by masquerading as a trustworthy entity in an electronic communication ■	N8624: 2nd CD 27032: 2010-06-15
physical asset	asset that has a tangible or material existence NOTE Physical assets usually refer to cash, equipment, inventory and properties owned by the individual or organization. Software is considered an intangible asset, or a non-physical asset. ■	N8624: 2nd CD 27032: 2010-06-15
Physical Credential	credential comprised of a tangible object (e.g, a smart card). ■	N8810: 1st CD 29115 | X.eaa: 2010-06-10

Term	Definition	ISO/IEC JTC 1/SC 27 Document
physical protection	safeguarding of a cryptographic module, CSPs and PSPs using physical means ■	N8776: 2nd WD 19790: 2010-07-16
PII controller	entity (or entities) that determines the purposes and means for processing PII but does not include individual persons who use data for personal purposes NOTE A PII controller sometimes instructs others (e.g., PII processors) to process PII on its behalf while the responsibility for the processing remains with the PII controller. ■	N8806: 4th CD 29100: 2010-06-10
PII disclosure	release, transfer, access provisioning, or divulgation of PII in any form to a third party ■	N8806: 4th CD 29100: 2010-06-10
PII principal	individual person to whom the PII relates NOTE Depending on the jurisdiction and the particular data protection and privacy legislation, the concept of a 'PII principal' is also be defined as a 'PII owner', 'data owner', or 'data subject'. In some jurisdictions, the 'data owner' is the individual whose PII is processed by someone and who continues to hold ownership to his/her own PII. In other jurisdictions, the 'data owner' is not a PII principal but is a person or entity who received the right to process PII from an individual. ■	N8806: 4th CD 29100: 2010-06-10
PII processor	entity that processes PII on behalf of and in accordance with the instructions of a PII controller ■	N8806: 4th CD 29100: 2010-06-10
plaintext	unencrypted information. ■	ISO/IEC 10116: 2006-02-01 (3rd ed.)
plaintext	unenciphered information ■	ISO/IEC 9798-1: 2010-07-01 (3rd ed.)
plaintext	unencrypted information [ISO/IEC 10116:1997]. ■	ISO/IEC 18033-1: 2005-02-01 (1st ed.)
plaintext	unencrypted information [ISO/IEC 10116:1997] ■	ISO/IEC 18033-2: 2006-05-01 (1st ed.)
plaintext	unencrypted information [ISO/IEC 10116] ■	ISO/IEC 19772: 2009-02-15 (1st ed.)
plaintext	unenciphered information [ISO/IEC 9797-1:1999] ■	N8755: 1st CD 29192-2: 2010-06-22
plaintext	unenciphered information [ISO/IEC 9797-1:1999] ■	N8749: 2nd CD 18033-4: 2010-05-19
plaintext	unenciphered information [ISO/IEC 9797-1: 1999] ■	N8757: 2nd WD 29192-3: 2010-07-01
plaintext	unencrypted information [ISO/IEC 10116:2006] ■	N8751: FCD 29150: 2010-06-10
plaintext	unenciphered information [ISO/IEC 9797-1:1999] ■	ISO/IEC FDIS 18033-3: 2010-07-12
plaintext	unencrypted information [ISO/IEC 9798-1:2010] ■	N8861: PreFDIS 9797-1: 2010-09-03
plaintext key	an unencrypted cryptographic key or a cryptographic key obfuscated by non-approved methods which is considered unprotected ■	N8776: 2nd WD 19790: 2010-07-16

Term	Definition	ISO/IEC JTC 1/SC 27 Document
point-to-point key establishment	direct establishment of keys between entities, without involving a third party ■	ISO/IEC 11770-2: 2008-06-15 (2nd ed.)
Point-to-Point Protocol - PPP	a standard method for encapsulating network layer protocol information over point-to-point links (RFC 1334). ■	ISO/IEC 18028-4: 2005-04-01 (1st ed.)
policy	overall intention and direction as formally expressed by management ■	N8718: 1st WD 27000: 2010-05-27
policy	set of rules, an identifier for the rule-combining algorithm, and (optionally) a set of obligations. A policy may be a component of a policy set. [XACML] ■	N8812: 3rd WD 29146: 2010-07-14
port	physical/logical input or output point of a cryptographic module that provides access to the module ■	N8776: 2nd WD 19790: 2010-07-16
port	endpoint to a connection NOTE In the context of the Internet protocol a port is a logical channel endpoint of a TCP or UDP connection. Application protocols which are based on TCP or UDP have typically assigned default port numbers, e.g. port 80 for HTTP. ■	ISO/IEC 27033-1: 2009-12-15 (1st ed.)
Post Office Protocol v3 - POP3	email protocol defined in RFC 1939 which allows a mail client to retrieve email stored on the email server. ■	ISO/IEC 18028-4: 2005-04-01 (1st ed.)
potential vulnerability	suspected, but not confirmed, weakness NOTE Suspicion is by virtue of a postulated attack path to violate the SFRs. ■	ISO/IEC 15408-1: 2009-12-15 (3rd ed.)
potential vulnerability	suspected, but not confirmed, weakness NOTE Suspicion is by virtue of a postulated attack path to violate the SFRs. ■	N8784: 1st WD 20004: 2010-08-06
potentially unwanted software	deceptive software, including malicious software, and non-malicious software that exhibit the characteristics of deceptive software ■	N8624: 2nd CD 27032: 2010-06-15
power consumption	electrical power consumed by a circuit during operation ■	N8753: 1st CD 29192-1: 2010-06-22
prefix free representation	representation of a data element for which concatenation with any other data does not produce a valid representation ■	ISO/IEC 11770-3: 2008-07-15 (2nd ed.)
prefix free set	set S of bit/octet strings such that there do not exist strings $x \neq y \in S$ such that x is a prefix of y ■	ISO/IEC 18033-2: 2006-05-01 (1st ed.)
pre-operational self-test	test performed by a cryptographic module between the time a cryptographic module is powered on or instantiated (after being powered off, reset, rebooted, cold-start, power interruption, etc.) and transitions to the operational state ■	N8776: 2nd WD 19790: 2010-07-16
preparation	activity in the life-cycle phase of a product, comprising the customer's acceptance of the delivered TOE and its installation which may include such things as booting, initialization, start-up and progressing the TOE to a state ready for operation ■	ISO/IEC 15408-1: 2009-12-15 (3rd ed.)

Term	Definition	ISO/IEC JTC 1/SC 27 Document
pre-selection algorithm	algorithm to reduce the number of templates that need to be matched in an identification search of the enrolment database ■	ISO/IEC 19792: 2009-08-01 (1st ed.)
pre-selection error	<pre-selection algorithm> error that occurs when the corresponding enrolment template is not in the preselected subset of candidates when a sample from the same biometric characteristic on the same user is given NOTE In pre-selection that is based on building partitions/classes of users, pre-selection errors happen when the enrolment template and a subsequent sample from the same biometric characteristic on the same user are placed in different partitions. ■	ISO/IEC 19792: 2009-08-01 (1st ed.)
preservation	process to maintain and safeguard the integrity and/or original condition of the potential digital evidence ■	N8640: 3rd WD 27037: 2010-05-31
pre-signature	octet string computed in the signature generation process which is a function of the randomizer but which is independent of the message NOTE Adapted from ISO/IEC 14888-1:1998. ■	ISO/IEC 9796-3: 2006-09-15 (2nd ed.)
Pretty Good Privacy - PGP	publicly available encryption software program based on public key cryptography. The message formats are specified in RFC 1991 and RFC 2440. ■	ISO/IEC 18028-4: 2005-04-01 (1st ed.)
preventive action	action to eliminate the cause of a potential nonconformity or other undesirable potential situation [ISO 9000:2005] ■	N8718: 1st WD 27000: 2010-05-27
primality certificate	mathematical proof that a given number is indeed a prime. For small numbers primality is most efficiently proven by trial division. In these cases, the primality certificate may therefore be empty. ■	ISO/IEC 18032: 2005-01-15 (1st ed.)
prime number	positive integer greater than 1 which has no integer divisors other than 1 and itself ■	N8734: 3rd CD 9797-3: 2010-06-16
prime number **prime**	Integer $N > 1$ is prime if the only divisors of N are trivial divisors. ■	ISO/IEC 18032: 2005-01-15 (1st ed.)
primitive	function used to convert between data types ■	ISO/IEC 18033-2: 2006-05-01 (1st ed.)
principal	entity whose identity can be authenticated ■	ISO/IEC 9798-1: 2010-07-01 (3rd ed.)
Principal	entity whose identity can be authenticated. ■	N8810: 1st CD 29115 | X.eaa: 2010-06-10
priority call	telecommunications made by specific terminals in the event of emergencies, which should be handled with priority by restricting public calls. The specific terminals may span different services (VoIP, PSTN voice, IP data traffic, etc.) for wired and wireless networks. {ITU-T format} ■	ISO/IEC 27011/x.1051: 2008-12-15 (1st ed)
privacy breach	situation where PII is processed in an unlawful manner or in violation of one or more relevant privacy policies ■	N8806: 4th CD 29100: 2010-06-10

Term	Definition	ISO/IEC JTC 1/SC 27 Document
privacy control	technical and organisational measures aimed at mitigating risks that could result in privacy breaches NOTE 1 Privacy controls include policies, procedures, guidelines, practices or organizational structures, which can be administrative, technical, management, or legal in nature. NOTE 2 Control is also used as a synonym for safeguard or countermeasure. ■	N8806: 4th CD 29100: 2010-06-10
privacy enhancing technology - PET	coherent system of ICT measures that protect privacy by eliminating or reducing PII or by preventing unnecessary and/or undesired processing of PII; all without losing the functionality of the data system NOTE Examples of PETs include, but are not limited to, anonymization and pseudonymization tools that eliminate, reduce, mask, or de-identify PII or that prevent unnecessary, unauthorized and/or undesirable processing of PII. ■	N8806: 4th CD 29100: 2010-06-10
privacy policy	specification of objectives, rules, obligations and privacy controls with regard to the processing of PII in a particular setting ■	N8806: 4th CD 29100: 2010-06-10
privacy preferences	specific or implied choices made by an individual about how his/her PII should be processed ■	N8806: 4th CD 29100: 2010-06-10
privacy principles	set of shared values governing the privacy protection of the PII when processed in ICT systems ■	N8806: 4th CD 29100: 2010-06-10
privacy risk assessment	analysis of the risks of privacy breach involved in an envisaged processing operation NOTE This analysis, also known as privacy impact assessment, is achieved to (a) ensure processing conforms to applicable legal, regulatory, and policy requirements regarding privacy, (b) determine the risks and effects of processing PII, and (c) examine and evaluate privacy controls and alternative processes for handling PII to mitigate identified privacy risks. ■	N8806: 4th CD 29100: 2010-06-10
privacy safeguarding requirements	criteria to be fulfilled when implementing privacy controls designed to help mitigate risks of privacy breaches ■	N8806: 4th CD 29100: 2010-06-10
private	restricted to members of an authorized group: in the context of VPNs, it refers to the traffic flowing in a VPN connection ■	ISO/IEC 18028-5: 2006-07-01 (1st ed.)
Private Branch Exchange - PBX	usually a computer-based digital telephone switch for an enterprise. ■	ISO/IEC 18028-4: 2005-04-01 (1st ed.)
private decryption key	private key which defines the private decryption transformation ■	ISO/IEC 9798-1: 2010-07-01 (3rd ed.)

Term	Definition	ISO/IEC JTC 1/SC 27 Document
private key	key of an entity's asymmetric key pair which can only be used by that entity [ISO/IEC 11770-3] NOTE In the case of an asymmetric signature system, the private key defines the signature transformation. In the case of an asymmetric encipherment system, the private key defines the decipherment transformation. ■	ISO/IEC 13888-1: 2009-07-15 (3rd ed)
private key	data item of an asymmetric pair, that shall be kept secret and should only be used by a claimant in accordance with an appropriate response formula, thereby establishing its identity ■	ISO/IEC 9798-5: 2009-12-15 (3rd ed.)
private key	key of an entity's asymmetric key pair which should only be used by that entity [ISO/IEC 9798-1] ■	ISO/IEC FDIS 9796-2: 2010-09-10
private key	key of an entity's asymmetric key pair that is kept secret and which should only be used by that entity ■	ISO/IEC 9798-1: 2010-07-01 (3rd ed.)
private key	key of an entity's asymmetric key pair which should only be used by that entity [ISO/IEC 11770-1:1996] ■	ISO/IEC 18014-1: 2008-09-01 (2nd ed.)
private key	key of an entity's asymmetric key pair which should only be used by that entity [ISO/IEC 11770-1:1996]. NOTE A private key should not normally be disclosed. ■	ISO/IEC 18033-1: 2005-02-01 (1st ed.)
private key	key of an entity's asymmetric key pair which should only be used by that entity [ISO/IEC 11770-1:1996] NOTE See Clauses 7, 8.1. ■	ISO/IEC 18033-2: 2006-05-01 (1st ed.)
private key	key of an entity's asymmetric key pair which should only be used by that entity [ISO/IEC 9798-1:1997, definition 3.3.17] ■	ISO/IEC 18014-2: 2009-12-15 (2nd ed.)
private key	private data item of an asymmetric pair, that shall be kept secret and should only be used by a claimant in accordance with an appropriate response formula, thereby establishing its identity ■	N8759: 2nd WD 29192-4: 2010-06-15
private key	that key of a key pair associated with an entity's asymmetric cipher which shall be kept secret and used by that entity only [ISO/IEC 11770-1:1996] ■	N8751: FCD 29150: 2010-06-10
private key	key of an entity's asymmetric key pair that is kept private NOTE The security of an asymmetric system depends on the privacy of this key. ■	ISO/IEC FDIS 11770-1: 2010-07-26
private key	key of an entity's asymmetric key pair, which should only be used by that entity NOTE In the case of an asymmetric signature system the private key defines the signature transformation. In the case of an asymmetric encipherment system the private key defines the decipherment transformation ■	N8776: 2nd WD 19790: 2010-07-16

Term	Definition	ISO/IEC JTC 1/SC 27 Document
private key	key of an entity's asymmetric key pair which should only be used by that entity [ISO/IEC 9798-1:1997] ■	N8642: 2nd PDTR 29149: 2010-06-22
private key	key of an entity's asymmetric key pair which can only be used by that entity NOTE In the case of an asymmetric signature system, the private key defines the signature transformation. In the case of an asymmetric encipherment system, the private key defines the decipherment transformation. ■	ISO/IEC 11770-3: 2008-07-15 (2nd ed.)
private network	network that is subject to access controls which are intended to restrict use to members of an authorized group ■	ISO/IEC 18028-5: 2006-07-01 (1st ed.)
private signature key	data item specific to an entity and usable only by this entity in the signature generation process ■	ISO/IEC 9796-3: 2006-09-15 (2nd ed.)
private signature key	private key which defines the private signature transformation [ISO/IEC 9798-1] ■	ISO/IEC FDIS 9796-2: 2010-09-10
private signature key	private key which defines the private signature transformation NOTE This is sometimes referred to as a secret signature key. ■	ISO/IEC 9798-1: 2010-07-01 (3rd ed.)
procedure	specified way to carry out an activity or a process (2.40) [ISO 9000:2005] ■	N8718: 1st WD 27000: 2010-05-27
procedure	written description of a course of action to be taken to perform a given task [IEEE-Std. 610] ■	ISO/IEC 21827: 2008-10-15 (2nd ed.)
procedure parameter	transient public data item used in an instance of an authentication mechanism such as a witness, challenge or response ■	ISO/IEC 9798-5: 2009-12-15 (3rd ed.)
procedure parameter	transient public data item used in an instance of an authentication mechanism, e.g. a witness, challenge or response ■	N8759: 2nd WD 29192-4: 2010-06-15
process	set of interrelated or interacting activities which transforms inputs into outputs [ISO 9000:2005] ■	N8718: 1st WD 27000: 2010-05-27
process	set of interrelated activities which transform inputs into outputs NOTE Adapted from ISO/IEC 15288:2002. ■	ISO/IEC 21827: 2008-10-15 (2nd ed.)
process	An organised set of activities which uses resources to transform inputs to outputs [ISO 9000: 2000] ■	ISO/IEC TR 15443-1: 2005-02-01 (1st ed.)
PROCESS	Set of interrelated or interacting activities which transforms inputs into outputs [ISO 9000:2005] ■	N8732: 3rd WD 29193: 2010-08-06
process assurance	Assurance derived from an assessment of activities of a process. ■	ISO/IEC TR 15443-1: 2005-02-01 (1st ed.)
process capability	ability of a process to achieve a required goal ■	ISO/IEC TR 15443-3: 2007-12-15 (1st ed.)
processed biometric reference template	processed biometric sample or combination of processed biometric samples used as a biometric reference template ■	ISO/IEC 24761: 2009-05-15 (1st ed.)

Term	Definition	ISO/IEC JTC 1/SC 27 Document
processed biometric sample	biometric sample suitable for comparison ■	ISO/IEC 24761: 2009-05-15 (1st ed.)
processing of PII	any operation or set of operations performed upon PII NOTE Examples of processing operations of PII include, but are not limited to, the collection, storage, alteration, retrieval, consultation, disclosure, anonymization, pseudonymization, dissemination or otherwise making available, deletion or destruction of PII. ■	N8806: 4th CD 29100: 2010-06-10
product	IT security product, system, service NOTE 1 For the purpose of this part of ISO/IEC TR 15443, and similar to its usage in ISO 9000, the term product will be used in place of deliverable throughout the document. NOTE 2 The term product is synonymous with deliverable. ■	ISO/IEC TR 15443-3: 2007-12-15 (1st ed.)
product	system implemented or refined for sale or to be offered for free NOTE 1 In information technology, distinction is often made between hardware and software products, although the boundary is not always clear EXAMPLE A router can be seen as a hardware product even although is uses software ■	N8780: 1st CD 29147: 2010-06-10
PRODUCT	result of a process [ISO/IEC 9000:2005] A package of IT software, firmware and/or hardware, providing functionality designed for use or incorporation within a multiplicity of systems [ISO 15408-1] ■	N8732: 3rd WD 29193: 2010-08-06
product	result of a process [ISO 9000:2005] ■	N8632: FCD 27034-1: 2010-05-27
production	production life-cycle phase follows the development phase and consists of transforming the implementation representation into the implementation of the TOE, i.e. into a state acceptable for delivery to the customer NOTE 1 This phase may comprise manufacturing, integration, generation, internal transports, storage, and labelling of the TOE. NOTE 2 See also Figure 1. Figure 1 ? Terminology in CM and in the product life-cycle ■	ISO/IEC 15408-1: 2009-12-15 (3rd ed.)
production-grade	product, component or software that has been tested to meet operational specifications ■	N8776: 2nd WD 19790: 2010-07-16
profile	set of automatically generated data characterising a category of individuals that is intended to be applied to an individual, namely for the purpose of analysing or predicting personal preferences, behaviours and attitudes ■	N8806: 4th CD 29100: 2010-06-10
program code size	size of the program code in bytes ■	N8753: 1st CD 29192-1: 2010-06-22

Term	Definition	ISO/IEC JTC 1/SC 27 Document
proof	corroboration that evidence is valid in accordance with the non-repudiation policy in force NOTE Proof is evidence that serves to prove the truth or existence of something. ■	ISO/IEC 13888-1: 2009-07-15 (3rd ed)
Protection Profile	an implementation-independent set of security requirements for a category of IT products or systems that meet specific consumer needs (adapted from ISO/IEC 15408-1) ■	ISO/IEC 15292: 2001-12-15 (1st ed.)
Protection Profile	implementation-independent statement of security needs for a TOE type ■	ISO/IEC 15408-1: 2009-12-15 (3rd ed.)
Protection Profile	implementation-independent statement of security needs for a TOE type ■	N8784: 1st WD 20004: 2010-08-06
Protection Profile evaluation	assessment of a PP against defined criteria ■	ISO/IEC 15408-1: 2009-12-15 (3rd ed.)
protocol encapsulation	enveloping one data flow inside another by transporting protocol data units wrapped inside another protocol NOTE This is one method which can be used to establish tunnels in VPN technology. ■	ISO/IEC 18028-5: 2006-07-01 (1st ed.)
protocol model	specification of a protocol and its interaction under an adversarial model ■	N8778: 3rd CD 29128: 2010-06-11
protocol specification	all formal and informal descriptions of a specified protocol NOTE It includes all processes by each protocol participant, all communications between them and their order ■	N8778: 3rd CD 29128: 2010-06-11
prove	show correspondence by formal analysis in its mathematical sense NOTE It is completely rigorous in all ways. Typically, "prove" is used when there is a desire to show correspondence between two TSF representations at a high level of rigour. ■	ISO/IEC 15408-1: 2009-12-15 (3rd ed.)
provisioning	process of remotely searching for new software updates from a vendor's website and downloading authenticated updates ■	ISO/IEC 18043: 2006-06-15 (1st ed.)
pseudonym	identifier (3.1.4) that contains no PII (3.6.1) yet containing sufficient identity information (3.2.5) to allow a verifier (3.3.7) to link to a known identity (3.1.2) NOTE 1 A pseudonyms can be used to reduce privacy risks associated with the use of identifiers with fixed or known values. NOTE 2 A pseudonym can be an identifier with a value chosen by the person, or assigned randomly or a pseudonymous credential. ■	N8804: 3rd CD 24760-1: 2010-06-11

Term	Definition	ISO/IEC JTC 1/SC 27 Document
pseudonymization	process applied to PII which replaces identity information with an alias NOTE Pseudonymization allows, for example, a PII principal to use a resource or service without disclosing his or her identity, while still being held accountable for that use. After pseudonymization, it may still be possible to determine the PII principal's identity based on the alias and/or to link the PII principal's actions to one another and as a consequence, to the PII principal. ■	N8806: 4th CD 29100: 2010-06-10
pseudonymous identifier encoder - PIE	system, process or algorithm that generates a renewable biometric reference consisting of a pseudonymous identifier (PI) and possibly auxiliary data (AD) based on a biometric sample or biometric template ■	N8802: FCD 24745: 2010-05-19
pseudonymous identifier - PI	part of a renewable biometric reference that represents an individual or data subject within a certain domain by means of a protected identity that can be verified by means of a captured biometric sample and the auxiliary data (if any) NOTE 1 A pseudonymous identifier does not contain any information that allows retrieval of the original biometric sample, the original biometric features, or the true identity of its owner. NOTE 2 The pseudonymous identifier has no meaning outside the service domain. NOTE 3 Encrypted biometric data with a cipher that allows retrieval of the plain-text data is not a pseudonymous identifier. NOTE 4 A pseudonymous identifier is the element for comparison during biometric reference verification. NOTE 5 See Annex D, Table D.1 for concrete examples of instances for PI and AD. ■	N8802: FCD 24745: 2010-05-19
pseudo-random bit generator	Deterministic algorithm which when given some form of a bit sequence of length k outputs a sequence of bits of length $l > k$, computationally infeasible to distinguish from true random bits. ■	ISO/IEC 18032: 2005-01-15 (1st ed.)
pseudorandom sequence	sequence of bits or a number is pseudorandom if it appears to be selected at random even though the selection process is done by a deterministic algorithm ■	N8745: FCD 18031: 2010-05-18
public encryption key	public key which defines the public encryption transformation ■	ISO/IEC 9798-1: 2010-07-01 (3rd ed.)

Term	Definition	ISO/IEC JTC 1/SC 27 Document
public key	key of an entity's asymmetric key pair which can be made public [ISO/IEC 11770-3] NOTE In the case of an asymmetric signature scheme, the public key defines the verification transformation. In the case of an asymmetric encipherment system, the public key defines the encipherment transformation. A key that is 'publicly known' is not necessarily globally available. The key might only be available to all members of a pre-specified group. ■	ISO/IEC 13888-1: 2009-07-15 (3rd ed)
public key	data item of an asymmetric pair, that can be made public and shall be used by every verifier for establishing the claimant's identity ■	ISO/IEC 9798-5: 2009-12-15 (3rd ed.)
public key	key of an entity's asymmetric key pair which can be made public [ISO/IEC 9798-1] ■	ISO/IEC FDIS 9796-2: 2010-09-10
public key	key of an entity's asymmetric key pair which can be made public ■	ISO/IEC 9798-1: 2010-07-01 (3rd ed.)
public key	that key of an entity's asymmetric key pair which can be made public [ISO/IEC 11770-1:1996] ■	ISO/IEC 18014-1: 2008-09-01 (2nd ed.)
public key	that key of an entity's asymmetric key pair which can be made public [ISO/IEC 11770-1:1996]. ■	ISO/IEC 18033-1: 2005-02-01 (1st ed.)
public key	the key of an entity's asymmetric key pair which can be made public [ISO/IEC 11770-1:1996] NOTE See Clauses 7, 8.1. ■	ISO/IEC 18033-2: 2006-05-01 (1st ed.)
public key	that key of an entity's asymmetric key pair which can be made public NOTE In the case of an asymmetric signature scheme the public key defines the verification transformation. In the case of an asymmetric encipherment system the public key defines the encipherment transformation. A key that is 'publicly known' is not necessarily globally available. The key may only be available to all members of a pre-specified group. [ISO/IEC 11770-3:2008, definition 3.32] ■	ISO/IEC 18014-2: 2009-12-15 (2nd ed.)
public key	public data item of an asymmetric pair, that can be made public and shall be used by every verifier for establishing the claimant's identity ■	N8759: 2nd WD 29192-4: 2010-06-15
public key	that key of a key pair associated with an entity's asymmetric cipher which can be made public and used by any entity [ISO/IEC 11770-1:1996] ■	N8751: FCD 29150: 2010-06-10
public key	key of an entity's asymmetric key pair which can usually be made public without compromising security ■	ISO/IEC FDIS 11770-1: 2010-07-26

Term	Definition	ISO/IEC JTC 1/SC 27 Document
public key	that key of an entity's asymmetric key pair which can be made public [ISO/IEC 19790:2006, 3.56] NOTE In the case of an asymmetric signature system, the public key defines the verification transformation. In the case of an asymmetric encipherment system, the public key defines the encipherment transformation. A key that is “publicly known” is not necessarily globally available. The key may only be available to members of a pre-specified group. ■	ISO/IEC 24759: 2008-07-01 (1st ed.)
public key	that key of an entity's asymmetric key pair, which can be made public NOTE 1 In the case of an asymmetric signature system the public key defines the verification transformation. In the case of an asymmetric encipherment system the public key defines the encipherment transformation. A key that is 'publicly known' is not necessarily globally available. The key may only be available to all members of a pre-specified group NOTE2 For the purposes of this international standard, public keys are not considered CSPs ■	N8776: 2nd WD 19790: 2010-07-16
public key	that key of an entity's asymmetric key pair which can be made public NOTE In the case of an asymmetric signature scheme the public key defines the verification transformation. In the case of an asymmetric encipherment system the public key defines the encipherment transformation. A key that is 'publicly known' is not necessarily globally available. The key may only be available to all members of a pre-specified group. [ISO/IEC 11770-3:2008] ■	N8642: 2nd PDTR 29149: 2010-06-22
public key	key of an entity's asymmetric key pair which can be made public NOTE In the case of an asymmetric signature system, the public key defines the verification transformation. In the case of an asymmetric encipherment system, the public key defines the encipherment transformation. A key that is “publicly known” is not necessarily globally available. The key can be available only to all members of a pre-specified group. ■	ISO/IEC 11770-3: 2008-07-15 (2nd ed.)
public key (asymmetric) cryptographic algorithm	a cryptographic algorithm that uses two related keys, a public key and a private key. The two keys have the property that deriving the private key from the public key is computationally infeasible ■	N8776: 2nd WD 19790: 2010-07-16
public key certificate	public key information of an entity signed by the certification authority and thereby rendered unforgeable [ISO/IEC 11770-3] ■	ISO/IEC 13888-1: 2009-07-15 (3rd ed)

Term	Definition	ISO/IEC JTC 1/SC 27 Document
public key certificate	public key information of an entity signed by the certification authority and thereby rendered unforgeable [ISO/IEC 11770-1:1996] ■	ISO/IEC 18014-1: 2008-09-01 (2nd ed.)
public key certificate	public key information of an entity signed by the certification authority and thereby rendered unforgeable [ISO/IEC 11770-3:2008, definition 3.33] ■	ISO/IEC 18014-2: 2009-12-15 (2nd ed.)
public key certificate	public key information of an entity signed by the certification authority ■	ISO/IEC FDIS 11770-1: 2010-07-26
public key certificate	public key information of an entity signed by an appropriate certification authority and thereby rendered unforgeable ■	N8776: 2nd WD 19790: 2010-07-16
public key certificate	public key information of an entity signed by the certification authority and thereby rendered unforgeable [ISO/IEC 11770-3:2008] ■	N8642: 2nd PDTR 29149: 2010-06-22
public key certificate	public key information of an entity signed by the certification authority and thereby rendered unforgeable ■	ISO/IEC 11770-3: 2008-07-15 (2nd ed.)
public key certificate (certificate)	public key information of an entity signed by the certification authority and thereby rendered unforgeable NOTE See also Annex C. ■	ISO/IEC 9798-1: 2010-07-01 (3rd ed.)
public key directory - PKD	directory containing a well defined (sub)set of public key certificates. This directory can contain certificates from different Certification Authorities. ■	ISO/IEC 15945: 2002-02-01 (1st ed.)
public key information	information specific to a single entity and which contains at least the entity's distinguishing identifier and a public key for this entity NOTE Other information regarding the certification authority, the entity, and the public key may be included in the public key certificate, such as the validity period of the public key, the validity period of the associated private key, or the identifier of the involved algorithms (see also Annex C). ■	ISO/IEC 9798-1: 2010-07-01 (3rd ed.)
public key information	information containing at least the entity's distinguishing identifier and public key, but which can include other static information regarding the certification authority, the entity, restrictions on key usage, the validity period, or the involved algorithms [ISO/IEC 11770-3:2008] ■	ISO/IEC FDIS 11770-1: 2010-07-26
public key information	information containing at least the entity's distinguishing identifier and public key, but which can include other static information regarding the certification authority, the entity, restrictions on key usage, the validity period, or the involved algorithms ■	ISO/IEC 11770-3: 2008-07-15 (2nd ed.)

Term	Definition	ISO/IEC JTC 1/SC 27 Document
public key infrastructure - PKI	system consisting of TTPs, together with the services they make available to support the application (including generation and validation) of digital signatures, and of the persons or technical components, who use these services. NOTE Sometimes the persons and the technical components participating in a PKI, by using the services of TTPs, but not being TTPs themselves, are referred to as end entities. An example of a technical equipment used by an end entity is a smartcard which may be used as a storage and/or processing device. ■	ISO/IEC 15945: 2002-02-01 (1st ed.)
public key system	(digital signature) cryptographic scheme consisting of three functions: - key production, a method for generating a key pair made up of a private signature key and a public verification key; - signature production, a method for generating a signature Σ from a message representative F and a private signature key; - signature opening, a method for obtaining the recovered message representative F^* from a signature Σ and a public verification key NOTE The output of this function also contains an indication as to whether the signature opening procedure succeeded or failed. ■	ISO/IEC FDIS 9796-2: 2010-09-10
public security parameter - PSP	security related public information whose modification can compromise the security of a cryptographic module EXAMPLE Public cryptographic keys, public key certificates, self-signed certificates, trust anchors, one time passwords associated with a counter and internally held date and time ■	N8776: 2nd WD 19790: 2010-07-16
public verification key	data item which is mathematically related to a private signature key and is known by or accessible to all entities and which is used by the verifier in the signature verification process ■	ISO/IEC 9796-3: 2006-09-15 (2nd ed.)
public verification key	public key which defines the public verification transformation [ISO/IEC 9798-1] ■	ISO/IEC FDIS 9796-2: 2010-09-10
public verification key	public key which defines the public verification transformation ■	ISO/IEC 9798-1: 2010-07-01 (3rd ed.)
pure DRBG	DRBG whose entropy sources are seeds ■	N8745: FCD 18031: 2010-05-18
pure NRBG	(physical or non-physical) NRBG whose entropy sources are non-deterministic ■	N8745: FCD 18031: 2010-05-18
radix	Base of a geometric progression. ■	ISO/IEC 7064: 2003-02-15 (2nd ed.)
RAM size	size of temporary storage space a program requires in random access memory ■	N8753: 1st CD 29192-1: 2010-06-22
random bit generator - RBG	device or algorithm that outputs a sequence of bits that appears to be statistically independent and unbiased ■	N8745: FCD 18031: 2010-05-18

Term	Definition	ISO/IEC JTC 1/SC 27 Document
random bit generator - RBG	device or algorithm that outputs a sequence of bits that appears to be statistically independent and unbiased [ISO/IEC 19790:2006, 3.59] NOTE See ISO/IEC 18031:2005. ■	ISO/IEC 24759: 2008-07-01 (1st ed.)
random bit generator - RBG	device or algorithm that outputs a sequence of bits that appears to be statistically independent and unbiased ■	N8776: 2nd WD 19790: 2010-07-16
random element derivation function	function that utilizes a password and other parameters as input, and outputs a random element ■	ISO/IEC 11770-4: 2006-05-01 (1st ed.)
random number	time variant parameter whose value is unpredictable [ISO/IEC 9798-1:1997, definition 3.3.24] ■	ISO/IEC 9798-5: 2009-12-15 (3rd ed.)
random number	time variant parameter whose value is unpredictable (see also Annex B) ■	ISO/IEC 9798-1: 2010-07-01 (3rd ed.)
random number	time variant parameter whose value is unpredictable [ISO/IEC 9798-1] ■	N8762: 1st WD 20009-1: 2010-07-13
random number	time variant parameter whose value is unpredictable [ISO/IEC 9798-1] ■	N8763: 1st WD 20009-2: 2010-06-20
random number	time variant parameter, whose value is unpredictable ■	N8743: 2nd CD 11770-5: 2010-07-29
random number	time variant parameter whose value is unpredictable [ISO/IEC 9798-1:1997] ■	N8759: 2nd WD 29192-4: 2010-06-15
random number	time variant parameter whose value is unpredictable ■	ISO/IEC 11770-2: 2008-06-15 (2nd ed.)
random number, random bit	time variant parameter whose value is unpredictable ■	ISO/IEC FDIS 11770-1: 2010-07-26
randomized	dependent on a randomizer [ISO/IEC 14888-1] ■	ISO/IEC 9796-3: 2006-09-15 (2nd ed.)
randomizer	secret integer produced by the signing entity in the pre-signature production process, and not predictable by other entities NOTE Adapted from ISO/IEC 14888-1:1998. ■	ISO/IEC 9796-3: 2006-09-15 (2nd ed.)
raw biometric reference template	raw biometric sample or combination of raw biometric samples used as a biometric reference template ■	ISO/IEC 24761: 2009-05-15 (1st ed.)
raw biometric sample	biometric sample obtained directly from a biometric sensor ■	ISO/IEC 24761: 2009-05-15 (1st ed.)
recipient	entity that gets (receives or fetches) a message for which non-repudiation services are to be provided ■	ISO/IEC 13888-1: 2009-07-15 (3rd ed)
record	document stating results achieved or providing evidence of activities performed [ISO 9000:2005] ■	N8718: 1st WD 27000: 2010-05-27
record	retain a written description of procedures, events, observations, insights and results in sufficient detail to enable the work performed during the evaluation to be reconstructed at a later time ■	N8912: Corrected 18045: 2010-09-15
recoverable part	part of the message conveyed in the signature ■	ISO/IEC FDIS 9796-2: 2010-09-10
recovery point objective - RPO	point in time to which data must be recovered after a disruption has occurred ■	N8622: PreFDIS 27031: 2010-08-18

Term	Definition	ISO/IEC JTC 1/SC 27 Document
recovery time objective - RTO	period of time within which minimum levels of services and/or products and the supporting systems, applications, or functions must be recovered after a disruption has occurred ■	N8622: PreFDIS 27031: 2010-08-18
reduction-function	a function RED that is applied to the block H_q of length L_Φ to generate the hash-code H of length L_p ■	ISO/IEC 10118-4: 1998-12-15 (1st ed.)
redundancy	information that is known and can be checked ■	ISO/IEC 11770-2: 2008-06-15 (2nd ed.)
reference identifier - IR	identifier (3.1.4) in a domain (3.2.3) with a value that remains the same for the duration of the existence of the entity (3.1.1) and is not associated with another entity for a period specified in a policy after the entity ceases to exist NOTE A reference identifier persists at least for the existence of the entity in a domain and may exist longer than the entity, e.g. for archival purposes. EXAMPLE A driver license' number that stays the same for an individual drivers driving life is a persistent identifier that reference additional identity information and is an identity reference. An IP address is not an identifier reference as it can be assigned to other entities. ■	N8804: 3rd CD 24760-1: 2010-06-11
reference-identifier generator	tool used during enrolment (3.4.3) to provide a fresh unique value for an reference identifier (3.1.6) EXAMPLE A database management system can be the reference identifier generator when it assigns a unique record identifier to a new record being added to a table. ■	N8804: 3rd CD 24760-1: 2010-06-11
refinement	addition of details to a component ■	ISO/IEC 15408-1: 2009-12-15 (3rd ed.)
reflection attack	masquerade which involves sending a previously transmitted message back to its originator ■	ISO/IEC 9798-1: 2010-07-01 (3rd ed.)
register	set of files (electronic, or a combination of electronic and paper) containing entry labels and their associated definitions and related information ■	ISO/IEC 15292: 2001-12-15 (1st ed.)
register entry	information within a register relating to a specific PP or package ■	ISO/IEC 15292: 2001-12-15 (1st ed.)
registration	the process of assigning a register entry ■	ISO/IEC 15292: 2001-12-15 (1st ed.)
registration authority – RA	entity responsible for providing assured user identities to the certification authority ■	ISO/IEC FDIS 11770-1: 2010-07-26
registration authority – RA	trusted entity that establishes and vouches for the identity of a claimant to a CSP. The RA may be an integral part of a CSP, or it may be independent of a CSP, but it has a relationship with the CSP. ■	N8810: 1st CD 29115 | X.eaa: 2010-06-10

Term	Definition	ISO/IEC JTC 1/SC 27 Document
registration authority – RA	entity who is responsible for identification and authentication of subjects of certificates, but is not a CA or an AA, and hence does not sign or issue certificates. An RA may assist in the certificate application process, revocation process, or both. ■	ISO/IEC TR 14516: 2002-06-15 (1st ed.)
registration authority - RA	Authority entitled and trusted to perform the registration service as described below. ■	ISO/IEC 15945: 2002-02-01 (1st ed.)
registration service	The service of identifying entities and registering them in a way that allows the secure assignment of certificates to these entities. ■	ISO/IEC 15945: 2002-02-01 (1st ed.)
rekeying	process of updating and redistributing the *shared secret key*, and optionally, *key encryption keys* to satisfy security conditions NOTE This process is executed by the *key distribution centre*. ■	N8743: 2nd CD 11770-5: 2010-07-29
reliability	property of consistent intended behaviour and results ■	N8718: 1st WD 27000: 2010-05-27
reliability	property of consistent behaviour and results [ISO/IEC TR 13335-1:1996] ■	ISO/IEC 21827: 2008-10-15 (2nd ed.)
reliability	probability of failure-free (or otherwise satisfactory) software operation for a specified/expected period/interval of time, or for a specified/expected number of operations, in a specified/expected environment under specified/expected operating conditions. [IEEE Std 610.12-1990, ISO/IEC 9126, NIST SP 500-209] ■	N8732: 3rd WD 29193: 2010-08-06
reliability	property of consistent intended behavior and results [ISO/IEC 27000] ■	N8640: 3rd WD 27037: 2010-05-31
relying party	Entity that relies on an identity representation or claim by a claimant within some request context in order to authenticate or grant access to other entities based on identity information from a CSP. ■	N8810: 1st CD 29115 | X.eaa: 2010-06-10
relying party	entity (3.1.1) that relies on the validity of identity information (3.2.5) NOTE A relying party is exposed to risk caused by incorrect identity information. Typically it has a trust relationship with identity information authorities. ■	N8804: 3rd CD 24760-1: 2010-06-11
remediate	patch, fix, upgrade, configuration or documentation change to address a vulnerability NOTE A change intended to resolve or mitigate a vulnerability. An update typically takes the form of a configuration change, binary file replacement, hardware change, or source code patch, etc. Updates are usually provided by vendors. Vendor use different terms including patch, fix, hotfix, and upgrade. ■	N8780: 1st CD 29147: 2010-06-10

Term	Definition	ISO/IEC JTC 1/SC 27 Document
remote access	process of accessing network resources from another network, or from a terminal device which is not permanently connected, physically or logically, to the network it is accessing ■	ISO/IEC 27033-1: 2009-12-15 (1st ed.)
Remote access	authorized access to a system from outside of a security domain. ■	ISO/IEC 18028-4: 2005-04-01 (1st ed.)
Remote Access Dial-in User Service - RADIUS	an Internet Security protocol (RFC 2138 and RFC 2139) for authenticating remote users. ■	ISO/IEC 18028-4: 2005-04-01 (1st ed.)
Remote Access Service - RAS	usually hardware and software to provide remote access. ■	ISO/IEC 18028-4: 2005-04-01 (1st ed.)
remote attestation	processes of using digital certificates to ensure the identity as well as the hardware and software configuration of IDS and to securely transmit this information to a trusted operations center ■	ISO/IEC 18043: 2006-06-15 (1st ed.)
remote office and branch office	corporate offices externally connected to a WAN or a LAN using servers to provide branch users with services (e.g., file, print and the other service) required to maintain their daily business routine. ■	N8630: 2nd WD 27033-4: 2010-06-16
remote user	user at a site other than the one at which the network resources being used are located ■	ISO/IEC 27033-1: 2009-12-15 (1st ed.)
removable cover	physical means which permits access to the physical contents of a cryptographic module ■	N8776: 2nd WD 19790: 2010-07-16
renewability	generic ability to create multiple, independent transformed biometric references from one or more biometric samples obtained from the same data subject for the purposes of security and privacy enhancement ■	N8802: FCD 24745: 2010-05-19
renewable biometric reference	revocable / renewable identifier that represents an individual or data subject within a certain domain by means of a protected binary identity (re)constructed from the captured biometric sample ■	N8802: FCD 24745: 2010-05-19
repeatability	a process conducted to get the same test results on the same testing environment (same computer, hard disk, mode of operation, etc.) ■	N8640: 3rd WD 27037: 2010-05-31
replay attack	masquerade which involves use of previously transmitted messages ■	ISO/IEC 9798-1: 2010-07-01 (3rd ed.)
Replay Attack	masquerade which involves use of previously transmitted messages. ■	N8810: 1st CD 29115 | X.eaa: 2010-06-10
report	include evaluation results and supporting material in the Evaluation Technical Report or an Observation Report ■	N8912: Corrected 18045: 2010-09-15
representative	bit string produced by a format mechanism ■	ISO/IEC 14888-2: 2008-04-15 (2nd ed.)
reproducibility	process to get the same test results on a different testing environment (different computer, hard disk, operator, etc.) ■	N8640: 3rd WD 27037: 2010-05-31
Repudiation	denial of previous commitments or actions. ■	N8810: 1st CD 29115 | X.eaa: 2010-06-10

Term	Definition	ISO/IEC JTC 1/SC 27 Document
Request for Comment - RFC	title for Internet standards proposed by the IETF. ■	ISO/IEC 18028-4: 2005-04-01 (1st ed.)
reseeding	specialised internal state transition function which updates the internal state in the event that a new seed value is supplied NOTE The usage of the term 'reseeding' is not unique in the literature. Some authors denote each mechanism as 'reseeding' that replaces the current value of the internal state by a fresh value. This standard follows this terminology. However, often one distinguishes between 'reseeding' and 'seed update'. The term 'reseeding' then only comprises mechanisms that replace the internal state by a new value, which does not depend on the current value (essentially a new seeding process). In contrast 'seed update' denotes a mechanism that computes the new internal state from its current value and other (usually non-deterministic) data (cf. 9.6.3). ■	N8745: FCD 18031: 2010-05-18
residual risk	risk (2.45) remaining after risk treatment (2.58) ■	N8718: 1st WD 27000: 2010-05-27
residual risk	risk remaining after risk treatment NOTE 1 Residual risk can contain unidentified risk. NOTE 2 Residual risk can also be known as "retained risk". [ISO 31000:2009 ■	N8923: FCD 27005: 2010-06-02
residual risk	risk that remains after safeguards have been implemented [ISO/IEC TR 13335-1:1996] NOTE This definition differs from that used in ISO/IEC Guide 73. ■	ISO/IEC 21827: 2008-10-15 (2nd ed.)
residual risk	risk remaining after risk treatment ■	ISO/IEC TR 15443-3: 2007-12-15 (1st ed.)
residual risk	risk remaining after risk treatment [ISO/IEC Guide 73:2002] ■	ISO/IEC TR 19791: 2010-04-01 (2nd ed.)
residual vulnerability	weakness that cannot be exploited in the operational environment for the TOE, but that could be used to violate the SFRs by an attacker with greater attack potential than is anticipated in the operational environment for the TOE ■	ISO/IEC 15408-1: 2009-12-15 (3rd ed.)
residual vulnerability	weakness that cannot be exploited in the operational environment for the TOE, but that could be used to violate the SFRs by an attacker with greater attack potential than is anticipated in the operational environment for the TOE ■	N8784: 1st WD 20004: 2010-08-06
resilience	ability of an organization to resist being affected by disruptions ■	N8622: PreFDIS 27031: 2010-08-18
Resource	resource can be data, service, or system component. [XACML] ■	N8812: 3rd WD 29146: 2010-07-14
response	procedure parameter produced by the claimant, and processed by the verifier for checking the identity of the claimant ■	ISO/IEC 9798-5: 2009-12-15 (3rd ed.)

Term	Definition	ISO/IEC JTC 1/SC 27 Document
response	procedure parameter produced by the claimant, and processed by the verifier for checking the identity of the claimant ■	N8759: 2nd WD 29192-4: 2010-06-15
response (incident response or intrusion response)	actions taken to protect and restore the normal operational conditions of an Information System and the information stored in them when an attack or intrusion occurs ■	ISO/IEC 18043: 2006-06-15 (1st ed.)
retained role	optional role permitted by a crypto officer and assumed by an individual or a process (i.e., subject) acting on behalf of an individual allowing the retained role operator's authentication to be preserved over resetting, rebooting, or power cycling of the cryptographic module ■	N8776: 2nd WD 19790: 2010-07-16
retirement	withdrawal of active support by the operation and maintenance organization, partial or total replacement by a new system, or installation of an upgraded system ■	N8732: 3rd WD 29193: 2010-08-06
review	activity undertaken to determine the suitability, adequacy and effectiveness of the subject matter to achieve established objectives ■	N8718: 1st WD 27000: 2010-05-27
review objective	set of determination statements related to a particular control under review ■	N8706: 1st PDTR 27008: 2010-06-11
review objects	specific items being reviewed, e.g. specifications, mechanisms, activities, and individuals ■	N8706: 1st PDTR 27008: 2010-06-11
revocability	ability to prevent future successful verification of a specific biometric reference and the corresponding identity reference EXAMPLE Rejection of an entity may occur on the grounds of its appearance on a revocation list. ■	N8802: FCD 24745: 2010-05-19
revocation process	(to be considered) ■	N8760: 1st WD 20008-1: 2010-06-14
risk	effect of uncertainty on objectives [ISO Guide 73:2009] ■	N8718: 1st WD 27000: 2010-05-27
risk	potential that a given threat will exploit vulnerabilities of an asset or group of assets to cause loss or damage to the assets [ISO/IEC TR 13335-1:1996] NOTE This definition differs from that used in ISO/IEC Guide 73. ■	ISO/IEC 21827: 2008-10-15 (2nd ed.)
risk	potential that a given threat will exploit vulnerabilities of an asset or group of assets and thereby cause harm to the organization NOTE This definition is identical to that of 'information security risk' in ISO/IEC 27005:2008. ■	ISO/IEC TR 19791: 2010-04-01 (2nd ed.)
risk acceptance	informed decision to take a particular risk (2.45) [ISO Guide 73:2009] ■	N8718: 1st WD 27000: 2010-05-27
risk analysis	process to comprehend the nature of risk (2.45) and to determine the level of risk (2.31) [ISO Guide 73:2009] ■	N8718: 1st WD 27000: 2010-05-27

Term	Definition	ISO/IEC JTC 1/SC 27 Document
risk analysis	process to comprehend the nature of risk and to determine the level of risk NOTE 1 Risk analysis provides the basis for risk evaluation and decisions about risk treatment. NOTE 2 Risk analysis includes risk estimation. [ISO 31000:2009] ■	N8923: FCD 27005: 2010-06-02
risk analysis	process of identifying security risks, determining their magnitude and identifying areas needing safeguards [ISO/IEC TR 13335-1:1996] NOTE This definition differs from that used in ISO/IEC Guide 73. ■	ISO/IEC 21827: 2008-10-15 (2nd ed.)
risk analysis	systematic use of information to identify sources and to estimate the risk [ISO/IEC Guide 73:2002] ■	ISO/IEC TR 19791: 2010-04-01 (2nd ed.)
risk assessment	overall process (2.40) of risk identification (2.53), risk analysis (2.47) and risk evaluation (2.52) [ISO Guide 73:2009] ■	N8718: 1st WD 27000: 2010-05-27
risk assessment	overall process of risk identification, risk analysis and risk evaluation [ISO 31000:2009] ■	N8923: FCD 27005: 2010-06-02
risk assessment	overall process of risk analysis and risk evaluation [ISO/IEC Guide 73:2002, definition 3.3.1] NOTE 1 Risk evaluation is the process of comparing the estimated risk against given risk criteria to determine the significance of the risk. NOTE 2 For the purpose of this part of ISO/IEC TR 15443, risk assessment, risk analysis and threat-risk-analysis are summarily called risk assessment. ■	ISO/IEC TR 15443-3: 2007-12-15 (1st ed.)
risk assessment	overall process of risk analysis and risk evaluation [ISO/IEC Guide 73:2002] ■	ISO/IEC TR 19791: 2010-04-01 (2nd ed.)
risk avoidance	informed decision to not become involved in, or action to withdraw from, an activity in order not to be exposed to a particular risk (2.45) ■	N8718: 1st WD 27000: 2010-05-27
risk avoidance	informed decision not to become involved in, or action to withdraw from, an activity in order not to be exposed to a particular risk NOTE Risk avoidance can be based on the result of risk evaluation and/or legal and regulatory obligations. [ISO 31000:2009] ■	N8923: FCD 27005: 2010-06-02
risk communication	exchange or sharing of information about risk (2.45) between the decision-maker and other stakeholders (2.59) ■	N8718: 1st WD 27000: 2010-05-27
risk communication	exchange or sharing of information about risk between the decision-maker and other stakeholders ■	N8923: FCD 27005: 2010-06-02
risk criteria	terms of reference against which the significance of risk (2.45) is evaluated [ISO Guide 73:2009] ■	N8718: 1st WD 27000: 2010-05-27

Term	Definition	ISO/IEC JTC 1/SC 27 Document
risk criteria	terms of reference against which the significance of a risk is evaluated NOTE 1 Risk criteria are based on organizational objectives, and external and internal context. NOTE 2 Risk criteria can be derived from standards, laws, policies and other requirements. [ISO 31000:2009] ■	N8923: FCD 27005: 2010-06-02
risk evaluation	process (2.40) of comparing the results of risk analysis (2.47) with risk criteria (2.51) to determine whether the risk (2.45) and/or its magnitude is acceptable or tolerable [ISO Guide 73:2009] ■	N8718: 1st WD 27000: 2010-05-27
risk evaluation	process of comparing the results of risk analysis with risk criteria to determine whether the risk and/or its magnitude is acceptable or tolerable NOTE Risk evaluation assists in the decision about risk treatment. [ISO 31000:2009] ■	N8923: FCD 27005: 2010-06-02
risk identification	process of finding, recognizing and describing risks (2.45) [ISO Guide 73:2009] ■	N8718: 1st WD 27000: 2010-05-27
risk identification	process of finding, recognizing and describing risks NOTE 1 Risk identification involves the identification of risk sources, events, their causes and their potential consequences. NOTE 2 Risk identification can involve historical data, theoretical analysis, informed and expert opinions, and stakeholders' needs. [ISO 31000:2009] NOTE 3 In the context of this International Standard the term "activity" is used instead of the term "process" for risk identification. ■	N8923: FCD 27005: 2010-06-02
risk management	coordinated activities to direct and control an organization with regard to risk (2.45) [ISO Guide 73:2009] ■	N8718: 1st WD 27000: 2010-05-27
risk management	coordinated activities to direct and control an organization with regard to risk [ISO 31000:2009] ■	N8923: FCD 27005: 2010-06-02
risk management	process of assessing and quantifying risk and establishing an acceptable level of risk for the organization [ISO/IEC TR 13335-1:1996] NOTE This definition differs from that used in ISO/IEC Guide 73. ■	ISO/IEC 21827: 2008-10-15 (2nd ed.)
risk management	coordinated activities to direct and control an organization with regard to risk [ISO/IEC Guide 73:2002] ■	ISO/IEC TR 19791: 2010-04-01 (2nd ed.)
risk management process	systematic application of management policies, procedures and practices to the activities of communicating, consulting, establishing the context and identifying, analyzing, evaluating, treating, monitoring and reviewing risk (2.45) [ISO Guide 73:2009] ■	N8718: 1st WD 27000: 2010-05-27

Term	Definition	ISO/IEC JTC 1/SC 27 Document
risk reporting	form of communication intended to inform particular internal or external stakeholders (2.59) by providing information regarding the current state of risk (2.45) and its management [ISO Guide 73:2009] ■	N8718: 1st WD 27000: 2010-05-27
risk source	element which alone or in combination has the intrinsic potential to give rise to risk (2.45) [ISO Guide 73:2009] ■	N8718: 1st WD 27000: 2010-05-27
risk treatment	process (2.40) to modify risk (2.45) [ISO Guide 73:2009] ■	N8718: 1st WD 27000: 2010-05-27
risk treatment	process to modify risk NOTE 1 Risk treatment can involve: - avoiding the risk by deciding not to start or continue with the activity that gives rise to the risk; - taking or increasing risk in order to pursue an opportunity; - removing the risk source; - changing the likelihood; - changing the consequences; - sharing the risk with another party or parties (including contracts and risk financing); and - retaining the risk by informed choice. NOTE 2 Risk treatments that deal with negative consequences are sometimes referred to as "risk mitigation", "risk elimination", "risk prevention" and "risk reduction". NOTE 3 Risk treatment can create new risks or modify existing risks. [ISO 31000:2009] ■	N8923: FCD 27005: 2010-06-02
risk treatment	process of selection and implementation of measures to modify risk ■	ISO/IEC TR 15443-3: 2007-12-15 (1st ed.)
risk treatment	process of selection and implementation of options to modify risk [ISO/IEC Guide 73:2002] ■	ISO/IEC TR 19791: 2010-04-01 (2nd ed.)
role	security attribute associated to a user defining the user access rights or limitations to services of a cryptographic module NOTE One or more services may be associated to a role. A role may be associated to one or more users and a user may assume one or more roles. ■	ISO/IEC 24759: 2008-07-01 (1st ed.)
role	predefined set of rules establishing the allowed interactions between a user and the TOE ■	ISO/IEC 15408-1: 2009-12-15 (3rd ed.)
role	security attribute associated to a user defining the user access rights or limitations to services of a cryptographic module. One or more services may be associated to a role. A role may be associated to one or more users and a user may assume one or more roles ■	N8776: 2nd WD 19790: 2010-07-16

Term	Definition	ISO/IEC JTC 1/SC 27 Document
role	specification of the interactions available to an entity (3.1.1) in a domain (3.2.3) NOTE 1 A role of an entity can be made explicit as an attribute, e.g. by a credential. NOTE 2 A role typically implies a collection of privileges to access services or use resources available in a domain. ■	N8804: 3rd CD 24760-1: 2010-06-11
role	job function within the context of an organization with some associated semantics regarding the authority and responsibility conferred on the user assigned to the role. [ANSI-RBAC] ■	N8812: 3rd WD 29146: 2010-07-14
Role Based Access Controls - RBAC	A role based access control (RBAC) policy bases access control decisions on the functions a user is allowed to perform within an organization. The users cannot pass access permissions on to other users at their discretion. This is a fundamental difference between RBAC and DAC (Reference: 15th National Computer Security Conference (1992), Baltimore MD, pp. 554 - 563, David F. Ferraiolo and D. Richard Kuhn, National Institute of Standards and Technology) ■	N8812: 3rd WD 29146: 2010-07-14
root node	node in a *tree* which is not a child of any other node i.e. the "top" of the *tree* ■	N8743: 2nd CD 11770-5: 2010-07-29
round function	function φ (.,.) that transforms two binary strings of lengths L_1 and L_2 to a binary string of length L_2 NOTE The round function is used iteratively. ■	ISO/IEC FDIS 10118-2: 2010-03-10
round-function	function Φ(.,.) that transforms two binary strings of lengths L_1 and L_2 to a binary string of length L_2 NOTE - it is used iteratively as part of a hash-function, where it combines a data string of length L_1 with the previous output of length L_2 ■	ISO/IEC 10118-1: 2000-06-15 (2nd ed.)
round-function	function Φ(.,.) that transforms two binary strings of length L_Φ to a binary string of length L_Φ NOTE It is used iteratively as part of a hash-function, where it combines an 'expanded' data block of length L_Φ with the previous output of length L_Φ ■	ISO/IEC 10118-4: 1998-12-15 (1st ed.)
round-function	function that transforms two binary strings of lengths L_1 and L_2 to a binary string of length L_2 NOTE 1 It is used iteratively as part of a hash-function, where it combines a data string of length L_1 with the previous output of length L_2. [ISO/IEC 10118-1] NOTE 2 This function is also referred to as compression function in a certain hash-function text. ■	ISO/IEC FDIS 9797-2: 2009-09-18

Term	Definition	ISO/IEC JTC 1/SC 27 Document
router	network device that is used to establish and control the flow of data between different networks, which themselves can be based on different networks protocols, by selecting paths or routes based upon routing protocol mechanisms and algorithms [ISO/IEC 18028-1] NOTE The routing information is kept in a routing table. ■	ISO/IEC 18043: 2006-06-15 (1st ed.)
router	network device that is used to establish and control the flow of data between different networks by selecting paths or routes based upon routing protocol mechanisms and algorithms NOTE 1 The networks can themselves be based on different protocols. NOTE 2 The routing information is kept in a routing table. ■	ISO/IEC 27033-1: 2009-12-15 (1st ed.)
rule	most elementary unit of a policy. A rule has a target, an effect, and a condition. [XACML] ■	N8812: 3rd WD 29146: 2010-07-14
runtime environment	virtual machine state which provides software services for processes or programs while a computer is running. It may pertain to the operating system itself, or the software that runs beneath it. The primary purpose is to accomplish the objective of "platform independent" programming ■	N8776: 2nd WD 19790: 2010-07-16
safety	persistence of dependability in the face of accidents or mishaps, i.e., unplanned events that result in death, injury, illness, damage to or loss of property, or environmental harm. [IEEE Std 1228-1994, Rushby] ■	N8732: 3rd WD 29193: 2010-08-06
salt	random data item produced by the signing entity during the generation of the message representative in Signature scheme 2 ■	ISO/IEC FDIS 9796-2: 2010-09-10
salt	random variable incorporated as secondary input to a one-way or encryption function that is used to derive password verification data ■	ISO/IEC 11770-4: 2006-05-01 (1st ed.)
salt	non-secret, often random, value that is used in a hashing process, usually to ensure that the results of computations for one instance cannot be reused by an attacker. NOTE - It is also referred to as sand. ■	N8810: 1st CD 29115 | X.eaa: 2010-06-10
salt	optional bit string for producing a representative ■	ISO/IEC 14888-2: 2008-04-15 (2nd ed.)

Term	Definition	ISO/IEC JTC 1/SC 27 Document
scale	ordered set of values, continuous or discrete, or a set of categories to which the attribute is mapped [ISO/IEC 15939:2007] NOTE The type of scale depends on the nature of the relationship between values on the scale. Four types of scale are commonly defined: - nominal: the measurement values are categorical; - ordinal: the measurement values are rankings; - interval: the measurement values have equal distances corresponding to equal quantities of the attribute; - ratio: the measurement values have equal distances corresponding to equal quantities of the attribute, where the value of zero corresponds to none of the attribute. These are just examples of the types of scale. ■	ISO/IEC 27004: 2009-12-15 (1st ed.)
scam	fraud or confidence trick ■	N8624: 2nd CD 27032: 2010-06-15
scenario	example of system usage in the form of action and event sequences. Scenarios are recorded as UML or any other sequence diagrams. [Neumann/Strembeck] ■	N8812: 3rd WD 29146: 2010-07-14
scheme	set of rules defining the environment, including criteria and methodology required to conduct an assessment [adapted from ISO/IEC18045 (Common Evaluation Methodology)]. ■	ISO/IEC TR 15443-1: 2005-02-01 (1st ed.)
scheme	set of rules, established by an evaluation authority, defining the evaluation environment, including criteria and methodology required to conduct IT security evaluations ■	N8912: Corrected 18045: 2010-09-15
secondary use	processing of PII for a purpose different than the purpose(s) for which it was collected ■	N8806: 4th CD 29100: 2010-06-10
secrecy	security property for a cryptographic protocol that means a message or data shoud not be learned by unauthorized entities in the protocol ■	N8778: 3rd CD 29128: 2010-06-11
secret	value known only to authorized entities	ISO/IEC 11770-4: 2006-05-01 (1st ed.)
secret	information that must be known only to authorised users and/or the TSF in order to enforce a specific SFP ■	ISO/IEC 15408-1: 2009-12-15 (3rd ed.)
secret credential	credential based on the "something you know" factor (e.g., password). ■	N8810: 1st CD 29115 | X.eaa: 2010-06-10
secret key	key used with symmetric cryptographic techniques and usable only by a set of specified entities NOTE Adapted from ISO/IEC 11770-3:1999, 3.35. ■	ISO/IEC 13888-1: 2009-07-15 (3rd ed)
secret key	key used with symmetric cryptographic techniques and usable only by a set of specified entities [ISO/IEC 11770-1] ■	ISO/IEC FDIS 13888-2: 2010-08-06
secret key	function that utilizes a key token factor, a key token and other parameters as input, and outputs a secret value, which is used to compute one or more secret keys ■	ISO/IEC 11770-4: 2006-05-01 (1st ed.)

Term	Definition	ISO/IEC JTC 1/SC 27 Document
secret key	key used with symmetric cryptographic techniques by a specified set of entities [ISO/IEC 11770-3:1999]. ■	ISO/IEC 18033-1: 2005-02-01 (1st ed.)
secret key	key used with symmetric cryptographic techniques by a specified set of entities [ISO/IEC 11770-3:1999] ■	ISO/IEC 18033-2: 2006-05-01 (1st ed.)
secret key	key used with symmetric cryptographic techniques by a specified set of entities [ISO/IEC 18033-1] ■	ISO/IEC 19772: 2009-02-15 (1st ed.)
secret key	key used with symmetric cryptographic techniques by a specified set of entities [ISO/IEC 11770-3:1999] ■	N8749: 2nd CD 18033-4: 2010-05-19
secret key	key used with symmetric cryptographic techniques by a specified set of entities [ISO/IEC 11770-3: 1999] ■	N8757: 2nd WD 29192-3: 2010-07-01
secret key	key used with symmetric cryptographic techniques by a specified set of entities [ISO/IEC 11770-3:2008] ■	N8751: FCD 29150: 2010-06-10
secret key	key used with symmetric cryptographic techniques and usable only by a set of specified entities ■	ISO/IEC FDIS 11770-1: 2010-07-26
secret key	a cryptographic key, used with a secret key cryptographic algorithm that is uniquely associated with one or more entities and should not be made public ■	N8776: 2nd WD 19790: 2010-07-16
secret key	key used with symmetric cryptographic techniques by a specified set of entities ■	ISO/IEC 11770-3: 2008-07-15 (2nd ed.)
secret parameter	number or bit string that does not appear in the public domain and is only used by a claimant, e.g. a private key ■	ISO/IEC 9798-5: 2009-12-15 (3rd ed.)
secret parameter	number or bit string that does not appear in the public domain and is only used by a claimant, e.g., a private key ■	N8759: 2nd WD 29192-4: 2010-06-15
secret parameter	input to the RBG during initialisation, which provides additional entropy in the case of an entropy source failure or compromise ■	N8745: FCD 18031: 2010-05-18
secret value derivation function	key used with symmetric cryptographic techniques by a specified set of entities [ISO/IEC 18033-1:2005] ■	ISO/IEC 11770-4: 2006-05-01 (1st ed.)
secure application	application for which the Actual Level of Trust is equal to the Targeted Level of Trust, as defined by the organization using the application ■	N8632: FCD 27034-1: 2010-05-27
secure envelope - SENV	set of data items which is constructed by an entity in such a way that any entity holding the secret key can verify their integrity and origin NOTE For the purpose of generating evidence, the SENV is constructed and verified by a trusted third party (TTP) with a secret key known only to the TTP. ■	ISO/IEC 13888-1: 2009-07-15 (3rd ed)
secure shell - SSH	a protocol that provides secure remote login utilising an insecure network. SSH is proprietary but will become an IETF standard in the near future. SSH was originally developed by SSH Communications Security. ■	ISO/IEC 18028-4: 2005-04-01 (1st ed.)

Term	Definition	ISO/IEC JTC 1/SC 27 Document
Secure Sockets Layer - SSL	protocol located between the network layer and the application layer provides authentication of clients and server and integrity and confidentiality services. SSL was developed by Netscape and builds the basis for TLS. ■	ISO/IEC 18028-4: 2005-04-01 (1st ed.)
secure state	state in which the TSF data are consistent and the TSF continues correct enforcement of the SFRs ■	ISO/IEC 15408-1: 2009-12-15 (3rd ed.)
security	All aspects related to defining, achieving, and maintaining confidentiality, integrity, availability, accountability, authenticity, and reliability [ISO/IEC13335-1]. Note: A product, system, or service is considered to be secure to the extent that its users can rely that it functions (or will function) in the intended way. This is usually considered in the context of an assessment of actual or perceived threats. a) The capability of the software product to protect information and data so that unauthorised persons or systems cannot read or modify them and authorised persons or systems are not denied access to them [ISO/IEC 9126-1]. ■	ISO/IEC TR 15443-1: 2005-02-01 (1st ed.)
security	all aspects related to defining, achieving, and maintaining confidentiality, integrity, availability, non-repudiation, accountability, authenticity, and reliability [ISO/IEC 13335-1:2004, definition 2.11] ■	ISO/IEC TR 15443-3: 2007-12-15 (1st ed.)
security assessment	verification of a security deliverable against a security standard using the corresponding security method to establish compliance and determine the security assurance. a) The last stage of the product evaluation process [ISO/IEC 14598-1]. ■	ISO/IEC TR 15443-1: 2005-02-01 (1st ed.)
security attribute	property of subjects, users (including external IT products), objects, information, sessions and/or resources that is used in defining the SFRs and whose values are used in enforcing the SFRs ■	ISO/IEC 15408-1: 2009-12-15 (3rd ed.)
security authority	entity that is responsible for the definition or enforcement of security policy NOTE Adapted from ISO/IEC 10181-1, 3.3.17. ■	ISO/IEC 13888-1: 2009-07-15 (3rd ed)
security authority	entity that is responsible for the definition, implementation or enforcement of security policy [ISO/IEC 10181-1:1996] ■	ISO/IEC FDIS 11770-1: 2010-07-26
security authority	entity accountable for the administration of a security policy within a security domain. ■	ISO/IEC 15816: 2002-02-01 (1st ed.)
security certificate	set of security-relevant data issued by a security authority or trusted third party, together with security information which is used to provide the integrity and data origin authentication NOTE Adapted from ISO/IEC 10181-1, 3.3.18. ■	ISO/IEC 13888-1: 2009-07-15 (3rd ed)

Term	Definition	ISO/IEC JTC 1/SC 27 Document
security controls	management, operational, and technical controls (i.e., safeguards or countermeasures) prescribed for an information system to protect the confidentiality, integrity, and availability of the system and its information [NIST SP 800-53] NOTE This definition is intended to include controls that provide accountability, authenticity, non-repudiation, privacy and reliability, which are sometimes considered as distinct from confidentiality, integrity and availability. ■	ISO/IEC TR 19791: 2010-04-01 (2nd ed.)
security domain	set of elements, security policy, security authority and set of security-relevant activities in which the set of elements are subject to the security policy for the specified activities, and the security policy is administered by the security authority for the security domain [ISO/IEC 10181-1:1996] ■	ISO/IEC FDIS 11770-1: 2010-07-26
security domain	collection of resources to which an active entity has access privileges ■	ISO/IEC 15408-1: 2009-12-15 (3rd ed.)
security domain	portion of an operational system that implements the same set of security policies ■	ISO/IEC TR 19791: 2010-04-01 (2nd ed.)
security domain	collection of users and systems subject to a common security policy. ■	ISO/IEC 15816: 2002-02-01 (1st ed.)
security domain	set of assets and resources subject to a common security policy ■	ISO/IEC 27033-1: 2009-12-15 (1st ed.)
security element	indivisible security requirement. ■	ISO/IEC TR 15443-1: 2005-02-01 (1st ed.)
security event	identified occurrence of a system, service or network state indicating a possible breach of information security, policy or failure of controls, or a previously unknown situation that may be security relevant [ISO 27000:2009] ■	N8636: FCD 27035: 2010-05-19
security function	cryptographic algorithms together with modes of operation, such as block ciphers, stream ciphers, asymmetric key, message authentication codes, hash functions, or other security functions, random bit generators, entity authentication and key establishment all approved either by ISO/IEC or an approval authority [ISO/IEC 19790:2006, 3.63] NOTE See ISO/IEC 19790:2006, Annex D. ■	ISO/IEC 24759: 2008-07-01 (1st ed.)
security function	cryptographic algorithms together with modes of operation, such as block ciphers, stream ciphers, asymmetric key, message authentication codes, hash functions, or other security functions, random bit generators, entity authentication and key establishment all approved either by ISO/IEC or an approval authority NOTE See Annex C ■	N8776: 2nd WD 19790: 2010-07-16

Term	Definition	ISO/IEC JTC 1/SC 27 Document
security function policy	set of rules describing specific security behaviour enforced by the TSF and expressible as a set of SFRs ■	ISO/IEC 15408-1: 2009-12-15 (3rd ed.)
security gateway	point of connection between networks, or between subgroups within networks, or between software applications within different security domains intended to protect a network according to a given security policy ■	ISO/IEC 27033-1: 2009-12-15 (1st ed.)
security incident	single or a series of unwanted or unexpected information security events that have a significant probability of compromising business operations and threatening information security [ISO 27000:2009] ■	N8636: FCD 27035: 2010-05-19
Security Information Object - SIO	instance of an SIO Class. ■	ISO/IEC 15816: 2002-02-01 (1st ed.)
Security Information Object Class	Information Object Class that has been tailored for security use. ■	ISO/IEC 15816: 2002-02-01 (1st ed.)
security objective	statement of intent to counter identified threats and/or satisfy identified organisation security policies and assumptions [ISO/IEC 15408-1:2005, definition 2.42] ■	ISO/IEC TR 15443-3: 2007-12-15 (1st ed.)
security objective	statement of an intent to counter identified threats and/or satisfy identified organization security policies and/or assumptions ■	ISO/IEC 15408-1: 2009-12-15 (3rd ed.)
security policy	set of criteria for the provision of security services [ISO 7498-2] ■	ISO/IEC 13888-1: 2009-07-15 (3rd ed)
security policy	set of criteria for the provision of security services [ISO/IEC 7498-2] ■	ISO/IEC FDIS 13888-2: 2010-08-06
security policy	rules, directives and practices that govern how assets, including sensitive information, are managed, protected and distributed within an organization and its systems, particularly those which impact the systems and associated elements ■	ISO/IEC 21827: 2008-10-15 (2nd ed.)
security policy	set of rules internal to an organizational unit that regulate how this unit protects the management of its assets conform to specified organizational objectives within its legal and cultural context ■	ISO/IEC TR 15443-3: 2007-12-15 (1st ed.)
security policy information file	construct that conveys domain-specific security policy information. ■	ISO/IEC 15816: 2002-02-01 (1st ed.)
security problem	statement which in a formal manner defines the nature and scope of the security that the TOE is intended to address NOTE This statement consists of a combination of: - threats to be countered by the TOE, - the OSPs enforced by the TOE, and - the assumptions that are upheld for the TOE and its operational environment. ■	ISO/IEC 15408-1: 2009-12-15 (3rd ed.)
security property	formally or informally defined property which a cryptographic protocol is designed to assure such as secrecy, authenticity and anonymity ■	N8778: 3rd CD 29128: 2010-06-11

Term	Definition	ISO/IEC JTC 1/SC 27 Document
security property	text of the definition ■	N8732: 3rd WD 29193: 2010-08-06
security related requirements	requirements which have a direct effect on the secure operation of a system or enforce conformance to a specified security policy ■	ISO/IEC 21827: 2008-10-15 (2nd ed.)
security requirement	requirement, stated in a standardized language, which is meant to contribute to achieving the security objectives for a TOE ■	ISO/IEC 15408-1: 2009-12-15 (3rd ed.)
security strength	number associated with the amount of work (i.e. the number of operations) that is required to break a cryptographic algorithm or system NOTE Security strength is specified in bits and is a specific value from the set {80, 112, 128, 192, 256}. ■	ISO/IEC FDIS 9797-2: 2009-09-18
security strength	number associated with the amount of work (that is, the number of operations) that is required to break a cryptographic algorithm or system NOTE In ISO/IEC 29192, security strength is specified in bits, e.g. 80, 112, 128, 192, and 256. ■	N8753: 1st CD 29192-1: 2010-06-22
security strength	number associated with the amount of work (that is the number of operations) that is required to break a cryptographic algorithm or system NOTE Security strength is specified in bits and is a specific value from the set {80, 112, 128, 192, 256}. [ISO/IEC 9797-2] ■	N8760: 1st WD 20008-1: 2010-06-14
security strength	number associated with the amount of work (that is the number of operations) that is required to break a cryptographic algorithm or system NOTE Security strength is specified in bits and is a specific value from the set {80, 112, 128, 192, 256}. [ISO/IEC 9797-2] ■	N8763: 1st WD 20009-2: 2010-06-20
security target - ST	set of security requirements and specifications to be used as the basis for evaluation of an identified IT product or system (adapted from ISO/IEC 15408-1) ■	ISO/IEC 15292: 2001-12-15 (1st ed.)
security target - ST	implementation-dependent statement of security needs for a specific identified TOE ■	ISO/IEC 15408-1: 2009-12-15 (3rd ed.)
security target - ST	implementation-dependent statement of security needs for a specific identified TOE ■	N8784: 1st WD 20004: 2010-08-06
security token	set of security-relevant data that is protected by integrity and data origin authentication from a source which is not considered a security authority NOTE Adapted from ISO/IEC 10181-1, 3.3.26. ■	ISO/IEC 13888-1: 2009-07-15 (3rd ed)

Term	Definition	ISO/IEC JTC 1/SC 27 Document
Security/Multipurpose Internet Mail Extensions - S/MIME	protocol providing secure multipurpose mail exchange. Its current version 3 consists of five parts: RFC 3369 and RFC 3370 define the message syntax, RFC 2631to RFC 2633 define message specification, certificate handling and key agreement method. ■	ISO/IEC 18028-4: 2005-04-01 (1st ed.)
seed	string of bits that is used as input to a deterministic random bit generator (DRBG) NOTE The seed will determine a portion of the state of the DRBG. ■	N8745: FCD 18031: 2010-05-18
seed key	secret value which can be used to initialize a random bit generator ■	ISO/IEC 24759: 2008-07-01 (1st ed.)
seed key	secret value used to initialise a cryptographic function or operation ■	N8776: 2nd WD 19790: 2010-07-16
seedlife	period of time between initialising the DRBG with one seed and reseeding (fully initialising) that DRBG with another seed ■	N8745: FCD 18031: 2010-05-18
selection	specification of one or more items from a list in a component ■	ISO/IEC 15408-1: 2009-12-15 (3rd ed.)
selection	specification of one or more items from a list ■	N8784: 1st WD 20004: 2010-08-06
selective disclosure	principle of identity management (3.4.1) that gives an person a measure of control over the identity information (3.2.5) that may be transferred to a receiver, e.g. during authentication (3.3.2) ■	N8804: 3rd CD 24760-1: 2010-06-11
self-assessment evidence	evidence that the developer uses to verify whether a specified protocol fulfils its designated security properties NOTE It includes cryptographic protocol specification, adversarial model and output (transcripts) of formal verification tool. ■	N8778: 3rd CD 29128: 2010-06-11
self-synchronous stream cipher	stream cipher with the property that the keystream symbols are generated as a function of a secret key and a fixed number of previous ciphertext bits. ■	ISO/IEC 18033-1: 2005-02-01 (1st ed.)
semiformal	expressed in a restricted syntax language with defined semantics ■	ISO/IEC 15408-1: 2009-12-15 (3rd ed.)
sensitive data	data that, in user's view, requires protection ■	N8776: 2nd WD 19790: 2010-07-16
sensitive PII	category of PII that affect the PII principal's most intimate sphere, or likely to give rise, in case of misuse, to unlawful or arbitrary discrimination or to a substantial harm or risk to the PII principal NOTE: In some jurisdictions or in specific contracts, sensitive PII are defined in reference to the nature of the PII and may consist of PII revealing the racial origin, political opinions or religious or other beliefs, as well as personal data on health, sex life or criminal convictions, as well as other PII that may be defined as sensitive. NOTE Harm should be taken to include monetary and non-monetary damages. ■	N8806: 4th CD 29100: 2010-06-10

Term	Definition	ISO/IEC JTC 1/SC 27 Document
sensitive security parameters - SSP	critical security parameters (CSP) and public security parameters (PSP) ■	N8776: 2nd WD 19790: 2010-07-16
sensor	component/agent of IDS, which collects event data from an Information System or network under observation NOTE Also referred to as a monitor. ■	ISO/IEC 18043: 2006-06-15 (1st ed.)
sequence number	time variant parameter whose value is taken from a specified sequence which is non-repeating within a certain time period NOTE See also Annex B. ■	ISO/IEC 9798-1: 2010-07-01 (3rd ed.)
sequence number	time variant parameter whose value is taken from a specified sequence which is nonrepeating within a certain time period [ISO/IEC 11770-1:1996] ■	ISO/IEC 18014-1: 2008-09-01 (2nd ed.)
sequence number	time variant parameter whose value is taken from a specified sequence which is non-repeating within a certain time period [ISO/IEC 9798-1] ■	N8762: 1st WD 20009-1: 2010-07-13
sequence number	time variant parameter whose value is taken from a specified sequence which is non-repeating within a certain time period [ISO/IEC 9798-1] ■	N8763: 1st WD 20009-2: 2010-06-20
sequence number	time variant parameter whose value is taken from a specified sequence which is non-repeating within a certain time period ■	ISO/IEC FDIS 11770-1: 2010-07-26
sequence number	time variant parameter whose value is taken from a specified sequence which is non-repeating within a certain time period ■	ISO/IEC 11770-2: 2008-06-15 (2nd ed.)
sequence number	time variant parameter whose value is taken from a specified sequence which is non-repeating within a certain time period [ISO/IEC 11770-1:1996] ■	ISO/IEC 11770-3: 2008-07-15 (2nd ed.)
sequential cohesion	module containing functions each of whose output is input for the following function in the module [IEEE Std 610.12-1990] NOTE An example of a sequentially cohesive module is one that contains the functions to write audit records and to maintain a running count of the accumulated number of audit violations of a specified type. ■	ISO/IEC 15408-1: 2009-12-15 (3rd ed.)
Serial Line Internet Protocol - SLIP	packet framing protocol specified in RFC 1055 for transferring data using telephone lines (serial lines). ■	ISO/IEC 18028-4: 2005-04-01 (1st ed.)
server	computer system or program that provides services to other computers ■	ISO/IEC 18043: 2006-06-15 (1st ed.)
service	security process or task performed by a deliverable, organisation, or person. ■	ISO/IEC TR 15443-1: 2005-02-01 (1st ed.)

Term	Definition	ISO/IEC JTC 1/SC 27 Document
service	means of delivering value to acquirers by facilitating results acquirers want to achieve without the ownership of specific resources and risks NOTE 1 Adapted from ISO/IEC 20000-1:xxxx NOTE 2 A service is generally intangible. NOTE 3 Services may also be provided by a supplier to the service provider. ■	N8780: 1st CD 29147: 2010-06-10
service	any externally invoked operation and/or function that can be performed by a cryptographic module ■	N8776: 2nd WD 19790: 2010-07-16
service input	all data or control information utilised by the cryptographic module that initiates or obtains specific operations or functions ■	N8776: 2nd WD 19790: 2010-07-16
Service Level Agreement	contract that defines the technical support or business performance objectives including measures for performance and consequences for failure the provider of a service can provide its clients ■	ISO/IEC 18043: 2006-06-15 (1st ed.)
service level agreement	written agreement between a service provider and an organization that documents services and agreed service levels NOTE In the case of outsourced service providers, the service level agreement is a written contractually binding agreement ■	ISO/IEC 24762: 2008-02-01 (1st ed.)
service level commitment	commitment from a service provider (usually an internal service provider) to an organization that defines services and agreed service levels ■	ISO/IEC 24762: 2008-02-01 (1st ed.)
service output	all data and status information that results from operations or functions initiated or obtained by service input ■	N8776: 2nd WD 19790: 2010-07-16
service providers	in-house teams or external parties providing ICT DR services to organizations ■	ISO/IEC 24762: 2008-02-01 (1st ed.)
Service Set Identifier - SSID	identifier for wireless access points, usually in the form of a name. ■	ISO/IEC 18028-4: 2005-04-01 (1st ed.)
Session Roles	session role is the role activated by a user session. [ANSI-RBAC] ■	N8812: 3rd WD 29146: 2010-07-14
Shared Secret	secret used in authentication that is known to the claimant and the verifier. ■	N8810: 1st CD 29115 | X.eaa: 2010-06-10
shared secret key	*key* which is shared with all the active entities via a *key establishment mechanism for multiple entities* NOTE The *key* can be updated. ■	N8743: 2nd CD 11770-5: 2010-07-29
short input performance	performance of the cryptographic primitive when processing short inputs ■	N8753: 1st CD 29192-1: 2010-06-22

Term	Definition	ISO/IEC JTC 1/SC 27 Document
side-channel attack	attack based on information gained from the physical implementation of a cryptosystem, rather than brute force or theoretical weaknesses in the underlying algorithms EXAMPLE Timing information, power consumption, or electromagnetic emissions which can provide extra sources of information can be exploited to attack the system. ■	N8753: 1st CD 29192-1: 2010-06-22
sign	signature generation process that takes a message and a signing key of a signer to produce a signature ■	N8759: 2nd WD 29192-4: 2010-06-15
signature	pair of an octet string and an integer for providing authentication, generated in the signature generation process NOTE Adapted from ISO/IEC 14888-1:1998. ■	ISO/IEC 9796-3: 2006-09-15 (2nd ed.)
signature	string of bits resulting from the signature process [ISO/IEC 14888-1] ■	ISO/IEC FDIS 9796-2: 2010-09-10
signature	one or more data elements resulting from the signature process [ISO/IEC 14888-1] ■	N8760: 1st WD 20008-1: 2010-06-14
signature	one or more data elements resulting from the signature process [ISO/IEC 14888-1] ■	N8763: 1st WD 20009-2: 2010-06-20
signature	one or more data elements resulting from the signature process ■	N8751: FCD 29150: 2010-06-10
signature	one or more data elements resulting from the signature process ■	ISO/IEC 14888-1: 2008-04-15 (2nd ed.)
signature exponent	secret exponent for producing signatures ■	ISO/IEC 14888-2: 2008-04-15 (2nd ed.)
signature generation process	process which takes as inputs the message, the signature key and the domain parameters, and which gives as output the signature NOTE Adapted from the definition of signature process in ISO/IEC 14888-1:1998. ■	ISO/IEC 9796-3: 2006-09-15 (2nd ed.)
signature key	set of private data elements specific to an entity and usable only by this entity in the signature process NOTE Sometimes called a private signature key in other standards, e.g. ISO/IEC 9796-2, ISO/IEC 9796-3 and ISO/IEC 9798-7. [ISO/IEC 14888-1] ■	N8760: 1st WD 20008-1: 2010-06-14
signature key	set of private data elements specific to an entity and usable only by this entity in the signature process NOTE Sometimes called a private signature key in other standards, e.g. ISO/IEC 9796-2, ISO/IEC 9796-3 and ISO/IEC 9798-3. [ISO/IEC 14888-1] ■	N8763: 1st WD 20009-2: 2010-06-20
signature key	set of private data elements specific to an entity and usable only by this entity in the signature process [ISO/IEC 14888-1] ■	N8751: FCD 29150: 2010-06-10

Term	Definition	ISO/IEC JTC 1/SC 27 Document
signature key	set of private data elements specific to an entity and usable only by this entity in the signature process NOTE Sometimes called a private signature key in other standards, e.g. ISO/IEC 9796-2, ISO/IEC 9796-3 and ISO/IEC 9798-3. ■	ISO/IEC 14888-1: 2008-04-15 (2nd ed.)
signature process	process which takes as inputs the message, the signature key and the domain parameters, and which gives as output the signature [ISO/IEC 14888-1] ■	N8760: 1st WD 20008-1: 2010-06-14
signature process	process which takes as inputs the message, the signature key and the domain parameters, and which gives as output the signature [ISO/IEC 14888-1] ■	N8763: 1st WD 20009-2: 2010-06-20
signature process	process which takes as inputs the message, the signature key and the domain parameters, and which gives as output the signature ■	N8751: FCD 29150: 2010-06-10
signature process	process which takes as inputs the message, the signature key and the domain parameters, and which gives as output the signature ■	ISO/IEC 14888-1: 2008-04-15 (2nd ed.)
signature system	system based on asymmetric cryptographic techniques whose private transformation is used for signing and whose public transformation is used for verification ■	ISO/IEC 11770-3: 2008-07-15 (2nd ed.)
signature verification process	process, which takes as its input the signed message, the verification key and the domain parameters, and which gives as its output the recovered message if valid NOTE Adapted from the definition of verification process in ISO/IEC 14888-1: (To be published). ■	ISO/IEC 9796-3: 2006-09-15 (2nd ed.)
signcrypt	to apply signcryption on a plaintext ■	N8751: FCD 29150: 2010-06-10
signcryption	(reversible) transformation of data by a cryptographic algorithm to produce a ciphertext from which no information about the original data can be recovered (except possibly its length), nor can a new ciphertext be forged without detection, by an unauthorised entity, that is, it provides data confidentiality, data integrity, data origin authentication, and non-repudiation ■	N8751: FCD 29150: 2010-06-10
signcryption algorithm	one of the three component algorithms of a signcryption mechanism which takes as input a plaintext, a sender's public and private key pair, a recipient's public key and other data, outputs a ciphertext after performing a sequence of specified operations on the input ■	N8751: FCD 29150: 2010-06-10

Term	Definition	ISO/IEC JTC 1/SC 27 Document
signcryption mechanism	cryptographic technique used to protect the confidentiality and simultaneously guarantee the origin, integrity and non-repudiation of data, and which consists of three component algorithms: a key generation algorithm, a signcryption algorithm and a unsigncryption algorithm ■	N8751: FCD 29150: 2010-06-10
signed message	set of data items consisting of the signature, the part of the message which cannot be recovered from the signature, and an optional text field [ISO/IEC 14888-1:1998] ■	ISO/IEC 9796-3: 2006-09-15 (2nd ed.)
signed message	set of data elements consisting of the signature, the part of the message which cannot be recovered from the signature, and an optional text field [ISO/IEC 14888-1] ■	N8760: 1st WD 20008-1: 2010-06-14
signed message	set of data elements consisting of the signature, the part of the message which cannot be recovered from the signature, and an optional text field [ISO/IEC 14888-1] ■	N8763: 1st WD 20009-2: 2010-06-20
signed message	set of data elements consisting of the signature, the part of the message which cannot be recovered from the signature, and an optional text field [ISO/IEC 14888-1] ■	N8751: FCD 29150: 2010-06-10
signed message	set of data elements consisting of the signature, the part of the message which cannot be recovered from the signature, and an optional text field NOTE In the context of this part of ISO/IEC 14888, the entire message is included in the signed message and no part of the message is recovered from the signature. ■	ISO/IEC 14888-1: 2008-04-15 (2nd ed.)
signer	entity generating a digital signature ■	ISO/IEC 13888-1: 2009-07-15 (3rd ed)
signer	entity with an unique bit string as an identity, including the functions and the private data necessary to engage in generation of a signature ■	N8759: 2nd WD 29192-4: 2010-06-15
signer	entity generating a digital signature [ISO/IEC 13888-1:2009] ■	N8642: 2nd PDTR 29149: 2010-06-22
signing key	data item given by the trusted server that shall be kept secret and should only be used by a signer in accordance with the process of generation of a signature ■	N8759: 2nd WD 29192-4: 2010-06-15
simple input interface	interface for a device that allows the user to indicate to the device the successful or unsuccessful completion of a procedure, e.g. as could be implemented as a pair of buttons or a single button which is either pressed or not within a certain time interval ■	ISO/IEC FDIS 9798-6: 2010-08-05
Simple Mail Transfer Protocol - SMTP	internet protocol (RFC 821 and extensions) for sending mail to mail servers (outgoing). ■	ISO/IEC 18028-4: 2005-04-01 (1st ed.)

Term	Definition	ISO/IEC JTC 1/SC 27 Document
simple output interface	interface for a device that allows the device to indicate to the user the successful or unsuccessful completion of a procedure, e.g. as could be implemented by red and green lights or as single light which is lit in different ways to indicate success or failure ■	ISO/IEC FDIS 9798-6: 2010-08-05
simple power analysis SPA	direct analysis (primarily visual) of patterns of instruction execution (or execution of individual instructions), in relation to the electrical power consumption of a cryptographic module, for the purpose of extracting information correlated to a cryptographic operation ■	ISO/IEC 24759: 2008-07-01 (1st ed.)
simple power analysis SPA	direct (primarily visual) analysis of patterns of instruction execution (or execution of individual instructions), obtained through monitoring the variations in electrical power consumption of a cryptographic module, for the purpose of revealing the features and implementations of cryptographic algorithms and subsequently the values of cryptographic keys ■	N8776: 2nd WD 19790: 2010-07-16
single-chip cryptographic module	physical embodiment in which a single integrated circuit (IC) chip may be used as a standalone device or may be embedded within an enclosure or a product that may not be physically protected EXAMPLE Single integrated circuit (IC) chips or smart cards with a single IC chip ■	N8776: 2nd WD 19790: 2010-07-16
single-sign-on identity - SSO identity	identity (3.1.2) that includes an identity assertion (3.5.3) NOTE The identity assertion in a single-sign-on identity is created during authentication of an entity in one domain and can be used in authentication of the entity in any other domain in the same identity federation ■	N8804: 3rd CD 24760-1: 2010-06-11
slack space	the space between the end of a file and the end of the cluster it is stored in that may contain data from the file that previously occupied the space NOTE Slack space can occur within any storage device, and the relative amount is determined by the media type and size, e.g. RAM (Random Access Memory) slack, file slack, etc. ■	N8640: 3rd WD 27037: 2010-05-31
smooth integer	integer *r* whose prime factors are all small (i.e. less than some defined bound) ■	ISO/IEC 15946-5: 2009-12-15 (1st ed.)
social engineering	act of manipulating people into performing actions or divulging confidential information ■	ISO/IEC FDIS 27033-3: 2010-09-10
software	programs and data components within the cryptographic boundary and usually stored on erasable media which can be dynamically written and modified during execution [ISO/IEC 19790:2006, 3.66] EXAMPLE Erasable media may include but are not limited to hard drives. ■	ISO/IEC 24759: 2008-07-01 (1st ed.)

Term	Definition	ISO/IEC JTC 1/SC 27 Document
software	executable code of a cryptographic module that is stored on erasable media which can be dynamically written and modified during execution while operating in a modifiable operational environment EXAMPLE Erasable media may include but not limited to solid state memory, hard drives, etc ■	N8776: 2nd WD 19790: 2010-07-16
software cryptographic credential	credential that is comprised of software that contains a protected cryptographic key. NOTE - It is also referred to as a soft credential, soft cryptographic credential, or soft credential. ■	N8810: 1st CD 29115 | X.eaa: 2010-06-10
software engineering	application of a systematic, disciplined, quantifiable approach to the development and maintenance of software; that is, the application of engineering to software [IEEE Std 610.12-1990] NOTE As with engineering practices in general, some amount of judgement must be used in applying engineering principles. Many factors affect choices, not just the application of measures of modular decomposition, layering, and minimization. For example, a developer may design a system with future applications in mind that will not be implemented initially. The developer may choose to include some logic to handle these future applications without fully implementing them; further, the developer may include some calls to as-yet unimplemented modules, leaving call stubs. The developer's justification for such deviations from well-structured programs will have to be assessed using judgement, as well as the application of good software engineering discipline. ■	ISO/IEC 15408-1: 2009-12-15 (3rd ed.)
software module	a module that is composed solely of software ■	N8776: 2nd WD 19790: 2010-07-16
software/firmware load test	a set of tests performed on software or firmware which has to pass successfully before it can be a executed by a cryptographic module ■	N8776: 2nd WD 19790: 2010-07-16
software/firmware module interface - SFMI	a set of commands used to request the services of the software or firmware module, including parameters that enter or leave the module's cryptographic boundary as part of the requested service ■	N8776: 2nd WD 19790: 2010-07-16
spam	unsolicited e-mails, which can carry malicious contents and/or scam messages. ■	ISO/IEC 27033-1: 2009-12-15 (1st ed.)

Term	Definition	ISO/IEC JTC 1/SC 27 Document
spam	the abuse of electronic messaging systems to indiscriminately send unsolicited bulk messages NOTE While the most widely recognized form of spam is e-mail spam, the term is applied to similar abuses in other media: instant messaging spam, Usenet newsgroup spam, Web search engine spam, spam in blogs, wiki spam, mobile phone messaging spam, Internet forum spam and junk fax transmissions. ■	N8624: 2nd CD 27032: 2010-06-15
Specific SIO Class	SIO Class in which the data types for all components are fully specified. ■	ISO/IEC 15816: 2002-02-01 (1st ed.)
specify	provide specific details about an entity in a rigorous and precise manner ■	ISO/IEC 15408-1: 2009-12-15 (3rd ed.)
split knowledge	process by which a cryptographic key is split into multiple key components, individually sharing no knowledge of the complete key, that can be subsequently input into, or output from, a cryptographic module by separate entities and combined to recreate the original cryptographic key NOTE All or a subset of the components may be required to perform the combination. ■	ISO/IEC 24759: 2008-07-01 (1st ed.)
split knowledge	a process by which a cryptographic key is split into multiple key components, individually sharing no knowledge of the original key, that can be subsequently input into, or output from, a cryptographic module by separate entities and combined to recreate the original cryptographic key ■	N8776: 2nd WD 19790: 2010-07-16
spoliation	act of making or allowing unintentional and/or unavoidable change(s) to the potential digital evidence that diminish its evidential value NOTE Not all changes made to the evidence cause spoliation, even if unintended. ■	N8640: 3rd WD 27037: 2010-05-31
sponsor	an entity (organisation, individual etc.) responsible for the content of a register entry ■	ISO/IEC 15292: 2001-12-15 (1st ed.)
spoofing	impersonating a legitimate resource or user ■	ISO/IEC 27033-1: 2009-12-15 (1st ed.)
spyware	deceptive software that collects private or confidential information from a computer user NOTE Information can include matters such as web sites most frequently visited or more sensitive information such as passwords. ■	N8624: 2nd CD 27032: 2010-06-15
ST evaluation	assessment of an ST against defined criteria ■	ISO/IEC 15408-1: 2009-12-15 (3rd ed.)
stage	period within the life cycle of a deliverable comprising processes and activities NOTE Adapted from ISO/IEC 15288 ■	ISO/IEC TR 15443-3: 2007-12-15 (1st ed.)

Term	Definition	ISO/IEC JTC 1/SC 27 Document
stakeholder	person or organization that can affect, be affected by, or perceive themselves to be affected by a decision or activity [ISO Guide 73:2009] ■	N8718: 1st WD 27000: 2010-05-27
stakeholder	any individual, group or organisation that can affect, be affected by, or perceive itself to be affected by, a risk Note 1 A decision maker can be also a stakeholder Note 2 The term "stakeholder" includes but has a broader meaning than "interested party" which definition is provided by ISO 9000:2005 ■	N8712: 3rd WD 27014: 2010-05-28
stakeholder	person or organization that can affect, be affected by, or perceive themselves to be affected by a decision or activity NOTE A decision maker can be a stakeholder. [ISO 31000:2009] ■	N8923: FCD 27005: 2010-06-02
stakeholder	party having a right, share, or an asset at risk in a deliverable or in its possession of characteristics that meet the party's needs and expectations. a) A party having a right, share, or claim asset in a system or in its possession of characteristics that meet the party's needs and expectations [ISO/IEC 15288]. ■	ISO/IEC TR 15443-1: 2005-02-01 (1st ed.)
stakeholder	individual or organization having a right, share, claim or interest in the handling of potential vulnerabilities in a product or online service in such a way that it meets their needs and expectations NOTE Adapted from ISO/IEC 12207:2008. ■	N8780: 1st CD 29147: 2010-06-10
stakeholder	individual or organization having a right, share, claim or interest in a system or in its possession of characteristics that meet their needs and expectations [ISO/IEC 12207:2008] ■	N8624: 2nd CD 27032: 2010-06-15
standalone	system that does not have an active connection to an external device ■	N8640: 3rd WD 27037: 2010-05-31
starting variable (*SV*)	variable possibly derived from some initialization value and used in defining the starting point of the modes of operation. NOTE The method of deriving the starting variable from the initializing value is not defined in this International Standard. It needs to be described in any application of the modes of operation. ■	ISO/IEC 10116: 2006-02-01 (3rd ed.)
state	current internal state of a keystream generator ■	N8749: 2nd CD 18033-4: 2010-05-19
state	current internal state of a keystream generator ■	N8757: 2nd WD 29192-3: 2010-07-01
state	condition of a random bit generator or any part thereof with respect to time and circumstance ■	N8745: FCD 18031: 2010-05-18
statement of applicability	documented statement describing the control objectives (2.14) and controls (2.13) that are relevant and applicable to the organization's ISMS (2.27) ■	N8718: 1st WD 27000: 2010-05-27

Term	Definition	ISO/IEC JTC 1/SC 27 Document
status information	information that is output from a cryptographic module for the purposes of indicating certain operational characteristics or states of the module ■	N8776: 2nd WD 19790: 2010-07-16
Step	action or event within a scenario. [Neumann/Strembeck] ■	N8812: 3rd WD 29146: 2010-07-14
stream cipher	symmetric encryption system with the property that the encryption algorithm involves combining a sequence of plaintext symbols with a sequence of keystream symbols one symbol at a time, using an invertible function. Two types of stream cipher can be identified: synchronous stream ciphers and self-synchronous stream ciphers, distinguished by the method used to obtain the keystream. ■	ISO/IEC 18033-1: 2005-02-01 (1st ed.)
strict conformance	hierarchical relationship between a PP and an ST where all the requirements in the PP also exist in the ST NOTE This relation can be roughly defined as "the ST shall contain all statements that are in the PP, but may contain more". Strict conformance is expected to be used for stringent requirements that are to be adhered to in a single manner. ■	ISO/IEC 15408-1: 2009-12-15 (3rd ed.)
strong	not easily defeated; having strength or power greater than average or expected; able to withstand attack; solidly built ■	N8776: 2nd WD 19790: 2010-07-16
strong secret	secret with a sufficient degree of entropy that conducting an exhaustive search for the secret is infeasible, even given knowledge that would enable a correct guess for the secret to be distinguished from an incorrect guess NOTE - This might, for example, be achieved by randomly choosing the secret from a sufficiently large set of possible values with an even probability distribution. ■	ISO/IEC 11770-4: 2006-05-01 (1st ed.)
structural roles	type of healthcare personnel warranting differing levels of access control. Also known as "basic role", "organizational role," or "role group." Adapted from [ASTM 1986] ■	N8812: 3rd WD 29146: 2010-07-14
sub-activity	application of an assurance component of ISO/IEC 15408-3 NOTE Assurance families are not explicitly addressed in this International Standard because evaluations are conducted on a single assurance component from an assurance family. ■	N8912: Corrected 18045: 2010-09-15
(biometric data) subject	individual whose biometric reference is within the biometric system ■	N8802: FCD 24745: 2010-05-19
subject	active entity in the TOE that performs operations on objects ■	ISO/IEC 15408-1: 2009-12-15 (3rd ed.)
subject	actor whose attributes may be referenced by a predicate. [XACML] ■	N8812: 3rd WD 29146: 2010-07-14
subnet	portion of a network that shares a common address component ■	ISO/IEC 18043: 2006-06-15 (1st ed.)

Term	Definition	ISO/IEC JTC 1/SC 27 Document
subprocess	part of a biometric verification or enrolment process usually performing data capture, intermediate signal processing, final signal processing, storage, comparison, or decision ■	ISO/IEC 24761: 2009-05-15 (1st ed.)
subprocess index	integer uniquely assigned to each subprocess within a biometric processing unit (BPU) by the organization providing the BPU ■	ISO/IEC 24761: 2009-05-15 (1st ed.)
subprocess IO index	unique integer assigned to each data stream between subprocesses in a biometric processing unit (BPU) so that the validator can reconstruct the data flow between subprocesses in the BPU ■	ISO/IEC 24761: 2009-05-15 (1st ed.)
subsystem	one or more operational system components that are capable of execution separately from the rest of the system ■	ISO/IEC TR 19791: 2010-04-01 (2nd ed.)
supplementary check character	check character which does not belong to the character set of the strings which are to be protected. ■	ISO/IEC 7064: 2003-02-15 (2nd ed.)
supplier	individual or organization or an that provides a product or service to an acquirer NOTE 1 Adapted from ISO/IEC 12207:2008. NOTE 2 An acquirer is a stakeholder that acquires or procures a product or service from a supplier. Other terms commonly used for an acquirer are buyer, customer, owner, or purchaser. ■	N8780: 1st CD 29147: 2010-06-10
supplier	organization or an individual that enters into an agreement with the acquirer for the supply of a service ■	N8638: 3rd WD 27036: 2010-08-13
switch	device which provides connectivity between networked devices by means of internal switching mechanisms NOTE Switches are distinct from other local area network interconnection devices (e.g. a hub) as the technology used in switches sets up connections on a point-to-point basis. This ensures the network traffic is only seen by the addressed network devices and enables several connections to exist simultaneously routing. [ISO/IEC 18028-1] ■	ISO/IEC 18043: 2006-06-15 (1st ed.)
switch	device which provides connectivity between networked devices by means of internal switching mechanisms, with the switching technology typically implemented at layer 2 or layer 3 of the OSI reference model NOTE Switches are distinct from other local area network interconnection devices (e.g. a hub) as the technology used in switches sets up connections on a point to point basis. ■	ISO/IEC 27033-1: 2009-12-15 (1st ed.)
symmetric cipher	alternative term for symmetric encryption system. ■	ISO/IEC 18033-1: 2005-02-01 (1st ed.)

Term	Definition	ISO/IEC JTC 1/SC 27 Document
symmetric cipher	cipher based on symmetric cryptographic techniques that uses the same secret key for both the encryption and decryption algorithms [ISO/IEC 18033-1] ■	ISO/IEC 18033-2: 2006-05-01 (1st ed.)
symmetric cipher	cipher based on symmetric cryptographic techniques that uses the same secret key for both the encryption and decryption algorithms [ISO/IEC 18033-1] ■	N8751: FCD 29150: 2010-06-10
symmetric cryptographic technique	cryptographic technique that uses the same secret key for both the originator's and the recipient's transformation NOTE Without knowledge of the secret key, it is computationally infeasible to compute either the originator's or the recipient's transformation. ■	ISO/IEC 9798-1: 2010-07-01 (3rd ed.)
symmetric cryptographic technique	cryptographic technique that uses the same secret key for both the originator's and the recipient's transformation. Without knowledge of the secret key, it is computationally infeasible to compute either the originator's or the recipient's transformation. NOTE Examples of symmetric cryptographic techniques include symmetric ciphers and Message Authentication Codes (MACs). In a symmetric cipher, the same secret key is used to encrypt and decrypt data. In a MAC scheme, the same secret key is used to generate and verify MACs. ■	ISO/IEC 18033-1: 2005-02-01 (1st ed.)
symmetric cryptographic technique	cryptographic technique that uses the same secret key for both the originator's and the recipient's transformation NOTE 1 Without knowledge of the secret key, it is computationally infeasible to compute either the originator's or the recipient's transformation. NOTE 2 Examples of symmetric cryptographic techniques include symmetric ciphers and Message Authentication Codes (MACs). In a symmetric cipher, the same secret key is used to encrypt and decrypt data. In a MAC scheme, the same secret key is used to generate and verify MACs. ■	N8751: FCD 29150: 2010-06-10
symmetric cryptographic technique	cryptographic technique that uses the same secret key for both the originator's and the recipient's transformation NOTE Without knowledge of the secret key, it is computationally infeasible to compute either the originator's or the recipient's transformation. ■	ISO/IEC FDIS 11770-1: 2010-07-26
symmetric cryptographic technique	cryptographic technique that uses the same secret key for both the encryption and the decryption transformations system, and associated programs, and data ■	N8776: 2nd WD 19790: 2010-07-16
symmetric encipherment system	alternative term for symmetric encryption system. ■	ISO/IEC 18033-1: 2005-02-01 (1st ed.)
symmetric encryption algorithm	encryption algorithm that uses the same secret key for both the originator's and the recipient's transformation ■	ISO/IEC 9798-1: 2010-07-01 (3rd ed.)

Term	Definition	ISO/IEC JTC 1/SC 27 Document
symmetric encryption system	encryption system based on symmetric cryptographic techniques that uses the same secret key for both the encryption and decryption algorithms. ■	ISO/IEC 18033-1: 2005-02-01 (1st ed.)
symmetric encryption system	encryption system based on symmetric cryptographic techniques that uses the same secret key for both the encryption and decryption algorithms [ISO/IEC 18033-1] ■	ISO/IEC 19772: 2009-02-15 (1st ed.)
symmetric key based key establishment mechanism for multiple entities	process of establishing a *shared secret key* between all active entities, using symmetric cryptographic techniques ■	N8743: 2nd CD 11770-5: 2010-07-29
synchronous stream cipher	stream cipher with the property that the keystream symbols are generated as a function of a secret key, and are independent of the plaintext and ciphertext. ■	ISO/IEC 18033-1: 2005-02-01 (1st ed.)
system	discrete, distinguishable entity with a physical existence and a defined purpose, completely composed of integrated, interacting components, each of which does not individually comply with the required overall purpose NOTE 1 Adapted from ISO/IEC 15288. NOTE 2 In practice, a system is "in the eye of the beholder" and the interpretation of its meaning is frequently clarified by the use of an associative noun (e.g. product system, aircraft system). Alternatively the word system may be substituted simply by a context dependent synonym (e.g. product, aircraft), though this may then obscure a system principles perspective. NOTE 3 The system may need other systems during its life cycle to meet its requirements. For example, an operational system may need a system for conceptualization, development, production, operation, support or disposal. ■	ISO/IEC 21827: 2008-10-15 (2nd ed.)
system	specific IT installation, with a particular purpose and operational environment [ISO/IEC 15408–1]. a) A combination of interacting elements organized to achieve one or more stated purposes [ISO/IEC 15288]. NOTE 1. A system may be considered as a product and/or as the services it provides [ISO/IEC 15288]. NOTE 2. In practice, the interpretation of its meaning is frequently clarified by the use of an associative noun, e.g. aircraft system. Alternatively the word system may be substituted simply by a context dependent synonym, e.g. aircraft, though this may then obscure a system principles perspective [ISO/IEC 15288]. ■	ISO/IEC TR 15443-1: 2005-02-01 (1st ed.)
system	combination of interacting elements organized to achieve one or more stated purposes [ISO/IEC 15288:2008] ■	N8780: 1st CD 29147: 2010-06-10

Term	Definition	ISO/IEC JTC 1/SC 27 Document
system	combination of interacting elements organized to achieve one or more stated purposes [] a specific IT installation, with a particular purpose and operational environment [ISO 15408-1] ■	N8732: 3rd WD 29193: 2010-08-06
system life cycle	evolution with time of the system from conception through to disposal [ISO/IEC 15288]. ■	ISO/IEC TR 15443-1: 2005-02-01 (1st ed.)
system parameters	choice of parameters that selects a particular cryptographic scheme or function from a family of cryptographic schemes or functions ■	ISO/IEC 18033-2: 2006-05-01 (1st ed.)
system software	general purpose software within the cryptographic boundary designed to facilitate the operation of the cryptographic module [ISO/IEC 19790:2006, 3.70] EXAMPLES Operating system, compilers or utility programs. ■	ISO/IEC 24759: 2008-07-01 (1st ed.)
system target of evaluation	operational system that is being operated in accordance with its operational guidance, including both technical and operational controls NOTE Operational controls form part of the operational environment. They are not evaluated in ISO/IEC 15408 evaluation. ■	ISO/IEC TR 19791: 2010-04-01 (2nd ed.)
system time	time generated by the system clock and used by the operating system, not the time computed by the operating system NOTE The time generated by the system clock and the time computed by the operating system may not be synchronized. ■	N8640: 3rd WD 27037: 2010-05-31
tag	result of a MAC algorithm, adjoined to a possibly encrypted message to provide integrity protection ■	N8734: 3rd CD 9797-3: 2010-06-16
tamper detection	automatic determination by a cryptographic module that an attempt has been made to compromise the security of the module ■	N8776: 2nd WD 19790: 2010-07-16
tamper evidence	observable indication that an attempt has been made to compromise the security of a cryptographic module ■	ISO/IEC 24759: 2008-07-01 (1st ed.)
tamper evidence	the external indication that an attempt has been made to compromise the security of a cryptographic module NOTE The evidence of the tamper attempt should be observable by a human operator ■	N8776: 2nd WD 19790: 2010-07-16
tamper response	automatic action taken by a cryptographic module when tamper detection has occurred ■	N8776: 2nd WD 19790: 2010-07-16
tampering	act of intentionally making or allowing change(s) to a digital evidence ■	N8640: 3rd WD 27037: 2010-05-31
target of evaluation TOE	set of software, firmware and/or hardware possibly accompanied by guidance ■	N8784: 1st WD 20004: 2010-08-06

Term	Definition	ISO/IEC JTC 1/SC 27 Document
targeted level of trust	name or label of a set of Application Security Controls deemed necessary by the application owner for bringing the risk of a specific application down to an acceptable (or tolerable) level, as determined by an application security risk analysis ■	N8632: FCD 27034-1: 2010-05-27
task	collection of one or more scenarios. [Neumann/Strembeck] ■	N8812: 3rd WD 29146: 2010-07-14
technical controls	security controls (i.e., safeguards and countermeasures) for an information system that are primarily implemented and executed by the information system through mechanisms contained in the hardware, software, or firmware components of the system [NIST SP 800-53] ■	ISO/IEC TR 19791: 2010-04-01 (2nd ed.)
telecommunication records	information concerning the parties in a communication excluding the contents of the communication, and the time, and duration of the telecommunication took place. {ITU-T format} ■	ISO/IEC 27011/x.1051: 2008-12-15 (1st ed)
telecommunications applications	applications such as e-mail that are accessed by end-users and are built upon the network-based services. {ITU-T format} ■	ISO/IEC 27011/x.1051: 2008-12-15 (1st ed)
telecommunications business	business to provide telecommunications services in order to meet the demand of others. {ITU-T format} ■	ISO/IEC 27011/x.1051: 2008-12-15 (1st ed)
telecommunications equipment room	part of general building such as a room where equipment for providing telecommunications business are sited. {ITU-T format} ■	ISO/IEC 27011/x.1051: 2008-12-15 (1st ed)
telecommunications facilities	machines, equipment, wire and cables, physical buildings or other electrical facilities for the operation of telecommunications. {ITU-T format} ■	ISO/IEC 27011/x.1051: 2008-12-15 (1st ed)
telecommunications organizations	business entities who provide telecommunications services in order to meet the demand of others. {ITU-T format} ■	ISO/IEC 27011/x.1051: 2008-12-15 (1st ed)
telecommunications service customer	person or organization who enters into a contract with telecommunications organizations to be offered telecommunications services by them. {ITU-T format} ■	ISO/IEC 27011/x.1051: 2008-12-15 (1st ed)
telecommunications service user	person or organization who utilizes telecommunications services. ■	ISO/IEC 27011/x.1051: 2008-12-15 (1st ed)
telecommunications services	communications using telecommunications facilities, or any other means of providing communications either between telecommunications service users or telecommunications service customers. {ITU-T format} ■	ISO/IEC 27011/x.1051: 2008-12-15 (1st ed)

Term	Definition	ISO/IEC JTC 1/SC 27 Document
temporal cohesion	characteristics of a module containing functions that need to be executed at about the same time NOTE 1 Adapted from [IEEE Std 610.12-1990]. NOTE 2 Examples of temporally cohesive modules include initialization, recovery, and shutdown modules. ■	ISO/IEC 15408-1: 2009-12-15 (3rd ed.)
temporary key values TKV	any temporary variables or memory locations used to store intermediate SSP components during cryptographic calculations. These values include, but are not limited to, memory locations or variables used to store key schedule values, intermediate values of modular exponentiation operations, shared secrets and intermediate keyed digest values ■	N8776: 2nd WD 19790: 2010-07-16
terminal facilities	telecommunications facilities which are to be connected to one end of telecommunications circuit facilities and part of which is to be installed on the same premises (including the areas regarded as the same premises) or in the same building where any other part thereof is also to be installed. {ITU-T format} ■	ISO/IEC 27011/x.1051: 2008-12-15 (1st ed)
Test Access Points - TAP	typically passive devices that do not install any overhead on the packet; they also increase the level of the security as they make the data collection interface invisible to the network, where a switch can still maintain layer 2 information about the port. A TAP also gives the functionality of multiple ports so network issues can be debugged without losing the IDS capability. ■	ISO/IEC 18043: 2006-06-15 (1st ed.)
test crew	set of test subjects gathered for an evaluation NOTE Definition from [1]. ■	ISO/IEC 19792: 2009-08-01 (1st ed.)
third party	any natural or legal person, public authority, agency or any other body other than the PII principal, the PII controller and the PII processor, and the persons who are authorized to process the data under the direct authority of the PII controller or the PII processor ■	N8806: 4th CD 29100: 2010-06-10
threat	see risk source (2.57) ■	N8718: 1st WD 27000: 2010-05-27
threat	capabilities, intentions and attack methods of adversaries, or any circumstance or event, whether originating externally or internally, that has the potential to cause harm to information or to a program or system, or to cause these to harm others ■	ISO/IEC 21827: 2008-10-15 (2nd ed.)
threat	potential cause of an unwanted incident, which may result in harm to a system, individual or organization NOTE Adapted from ISO/IEC 27000:2009 ■	N8624: 2nd CD 27032: 2010-06-15

Term	Definition	ISO/IEC JTC 1/SC 27 Document
threat agent	originator and/or initiator of deliberate or accidental man-made threats ■	ISO/IEC 21827: 2008-10-15 (2nd ed.)
threat agent	entity that can adversely act on assets ■	ISO/IEC 15408-1: 2009-12-15 (3rd ed.)
threat agent	entity that can adversely act on assets ■	N8784: 1st WD 20004: 2010-08-06
threat modelling	provide users an understanding of the attributes of the software, identify attackers within the given operating environment and their goals and techniques, and identify possible future patterns and behaviors. The threat model is used to construct an attack profile. Vulnerabilities are then identified based on the attack history and threat model results. making or constructing schematic representation of a system, theory, phenomenon that provide users better understanding of the attributes of the software, mechanisms how attackers can exploit those attributes, possible foreseeable future problems and behaviours Note: Threat model is used to construct an attack profile. Vulnerabilities are identified based on the attack history and threat model results ■	N8732: 3rd WD 29193: 2010-08-06
threshold	boundary value of the comparison score used by the comparison application to automatically generate the matching decision ■	ISO/IEC 19792: 2009-08-01 (1st ed.)
time referencing scheme	time variant parameter which denotes a point in time with respect to a common time reference [ISO/IEC 11770-1:1996] ■	ISO/IEC 18014-1: 2008-09-01 (2nd ed.)
time stamp	time variant parameter which denotes a point in time with respect to a common time reference [ISO/IEC 18014-1:2008] ■	ISO/IEC 9798-2: 2008-12-15 (3rd ed.)
time stamp	time variant parameter which denotes a point in time with respect to a common reference NOTE See also Annex B. ■	ISO/IEC 9798-1: 2010-07-01 (3rd ed.)
time stamp	process of issuing a new time-stamp token to extend the validity period of an earlier time-stamp token ■	ISO/IEC 18014-1: 2008-09-01 (2nd ed.)
time stamp	time variant parameter which denotes a point in time with respect to a common reference [ISO/IEC 9798-1] ■	N8762: 1st WD 20009-1: 2010-07-13
time stamp	time variant parameter which denotes a point in time with respect to a common reference [ISO/IEC 9798-1] ■	N8763: 1st WD 20009-2: 2010-06-20
time stamp	data item which denotes a point in time with respect to a common time reference [ISO/IEC 11770-3:2008] ■	ISO/IEC FDIS 11770-1: 2010-07-26
time stamp	time variant parameter which denotes a point in time with respect to a common time reference [ISO/IEC 11770-1:1996] ■	N8642: 2nd PDTR 29149: 2010-06-22
time stamp	Time variant parameter which denotes a point in time with respect to a common reference. ■	N8810: 1st CD 29115 | X.eaa: 2010-06-10

Term	Definition	ISO/IEC JTC 1/SC 27 Document
time stamp	data item which denotes a point in time with respect to a common time reference ■	ISO/IEC 11770-3: 2008-07-15 (2nd ed.)
time stamp renewal	process of issuing a new time stamp to extend the validity period of an earlier time stamp [ISO/IEC 18014-1:2008] ■	N8642: 2nd PDTR 29149: 2010-06-22
time stamping authority	trusted third party trusted to provide evidence which includes the time when the secure time stamp is generated [ISO/IEC 13888-1:2004] ■	ISO/IEC 11770-3: 2008-07-15 (2nd ed.)
time stamping service	service which attests the existence of electronic data at a precise instant of time. NOTE – Time stamping services are useful and probably indispensable to support long-term validation of signatures. They will be defined in a separate document. ■	ISO/IEC 15945: 2002-02-01 (1st ed.)
time variant parameter	data item used to verify that a message is not a replay, such as a random number, a time stamp or a sequence number NOTE See also Annex B. ■	ISO/IEC 9798-1: 2010-07-01 (3rd ed.)
time variant parameter	entity which possesses data it wants to be time-stamped NOTE A requester can also be a trusted third party including a time-stamping authority. ■	ISO/IEC 18014-1: 2008-09-01 (2nd ed.)
time variant parameter	data item used to verify that a message is not a replay, such as a random number, a sequence number, or a time stamp [ISO/IEC 9798-1] ■	N8762: 1st WD 20009-1: 2010-07-13
time variant parameter	data item such as a random number, a sequence number, or a time stamp [ISO/IEC 11770-3: 2008] ■	ISO/IEC FDIS 11770-1: 2010-07-26
time variant parameter	data item used to verify that a message is not a replay, such as a random number, sequence number, or a time stamp ■	ISO/IEC 11770-2: 2008-06-15 (2nd ed.)
time variant parameter - TVP	data item used to verify that a message is not a replay, such as a random number, a sequence number, or a time stamp NOTE If time stamps are used, secure and synchronized time clocks are required. If sequence numbers are used, the ability to maintain and verify bilateral counters is required. ■	ISO/IEC 11770-3: 2008-07-15 (2nd ed.)
time-signal emission	data structure containing a verifiable binding between a data items' representation and a time-value NOTE A time-stamp token can also include additional data items in the binding. ■	ISO/IEC 18014-1: 2008-09-01 (2nd ed.)
timestamp	time variant parameter which denotes a point in time with respect to a common time reference [ISO/IEC 11770-1:1996] ■	N8640: 3rd WD 27037: 2010-05-31
time-stamp	time variant parameter which denotes a point in time with respect to a common time reference [ISO/IEC 18014-1] ■	ISO/IEC 13888-1: 2009-07-15 (3rd ed)

Term	Definition	ISO/IEC JTC 1/SC 27 Document
time-stamp	time variant parameter which denotes a point in time with respect to a common time reference [ISO/IEC 18014] ■	ISO/IEC FDIS 13888-2: 2010-08-06
time-stamp renewal	entity which possesses data and wants to verify that it has a valid time stamp bound to it NOTE The verification process can be performed by the verifier itself or by a trusted third party. ■	ISO/IEC 18014-1: 2008-09-01 (2nd ed.)
time-stamp requester	trusted third party trusted to provide a time-stamping service ■	ISO/IEC 18014-1: 2008-09-01 (2nd ed.)
time-stamp requester	entity which possesses data it wants to be time-stamped [ISO/IEC 18014-1:2008, definition 3.14] ■	ISO/IEC 18014-2: 2009-12-15 (2nd ed.)
time-stamp requester	entity which possesses data it wants to be time-stamped NOTE A requester can also be a trusted third party including a time-stamping authority. [ISO/IEC 18014-1:2008] ■	N8642: 2nd PDTR 29149: 2010-06-22
time-stamp token - TST	service providing evidence that a data item existed before a certain point in time ■	ISO/IEC 18014-1: 2008-09-01 (2nd ed.)
time-stamp token - TST	data structure containing a verifiable cryptographic binding between a data item's representation and a timevalue NOTE A time-stamp token can also include additional data items in the binding. [ISO/IEC 18014-1:2008, definition 3.15] ■	ISO/IEC 18014-2: 2009-12-15 (2nd ed.)
time-stamp token - TST	data structure containing a verifiable cryptographic binding between a data items' representation and a timevalue NOTE A time-stamp token can also include additional data items in the binding. [ISO/IEC 18014-1: 2008, definition 3.15] ■	ISO/IEC 18014-3: 2009-12-15 (2nd ed.)
time-stamp token - TST	data structure containing a verifiable binding between a data items' representation and a time-value NOTE A time-stamp token can also include additional data items in the binding. [ISO/IEC 18014-1:2008] ■	N8642: 2nd PDTR 29149: 2010-06-22
time-stamp token - TST	data structure containing a verifiable binding between a data items' representation and a time-value NOTE A time-stamp token can also include additional data items in the binding. [ISO/IEC 18014-1:2008] ■	N8640: 3rd WD 27037: 2010-05-31
time-stamp verifier	data item used by an entity to verify that a message is not a replay, such as a random number, a sequence number, or a time stamp [ISO/IEC 11770-1:1996] ■	ISO/IEC 18014-1: 2008-09-01 (2nd ed.)
time-stamp verifier	entity which possesses data and wants to verify that it has a valid time-stamp bound to it NOTE The verification process can be performed by the verifier itself or by a trusted third party. [ISO/IEC 18014-1:2008, definition 3.16] ■	ISO/IEC 18014-2: 2009-12-15 (2nd ed.)

Term	Definition	ISO/IEC JTC 1/SC 27 Document
time-stamp verifier	entity which possesses data and wants to verify that it has a valid time-stamp bound to it NOTE The verification process may be performed by the verifier itself or by a Trusted Third Party. [ISO/IEC 18014-1:2008] ■	N8642: 2nd PDTR 29149: 2010-06-22
time-stamping authority	trusted third party trusted to provide a time-stamping service [ISO/IEC 18014-1] ■	ISO/IEC 13888-1: 2009-07-15 (3rd ed)
time-stamping authority	trusted third party trusted to provide a time-stamping service [ISO/IEC 18014] ■	ISO/IEC FDIS 13888-2: 2010-08-06
time-stamping authority - TSA	security authority, or its agent, trusted by other entities with respect to security-related activities [ISO/IEC 11770-3:1999] ■	ISO/IEC 18014-1: 2008-09-01 (2nd ed.)
time-stamping authority - TSA	trusted third party trusted to provide a time-stamping service [ISO/IEC 18014-1:2008, definition 3.17] ■	ISO/IEC 18014-2: 2009-12-15 (2nd ed.)
time-stamping authority - TSA	trusted third party trusted to provide a time-stamping service [ISO/IEC 18014-1: 2008, definition 3.17] ■	ISO/IEC 18014-3: 2009-12-15 (2nd ed.)
time-stamping authority - TSA	trusted third party trusted to provide a time-stamping service [ISO/IEC 18014-1:2008] ■	N8642: 2nd PDTR 29149: 2010-06-22
time-stamping policy	concepts for describing temporal characteristics of geographic information, about the use of an atomic clock, the clock of the GPS signal, etc. NOTE See ISO 19108:2002. ■	ISO/IEC 18014-1: 2008-09-01 (2nd ed.)
time-stamping policy	named set of rules that indicates the applicability of a time-stamp token to a particular community or class of application with common security requirements ■	ISO/IEC 18014-2: 2009-12-15 (2nd ed.)
time-stamping policy	named set of rules that indicates the applicability of a time-stamp token to a particular community or class of application with common security requirements [ISO/IEC 18014-1:2008] ■	N8642: 2nd PDTR 29149: 2010-06-22
time-stamping service - TSS	standard time signals are emitted with reference to UTC according to standard schemes [ITU-R TF.460-6] ■	ISO/IEC 18014-1: 2008-09-01 (2nd ed.)
time-stamping service - TSS	service providing evidence that a data item existed before a certain point in time [ISO/IEC 18014-1:2008, definition 3.18] ■	ISO/IEC 18014-2: 2009-12-15 (2nd ed.)
time-stamping service - TSS	service providing evidence that a data item existed before a certain point in time [ISO/IEC 18014-1: 2008, definition 3.18] ■	ISO/IEC 18014-3: 2009-12-15 (2nd ed.)
time-stamping service - TSS	service providing evidence that a data item existed before a certain point in time [ISO/IEC 18014-1:2008] ■	N8642: 2nd PDTR 29149: 2010-06-22
time-stamping unit - TSU	set of hardware and software which is managed as a unit and generates time-stamp tokens ■	ISO/IEC 18014-2: 2009-12-15 (2nd ed.)
target of evaluation - TOE	set of software, firmware and/or hardware possibly accompanied by guidance ■	ISO/IEC 15408-1: 2009-12-15 (3rd ed.)

Term	Definition	ISO/IEC JTC 1/SC 27 Document
TOE evaluation	assessment of a TOE against defined criteria ■	ISO/IEC 15408-1: 2009-12-15 (3rd ed.)
TOE evaluation	assessment of a TOE against defined criteria ■	N8784: 1st WD 20004: 2010-08-06
TOE resource	anything useable or consumable in the TOE ■	ISO/IEC 15408-1: 2009-12-15 (3rd ed.)
TOE security functionality	combined functionality of all hardware, software, and firmware of a TOE that must be relied upon for the correct enforcement of the SFRs ■	ISO/IEC 15408-1: 2009-12-15 (3rd ed.)
token	message consisting of data fields relevant to a particular communication and which contains information that has been produced using a cryptographic technique ■	ISO/IEC 9798-5: 2009-12-15 (3rd ed.)
token	message consisting of data fields relevant to a particular communication and which contains information that has been transformed using a cryptographic technique ■	ISO/IEC 9798-1: 2010-07-01 (3rd ed.)
token	message consisting of data fields relevant to a particular communication and which contains information that has been transformed using a cryptographic technique [ISO/IEC 9798-1] ■	N8762: 1st WD 20009-1: 2010-07-13
token	message consisting of data fields relevant to a particular communication and which contains information that has been transformed using a cryptographic technique [ISO/IEC 9798-1] ■	N8763: 1st WD 20009-2: 2010-06-20
token	message consisting of data fields relevant to a particular communication and which contains information that has been produced using a cryptographic technique ■	N8759: 2nd WD 29192-4: 2010-06-15
token	physical device storing biometric reference and in some cases performing on-board biometric comparison such as smart cards, USB memory sticks or RFID chip in e-passport ■	N8802: FCD 24745: 2010-05-19
trace key	set of private data elements specific to an entity and usable only by this entity in the trace process NOTE Trace key is only available to an authorized entity with trace privilege. ■	N8763: 1st WD 20009-2: 2010-06-20
trace process	process which takes as input an anonymous signature, the trace key and the domain parameters, and which gives as output a user identifiable information ■	N8763: 1st WD 20009-2: 2010-06-20
trace, verb	perform an informal correspondence analysis between two entities with only a minimal level of rigour ■	ISO/IEC 15408-1: 2009-12-15 (3rd ed.)
tracing	simple directional relation between two sets of entities, which shows which entities in the first set correspond to which entities in the second ■	N8912: Corrected 18045: 2010-09-15

Term	Definition	ISO/IEC JTC 1/SC 27 Document
trailer	string of bits of length one or two octets, concatenated to the end of the recoverable part of the message during message representative production ■	ISO/IEC FDIS 9796-2: 2010-09-10
trailer	optional bit string on the right of a representative ■	ISO/IEC 14888-2: 2008-04-15 (2nd ed.)
transaction	sequence of attempts on the part of a user for the purposes of an enrolment, biometric verification or biometric identification NOTE There are three types of transaction: an enrolment sequence, resulting in an enrolment or a failure-to-enrol; a verification sequence, resulting in a verification decision; or an identification sequence, resulting in an identification decision. ■	ISO/IEC 19792: 2009-08-01 (1st ed.)
transaction	discrete event between an entity and service provider that supports a business or programmatic purpose. ■	N8810: 1st CD 29115 | X.eaa: 2010-06-10
transfers outside of the TOE	TSF mediated communication of data to entities not under the control of the TSF ■	ISO/IEC 15408-1: 2009-12-15 (3rd ed.)
translation	describes the process of describing security requirements in a standardized language NOTE Use of the term translation in this context is not literal and does not imply that every SFR expressed in standardized language can also be translated back to the security objectives. ■	ISO/IEC 15408-1: 2009-12-15 (3rd ed.)
Transport Layer Security Protocol - TLS	the successor of SSL is an official Internet Protocol (RFC 2246). ■	ISO/IEC 18028-4: 2005-04-01 (1st ed.)
tree	directed graph in which any two vertices are connected by exactly one path NOTE It contains more than one ancestor node. ■	N8743: 2nd CD 11770-5: 2010-07-29
trial division	Trial division of a number *N* means checking all prime numbers smaller than or equal to $\sqrt{N}$ to see if they divide *N*. ■	ISO/IEC 18032: 2005-01-15 (1st ed.)
trigger	event that causes the system to initiate a response NOTE also known as triggering event. ■	N8622: PreFDIS 27031: 2010-08-18
trivial divisor	Any integer *N* is always divisible by 1, -1, *N* and –*N*. These numbers are the trivial divisors of *N*. ■	ISO/IEC 18032: 2005-01-15 (1st ed.)
trojan trojan horse	malware that appears to perform a desirable function ■	N8624: 2nd CD 27032: 2010-06-15
trojan horse	malicious program that masquerades as a benign application ■	ISO/IEC 18043: 2006-06-15 (1st ed.)
trust	relationship between two elements, a set of activities and a security policy in which element x trusts element y if and only if x has confidence that y will behave in a well defined way (with respect to the activities) that does not violate the given security policy NOTE Adapted from ISO/IEC 10181-1, 3.3.28.] ■	ISO/IEC 13888-1: 2009-07-15 (3rd ed)

Term	Definition	ISO/IEC JTC 1/SC 27 Document
trust anchor	trusted information, which includes a public key algorithm, a public key value, an issuer name, and optionally, other parameters EXAMPLE Other parameters may include but not limited to a validity period NOTE A trust anchor may be provided in the form of a self-signed certificate ■	N8776: 2nd WD 19790: 2010-07-16
Trust Framework	set of technical, operational, and legal requirements, and enforcement mechanisms for parties exchanging identity information. ■	N8810: 1st CD 29115 | X.eaa: 2010-06-10
trusted channel	means by which a TSF and another trusted IT product can communicate with necessary confidence ■	ISO/IEC 15408-1: 2009-12-15 (3rd ed.)
trusted channel	trusted and safe communication link established between the cryptographic module and a sender or receiver to securely communicate unprotected plaintext CSPs, key components and authentication data NOTE A trusted channel protects against eavesdropping, as well as physical or logical tampering by unwanted operators/entities, processes or other devices, between the module's defined input or output ports and along the communication link with the intended endpoint ■	N8776: 2nd WD 19790: 2010-07-16
trusted IT product	IT product, other than the TOE, which has its security functional requirements administratively coordinated with the TOE and which is assumed to enforce its security functional requirements correctly NOTE An example of a trusted IT product would be one that has been separately evaluated. ■	ISO/IEC 15408-1: 2009-12-15 (3rd ed.)
Trusted Key Generation Centre - KGC	trusted third party, which, in an identity-based signature mechanism, generates a private signature key for each signing entity ■	ISO/IEC 14888-3: 2006-11-15 (2nd ed.)
trusted path	means by which a user and a TSF can communicate with the necessary confidence ■	ISO/IEC 15408-1: 2009-12-15 (3rd ed.)
trusted third party	security authority, or its agent, trusted by other entities with respect to security-related activities NOTE 1 Adapted from ISO/IEC 10181-1, 3.3.30. NOTE 2 In the context of ISO/IEC 13888, a trusted third party is trusted by the originator, the recipient, and/or the delivery authority for the purposes of non-repudiation, and by another party such as an adjudicator. ■	ISO/IEC 13888-1: 2009-07-15 (3rd ed)

Term	Definition	ISO/IEC JTC 1/SC 27 Document
trusted third party	security authority or its agent, trusted by other entities with respect to security related activities NOTE In the context of ISO/IEC 9798, a trusted third party is trusted by a claimant and/or a verifier for the purposes of authentication. ■	ISO/IEC 9798-1: 2010-07-01 (3rd ed.)
trusted third party	security authority, or its agent, trusted by other entities with respect to security related activities [ISO/IEC 10181-1:1996, definition 3.3.30] ■	ISO/IEC 18014-2: 2009-12-15 (2nd ed.)
trusted third party	security authority or its agent that is trusted with respect to some security-relevant activities (in the context of a security policy) [ISO/IEC 10181-1:1996] ■	ISO/IEC FDIS 11770-1: 2010-07-26
trusted third party	security authority, or its agent, trusted by other entities with respect to security related activities [ISO/IEC 10181-1:1996] ■	ISO/IEC 11770-3: 2008-07-15 (2nd ed.)
trusted third party - TTP	security authority, or its agent, trusted by other entities with respect to security-related activities [ISO/IEC 18014-1:2008] ■	ISO/IEC 9798-2: 2008-12-15 (3rd ed.)
trusted third party - TTP	set of rules that indicates the applicability of a time-stamp token to a particular community and/or class of application with common security requirements ■	ISO/IEC 18014-1: 2008-09-01 (2nd ed.)
trusted third party - TTP	security authority, or its agent, trusted by other entities with respect to security related activities [ISO/IEC 10181-1:1996, definition 3.3.30] ■	ISO/IEC 18014-3: 2009-12-15 (2nd ed.)
trusted third party - TTP	security authority, or its agent, trusted by other entities with respect to security related activities [ISO/IEC 10181-1:1996] ■	N8642: 2nd PDTR 29149: 2010-06-22
trusted third party - TTP	Security authority or its agent, trusted by other entities with respect to security related activities. NOTE - A trusted third party is trusted by a claimant and/or a verifier for the purposes of authentication. ■	N8810: 1st CD 29115 | X.eaa: 2010-06-10
trusted time-stamp	time-stamp assured by a time-stamping authority ■	ISO/IEC 13888-1: 2009-07-15 (3rd ed)
TSF data	data for the operation of the TOE upon which the enforcement of the SFR relies ■	ISO/IEC 15408-1: 2009-12-15 (3rd ed.)
TSF interface	means by which external entities (or subjects in the TOE but outside of the TSF) supply data to the TSF, receive data from the TSF and invoke services from the TSF ■	ISO/IEC 15408-1: 2009-12-15 (3rd ed.)
TSF self-protection	security architecture property whereby the TSF cannot be corrupted by non-TSF code or entities ■	ISO/IEC 15408-1: 2009-12-15 (3rd ed.)

Term	Definition	ISO/IEC JTC 1/SC 27 Document
tunnel	data path between networked devices which is established across an existing network infrastructure NOTE Tunnels can be established using techniques such as protocol encapsulation, label switching, or virtual circuits. ■	ISO/IEC 27033-1: 2009-12-15 (1st ed.)
unallocated space	area on electronic media that is not allocated space and potentially containing data from files which previously occupied it ■	N8640: 3rd WD 27037: 2010-05-31
unbiased source	source of bit strings (or numbers) from a sample space is said to be unbiased if all potential bit strings (or numbers) have the same possibility of being chosen NOTE 1 Equivalently, if the sample space consists of *r* elements, all elements will occur with probability 1/*r*. NOTE 2 This term can be contrasted to biased source. ■	N8745: FCD 18031: 2010-05-18
Uniform Resource Locator - URL	address scheme for web services. ■	ISO/IEC 18028-4: 2005-04-01 (1st ed.)
unilateral authentication	entity authentication that provides one entity with assurance of the other's identity but not vice versa [ISO/IEC 9798-1:1997, definition 3.3.33] ■	ISO/IEC 9798-5: 2009-12-15 (3rd ed.)
unilateral authentication	entity authentication which provides one entity with assurance of the other's identity but not vice versa ■	ISO/IEC 9798-1: 2010-07-01 (3rd ed.)
unilateral authentication	entity authentication which provides one entity with assurance of the other's identity but not vice versa [ISO/IEC 9798-1] ■	N8762: 1st WD 20009-1: 2010-07-13
unilateral authentication	entity authentication that provides one entity with assurance of the other's identity but not vice versa [ISO/IEC 9798-1:1997] ■	N8759: 2nd WD 29192-4: 2010-06-15
Uninterruptible Power Supply - UPS	usually a battery-based system to protect devices against power outages, sags and surges. ■	ISO/IEC 18028-4: 2005-04-01 (1st ed.)
unit of measurement	particular quantity, defined and adopted by convention, with which other quantities of the same kind are compared in order to express their magnitude relative to that quantity [ISO/IEC 15939:2007] ■	ISO/IEC 27004: 2009-12-15 (1st ed.)
universal hash-function	family of functions mapping strings of bits to fixed-length strings of bits, indexed by a parameter called the key, satisfying the property that for all distinct inputs, the probability over all keys that the outputs collide is small NOTE Universal hash functions were introduced by Carter and Wegman[4], and their application in MAC algorithms was first described by Wegman and Carter [8]. ■	N8734: 3rd CD 9797-3: 2010-06-16

Term	Definition	ISO/IEC JTC 1/SC 27 Document
unlinkability	property of two or more biometric references stemming from the same data subject being, from an adversary's perspective, not more related after his observation of these references than they are related based on his a-priori knowledge EXAMPLE An adversary cannot successfully link biometric references back to the same data subject. ■	N8802: FCD 24745: 2010-05-19
unlinkable authentication	method of verifying the user's access privilege where one can not determine if two transactions are authenticating a same user or not. ■	N8816: 3rd WD 29191: 2010-06-01
unsigncrypt	to apply unsigncryption on a ciphertext ■	N8751: FCD 29150: 2010-06-10
unsigncryption	verification and decryption of a ciphertext by a cryptographic algorithm ■	N8751: FCD 29150: 2010-06-10
unsigncryption algorithm	one of the three component algorithms of a signcryption mechanism which takes as input a ciphertext, a recipient's public and private key pair, a sender's public key and other data, outputs a pair consisting of either a symbolic value ACCEPT and a plaintext, or a symbolic value REJECT and the null string ■	N8751: FCD 29150: 2010-06-10
unsolicited email	email that is not welcome, or was not requested, or invited ■	N8624: 2nd CD 27032: 2010-06-15
user	Person or organization who utilizes information processing facilities or systems, e.g., employee, contractor or third party user. {ITU-T format} ■	ISO/IEC 27011/x.1051: 2008-12-15 (1st ed)
user	person interacting with a biometric system ■	ISO/IEC 19792: 2009-08-01 (1st ed.)
user	individual or organization that benefits from a product or online service during its utilization NOTE 1 Adapted from ISO/IEC 12207:2008. NOTE 2 The role of user and the role of operator may be vested, simultaneously or sequentially, in the same individual or organization. ■	N8780: 1st CD 29147: 2010-06-10
user	an individual or process (subject) acting on behalf of the individual that accesses a cryptographic module in order to obtain cryptographic services ■	N8776: 2nd WD 19790: 2010-07-16
user	person who uses or operates something [Concise Oxford English dictionary] NOTE For the purposes of this International Standard, the term "user" includes not only the end user, but also maintenance and operation roles, such as system administrator and database administrator. ■	N8632: FCD 27034-1: 2010-05-27
user	human being, but can be extended to include machines, networks, or intelligent autonomous agents. [ANSI-RBAC] ■	N8812: 3rd WD 29146: 2010-07-14
user data	data for the user, that does not affect the operation of the TSF ■	ISO/IEC 15408-1: 2009-12-15 (3rd ed.)

Term	Definition	ISO/IEC JTC 1/SC 27 Document
User Datagram Protocol - UDP	Internet networking protocol for connectionless communications (RFC 768). ■	ISO/IEC 18028-4: 2005-04-01 (1st ed.)
user keys	data item of a set of private signature key and public verification key ■	ISO/IEC 9796-3: 2006-09-15 (2nd ed.)
validated	assurance of tested conformance by a validation authority ■	N8776: 2nd WD 19790: 2010-07-16
validation	confirmation, through the provision of objective evidence, that the requirements for a specific intended use or application have been fulfilled ■	ISO/IEC 27004: 2009-12-15 (1st ed.)
validation	confirmation by examination and provision of objective evidence that the particular requirements for a specific intended use are fulfilled NOTE Adapted from ISO/IEC 15288. ■	ISO/IEC 21827: 2008-10-15 (2nd ed.)
validation	confirmation, through the provision of objective evidence, that requirements for a specific intended use or application have been fulfilled NOTE 1 The term "validated" is used to designate the corresponding status. NOTE 2 The use conditions for validation can be real or simulated. [ISO 9000] NOTE 3 In general, "validation" means "Are you building the right application?" ■	N8632: FCD 27034-1: 2010-05-27
validation	process to determine that presented identity information (3.2.5) associated with a particular entity (3.1.1) is applicable for the entity to be recognized in a particular domain (3.2.3) at some point in time NOTE Validation can involve checking that the required attributes are present, have the correct syntax and exist within a defined validity period. ■	N8804: 3rd CD 24760-1: 2010-06-11
validation authority	the entity that will validate the testing results for conformance to this standard ■	N8776: 2nd WD 19790: 2010-07-16
validator	<biometric verification> entity which makes a decision on whether the result of a biometric verification process is acceptable or not, based on the policy of the corresponding application, using one or more comparison decisions and possibly other information, supported by ACBio instances ■	ISO/IEC 24761: 2009-05-15 (1st ed.)
validity period	time period during which an identity or credential may be used in a transaction for authenticating an entity's authorization, identity, or attribute information within a given context. ■	N8810: 1st CD 29115 | X.eaa: 2010-06-10
varyadic	property of a function whose arity is variable ■	N8778: 3rd CD 29128: 2010-06-11

Term	Definition	ISO/IEC JTC 1/SC 27 Document
vendor	party that sells, produces or uses a biometric system and is responsible for providing the biometric system and all necessary evidence for evaluation NOTE In cases where a vendor decides to delegate certain tasks to another party (e.g. to a third party testing laboratory), this party shall be seen as a vendor as well. ■	ISO/IEC 19792: 2009-08-01 (1st ed.)
vendor	person or organisation that developed the product, or is responsible for maintaining it Editors Note: The editor request comments on the usage of the term "supplier" in the place of "vendor". The rational would be that "supplier" is the ISO/IEC definition that includes "vendor" this would align the document to use SC27 standard definitions in the document. Comments on this topic are requested. ■	N8780: 1st CD 29147: 2010-06-10
vendor	for the purpose of this standard, the vendor is the entity, group or association that submits the cryptographic module for testing and validation NOTE The vendor may or may not have designed or developed the cryptographic module but has access to all relevant documentation and design evidence ■	N8776: 2nd WD 19790: 2010-07-16
verdict	pass, fail or inconclusive statement issued by an evaluator with respect to an ISO/IEC 15408 evaluator action element, assurance component, or class NOTE Also see overall verdict. ■	N8912: Corrected 18045: 2010-09-15
verification	confirmation, through the provision of objective evidence, that specified requirements have been fulfilled [ISO 9000:2005] NOTE This could also be called compliance testing. ■	ISO/IEC 27004: 2009-12-15 (1st ed.)
verification	confirmation by examination and provision of objective evidence that specified requirements have been fulfilled NOTE Adapted from ISO/IEC 15288. ■	ISO/IEC 21827: 2008-10-15 (2nd ed.)
verification	assessment processes used to confirm that the security controls for an operational system are implemented correctly and are effective in their application ■	ISO/IEC TR 19791: 2010-04-01 (2nd ed.)

Term	Definition	ISO/IEC JTC 1/SC 27 Document
verification	confirmation, through the provision of objective evidence, that specified requirements have been fulfilled NOTE 1 The term "verified" is used to designate the corresponding status. NOTE 2 Confirmation can comprise activities such as performing alternative calculations, comparing a new design specification with a similar proven design specification, undertaking tests and demonstrations, and reviewing documents prior to issue. [ISO 9000] NOTE 3 In general, "verification" means "Are you building the application right?" ■	N8632: FCD 27034-1: 2010-05-27
verification	process of checking identity proofing information and credentials against issuers, data sources, or other internal or external resources with respect to authenticity, validity, correctness, and binding to the entity. ■	N8810: 1st CD 29115 | X.eaa: 2010-06-10
verification (biometrics)	process of confirming a claim that an individual who is the subject of a biometric capture process is the source of a claimed identity reference ■	N8802: FCD 24745: 2010-05-19
verification exponent	public key used as exponent by the claimant and the verifier ■	ISO/IEC 9798-5: 2009-12-15 (3rd ed.)
verification exponent	public exponent for verifying signed messages and sometimes also for producing signatures ■	ISO/IEC 14888-2: 2008-04-15 (2nd ed.)
verification key	value required to verify a MAC ■	ISO/IEC 13888-1: 2009-07-15 (3rd ed)
verification key	set of public data elements which is mathematically related to an entity's signature key and which is used by the verifier in the verification process NOTE Sometimes called a public verification key in other standards, e.g. ISO/IEC 9796-2, ISO/IEC 9796-3 and ISO/IEC 9798-7. [ISO/IEC 14888-1] ■	N8760: 1st WD 20008-1: 2010-06-14
verification key	set of public data elements which is mathematically related to an entity's signature key and which is used by the verifier in the verification process NOTE Sometimes called a public verification key in other standards, e.g. ISO/IEC 9796-2, ISO/IEC 9796-3 and ISO/IEC 9798-3. [ISO/IEC 14888-1] ■	N8763: 1st WD 20009-2: 2010-06-20
verification key	set of public data elements which is mathematically related to an entity's signature key and which is used by the verifier in the verification process [ISO/IEC 14888-1] ■	N8751: FCD 29150: 2010-06-10
verification key	set of public data elements which is mathematically related to an entity's signature key and which is used by the verifier in the verification process NOTE Sometimes called a public verification key in other standards, e.g. ISO/IEC 9796-2, ISO/IEC 9796-3 and ISO/IEC 9798-3. ■	ISO/IEC 14888-1: 2008-04-15 (2nd ed.)

Term	Definition	ISO/IEC JTC 1/SC 27 Document
verification process	process which takes as input the signed message, the verification key and the domain parameters, and which gives as output the result of the signature verification: valid or invalid [ISO/IEC 14888-1] ■	N8760: 1st WD 20008-1: 2010-06-14
verification process	process which takes as input the signed message, the verification key and the domain parameters, and which gives as output the result of the signature verification: valid or invalid ■	N8763: 1st WD 20009-2: 2010-06-20
verification process	process which takes as input the signed message, the verification key and the domain parameters, and which gives as output the result of the signature verification: valid or invalid [ISO/IEC 14888-1] ■	N8751: FCD 29150: 2010-06-10
verification process	process which takes as input the signed message, the verification key and the domain parameters, and which gives as output the result of the signature verification: valid or invalid ■	ISO/IEC 14888-1: 2008-04-15 (2nd ed.)
verifier	entity that verifies evidence ■	ISO/IEC 13888-1: 2009-07-15 (3rd ed)
verifier	entity including the functions necessary for engaging in authentication exchanges on behalf of an entity requiring an entity authentication ■	ISO/IEC 9798-5: 2009-12-15 (3rd ed.)
verifier	entity which is or represents the entity requiring an authenticated identity NOTE A verifier includes the functions necessary for engaging in authentication exchanges. ■	ISO/IEC 9798-1: 2010-07-01 (3rd ed.)
verifier	entity which is or represents the entity requiring an authenticated identity [ISO/IEC 9798-1] ■	N8762: 1st WD 20009-1: 2010-07-13
verifier	entity including the functions necessary for engaging in authentication exchanges on behalf of an entity requiring an entity authentication or for engaging in verifying a signature of a given message and signer ■	N8759: 2nd WD 29192-4: 2010-06-15
verifier	entity (3.1.1) that operates the functions necessary to complete authentication (3.3.2) NOTE A verifier may be the same as or act on behalf of the entity that controls identification of entities for a particular domain. ■	N8804: 3rd CD 24760-1: 2010-06-11
verifier	entity including the functions necessary for engaging in authentication exchanges on behalf of an entity requiring an entity authentication Interactions between claimants and verifiers are described in ISO/IEC 9798. ■	N8812: 3rd WD 29146: 2010-07-14
verify	verification process that takes a message, a signature and an identity of a signer to output accept meaning the given signature is generated by the signer with the corresponding signing key, or reject otherwise. ■	N8759: 2nd WD 29192-4: 2010-06-15

Term	Definition	ISO/IEC JTC 1/SC 27 Document
verify	rigorously review in detail with an independent determination of sufficiency NOTE Also see "confirm" (3.1.14). The term "verify" has more rigorous connotations. It is used in the context of evaluator actions where an independent effort is required of the evaluator. ■	ISO/IEC 15408-1: 2009-12-15 (3rd ed.)
verify	process of establishing the veracity of an assertion to a specified or understood level of assurance. ■	N8810: 1st CD 29115 | X.eaa: 2010-06-10
Violation of security policy	To be defined ■	N8732: 3rd WD 29193: 2010-08-06
virtual asset	representation of an asset in the Cyberspace NOTE In this context, currency can be defined as either a medium of exchange or a property that has value in a specific environment, such as a video game or a financial trading simulation exercise. ■	N8624: 2nd CD 27032: 2010-06-15
virtual circuit	data path between network devices established using a packet or cell switching technology such as X.25, ATM or Frame Relay ■	ISO/IEC 18028-5: 2006-07-01 (1st ed.)
virtual currency	monetary virtual assets ■	N8624: 2nd CD 27032: 2010-06-15
virtual local area network	independent network created from a logical point of view within a physical network ■	ISO/IEC 27033-1: 2009-12-15 (1st ed.)
Virtual Private Network - VPN	a private network utilising shared networks. E.g., A network based on a cryptographic tunnelling protocol operating over another network infrastructure. ■	ISO/IEC 18028-4: 2005-04-01 (1st ed.)
virtual world	simulated environment accessed by multiple users through an online interface NOTE 1 These simulated environments are often interactive. NOTE 2 The physical world in which people live, and the related characteristics, will be referred to as the "real world" to differentiate it from a virtual world. ■	N8624: 2nd CD 27032: 2010-06-15
vital record	electronic or paper record that is essential for preserving, continuing or reconstructing the operations of an organization and protecting the rights of an organization, its employees, its customers and its stakeholders ■	N8622: PreFDIS 27031: 2010-08-18
volatile data	data that is especially prone to change and can be easily modified EXAMPLE A change can be switching off the power or passing through a magnetic field. Volatile data also includes data that changes as the system state changes. Examples include data stored in RAM and dynamic IP addresses ■	N8640: 3rd WD 27037: 2010-05-31
vulnerability	weakness of an asset (2.3) or control (2.13) that can be exploited by a risk source (2.57) ■	N8718: 1st WD 27000: 2010-05-27

Term	Definition	ISO/IEC JTC 1/SC 27 Document
vulnerability	includes a weakness of an asset or group of assets which can be exploited by a threat [ISO/IEC TR 13335-1:1996] ■	ISO/IEC 21827: 2008-10-15 (2nd ed.)
vulnerability	weakness in the TOE that can be used to violate the SFRs in some environment ■	ISO/IEC 15408-1: 2009-12-15 (3rd ed.)
vulnerability	weakness of software, hardware, or online service that can be exploited by a threat NOTE 1 Adapted from ISO/IEC 27000:2009 NOTE 2 Examples of weaknesses in a system are software and hardware design flaws, poor administrative processes, lack of awareness and education, and advancements in the state of the art or improvements to current practices. Regardless of cause, an exploitation of such vulnerabilities may result in real threats to mission-critical information systems. NOTE 3 Vulnerabilities can be architecture flaws, coding errors, or other implementation errors, or insecure configuration. Vulnerabilities can also result from insufficient or incorrect security documentation, security awareness, or communication. ■	N8780: 1st CD 29147: 2010-06-10
vulnerability	weakness in the TOE that can be used to violate the SFRs in some environment ■	N8784: 1st WD 20004: 2010-08-06
vulnerability	weakness of an asset or control that can be exploited by a threat [ISO/IEC 27000:2009] ■	N8624: 2nd CD 27032: 2010-06-15
warranty	security service to correct or mitigate the deliverable's operation (deployment, performance, or delivery) if it does not satisfy its security policy. ■	ISO/IEC TR 15443-1: 2005-02-01 (1st ed.)
weak secret	secret that can be conveniently memorized by a human being; typically this means that the entropy of the secret is limited, so that an exhaustive search for the secret may be feasible, given knowledge that would enable a correct guess for the secret to be distinguished from an incorrect guess ■	ISO/IEC 11770-4: 2006-05-01 (1st ed.)
weakness	characteristic or property of software that, in proper conditions, could contribute to the introduction of vulnerabilities within that software ■	N8784: 1st WD 20004: 2010-08-06
WiFi Protected Access - WPA	specification for a security enhancement to provide confidentiality and integrity for wireless communications; it includes the temporal key implementation protocol (TKIP). WPA is the successor of WEP. ■	ISO/IEC 18028-4: 2005-04-01 (1st ed.)
Wired Equivalent Privacy - WEP	cryptographic protocol offering stream cipher encryption with a key length of 128 bits; it is defined within the IEEE 802.11 Wireless LAN specifications. ■	ISO/IEC 18028-4: 2005-04-01 (1st ed.)
Wireless Fidelity - WiFi	trademark provided by the WiFi Alliance promoting the use of wireless LAN equipment. ■	ISO/IEC 18028-4: 2005-04-01 (1st ed.)

Term	Definition	ISO/IEC JTC 1/SC 27 Document
Wireless LAN - WLAN	network using radio frequencies. The most common standards in use are IEEE 802.11b and 802.11g with up to 11 Mbps respectively 54 Mbps transfer rate utilising the 2,4 GHz frequency band. ■	ISO/IEC 18028-4: 2005-04-01 (1st ed.)
witness	procedure parameter that provides evidence of the claimant's identity to the verifier ■	ISO/IEC 9798-5: 2009-12-15 (3rd ed.)
witness	procedure parameter that provides evidence of the claimant's identity to the verifier ■	N8759: 2nd WD 29192-4: 2010-06-15
wolf	biometric sample that results in higher than normal similarity scores on a particular biometric system when compared to biometric references of enrolees ■	ISO/IEC 19792: 2009-08-01 (1st ed.)
word	string of 32 bits used in dedicated hash-functions 1, 2, 3 and 4 of Clauses 7, 8, 9 and 10 respectively, or a string of 64 bits used in dedicated hash-functions 5 and 6 of Clauses 11 and 12 respectively ■	ISO/IEC 10118-3: 2004-03-01 (3rd ed.)
word	string of 32 bits used in Dedicated Hash-Functions 1, 2, 3, 4 and 8, or a string of 64 bits used in Dedicated Hash-Functions 5 and 6 of ISO/IEC 10118-3 [ISO/IEC 10118-3] ■	ISO/IEC FDIS 9797-2: 2009-09-18
work product	artifact associated with the execution of a process [ISO/IEC 15504-1] NOTE A work product might be used, produced or changed by a process. ■	ISO/IEC 21827: 2008-10-15 (2nd ed.)
work product	All items (i.e. documents, reports, files, data, etc.) generated in the course of performing any process for developing and supplying the deliverable [SSE-CMM (ISO/IEC 21827)]. a) Result of a system of activities, which use resources to transform inputs into outputs [ISO 9001]. ■	ISO/IEC TR 15443-1: 2005-02-01 (1st ed.)
work profile	processing event that consists of all tasks performed by a user. [Neumann/Strembeck] ■	N8812: 3rd WD 29146: 2010-07-14
work unit	most granular level of evaluation work NOTE Each evaluation methodology action comprises one or more work units, which are grouped within the evaluation methodology action by ISO/IEC 15408 content and presentation of evidence or developer action element. The work units are presented in this International Standard in the same order as ISO/IEC 15408 elements from which they are derived. Work units are identified in the left margin by a symbol such as ALC_TAT.1-2. In this symbol, the string ALC_TAT.1 indicates ISO/IEC 15408 component (i.e. this International Standard sub-activity), and the final digit (2) indicates that this is the second work unit in the ALC_TAT.1 sub-activity. ■	N8912: Corrected 18045: 2010-09-15

Term	Definition	ISO/IEC JTC 1/SC 27 Document
zero-effort impostor attempt	attempt in which an individual submits his/her own biometric characteristics as if he/she were attempting successful verification against his/her own template, but the comparison is made against the template of another user ■	ISO/IEC 19792: 2009-08-01 (1st ed.)
zeroisation	method of destruction of stored data and CSPs to prevent retrieval and reuse ■	N8776: 2nd WD 19790: 2010-07-16
zombie computer drone	computer containing hidden software that enables the machine to be controlled remotely, usually to perform an attack on another computer NOTE Generally, a compromised machine is only one of many in a botnet, and will be used to perform malicious activities under remote direction. ■	N8624: 2nd CD 27032: 2010-06-15

TeleTrusT Germany

TeleTrusT was founded in 1989 as a non-profit association in Germany promoting the trustworthiness of information and communication technology in open systems environments. Today, TeleTrusT counts more than 100 members. TeleTrusT evolved to a well known and highly regarded competence network for applied cryptography and biometrics.

In various TeleTrusT working groups ICT-security experts, users and interested parties meet each other in frequent workshops, round-tables and expert talks. The activities focus on reliable and trustworthy solutions complying with international standards, laws and statutory requirements. TeleTrusT is keen to promote the acceptance of solutions supporting identification, authentification and signature schemes in electronic business and its processes.

TeleTrusT facilitates information and knowledge exchange between vendors, users and authorities. Subsequently, innovative ICT-security solutions can enter the market more quickly and effectively. TeleTrusT aims on standard compliant solutions in an interoperable scheme. Keeping in mind the raising importance of the European security market, TeleTrusT seeks co-operation with European and international organisations and authorities with similar objectives.

Contact:
Dr. Holger Muehlbauer
TeleTrusT
Managing Director
Chausseestrasse 17
10115 Berlin
GERMANY
Tel.: + 49 30 400 54 306
holger.muehlbauer@teletrust.de
www.teletrust.de


TeleTrusT
Pioneers in IT security.