



TeleTrust

Pioneers in IT security.

Sichere Informationstechnik bedeutet sichere Demokratie

13 Unternehmen und Organisationen gründeten 1989 TeleTrust Deutschland. Die Vision: Sichere Informationstechnik. Die Entwicklung hat gezeigt, wie wichtig dieses Anliegen war und ist. Das Internet ist inzwischen fester Bestandteil der vernetzten Informations- und Wissensgesellschaft. Mit der Verbreitung der digitalen Kommunikation und den steigenden Anforderungen an die IT-Sicherheit wuchs auch TeleTrust.

Aus der kleinen Fachgruppe der Anfangszeit wurde ein bundesweiter IT-Sicherheitsverband mit derzeit über 90 Mitgliedsunternehmen und -institutionen. Sein Anliegen ist es, die Vertrauenswürdigkeit von Informations- und Kommunikationstechnik zu stärken.

TeleTrust-Vorstandsvorsitzender Prof. Dr. Norbert Pohlmann (FH Gelsenkirchen) betont: „Gäbe es TeleTrust nicht, müsste der

Verband heute gegründet werden. Wichtig für die Zukunft ist: Wir benötigen einen Quantensprung in der IT-Sicherheitstechnologie, in der Vorgehensweise gegen Angreifer und in der Zusammenarbeit mit denjenigen Organisationen, die in der Lage sind, für eine vertrauenswürdige und sichere vernetzte Informations- und Wissensgesellschaft zu sorgen.“

Staat und Wirtschaft sind gemeinsam dafür verantwortlich,

die Vorteile der Informationstechnik abzusichern. Die digitale Abbildung organisatorischer Abläufe beschränkt sich längst nicht mehr auf Wirtschaftsunternehmen: Auch der Staat nutzt zunehmend Möglichkeiten zur Verschlankung seiner Prozesse und für den Kontakt mit den Bürgern. Für Wirtschaft, Behörden und Bürger birgt die digitale Kommunikation auch in Zukunft enormes Rationalisierungspotenzial.

„Vor 20 Jahren hatte IT-Sicherheit den Stellenwert einer ADAC-Prüfung vor Beginn der Reise. Heute entscheidet sie über die Wettbewerbsfähigkeit von Wirtschaftsräumen, und morgen wird sie der Maßstab für das Demokratieverständnis unserer Gesellschaft sein“, kommentiert der stellvertretende TeleTrust-Vorstandsvorsitzende Michael Leistenschneider (DATEV).

Um elektronische Kommunikation in allen Bereichen wirklich geschäftstauglich zu gestalten, müssen Inhalte vertraulich und vertrauenswürdig übermittelt werden und Transaktionen rechtsverbindlich sein. Als Mittler zwischen Technolo-

Anlässlich des 20-jährigen Bestehens von TeleTrust fand im November 2009 in Berlin eine Fachkonferenz unter dem Motto „Information – Technik – Vertrauen“ statt.



gie und Anwendungen entwickelt TeleTrust notwendige Standards, Architekturen und Konzepte.

Die Mitglieder von TeleTrust führen ihre verschiedenen Kompetenzen im Streben nach gemeinsamen Zielen zusammen: Während Wissenschaftler das „Machbare“ ausloten, setzen Informatiker und Ingenieure es technisch um – Juristen stecken den rechtlichen Rahmen ab und Unternehmer entwickeln passende Geschäftsmodelle. Dr. Holger Mühlbauer, TeleTrust-Geschäftsführer, fasst zusammen: „Unser interdisziplinärer Ansatz ist unsere Stärke. Die Vielfalt der Mitgliedschaft sichert dem Verband politische und wirtschaftliche Unabhängigkeit.“

TeleTrust kooperiert mit nationalen und internationalen Organisationen, um zu technischer Harmonisierung beizutragen. Resultat dieser Zusammenarbeit ist zum Beispiel die European Bridge CA, die weltweit eine „Brücke des Vertrauens“ zwischen verschiedenen Public-Key-Infrastrukturen (PKIs) schlägt, um sie auf sichere, aber einfache Weise zu verbinden. Technisch gelingt dies durch die Einigung auf einen gemeinsamen Nenner, der sichere Kommunikation über organisatorische Grenzen hinweg ermöglicht. TeleTrust bietet den Rahmen für die Weiterentwicklung vertrauenswürdiger Kommunikation, um künftige Herausforderungen zu meistern.

Fazit: Die Sicherheit der Informationstechnik ist Grundlage der nationalen Sicherheitspolitik, denn innere Sicherheit bedeutet auch Sicherheit der IT – und IT-Sicherheit bedeutet innere Sicherheit. Für die Sicherheitsinfrastruktur in Deutschland sind Staat und Wirtschaft gemeinsam verantwortlich; diese Aufgabe können sie nur in Kooperation mit engagierten Unternehmen, IT-Herstellern und IT-Nutzern erfüllen. In Deutschland bietet TeleTrust die Plattform für eine gemeinsame Sicherheitsinfrastrukturdiskussion in Wirtschaft und Politik. ■



auf der

CeBIT

Hannover

02.–06. März 2010



Anzeige

Zur Gewährleistung sicherer Informationen fokussiert sich Nexus auf die Themen Zugriff, Identifikation und Authentifizierung basierend auf offenen Technologien und Standards wie zum Beispiel PKI und SAML. Für eine sichere elektronische Kommunikation unterstützen wir Organisationen bei der Umsetzung einer kosteneffizienten und sicheren Kommunikationsplattform.

Nexus bietet die komplette Lösung für digitale IDs, Ausweise und elektronische Signaturen basierend auf PKI und digitalen Zertifikaten (u.a. gemäß deutschem Signaturgesetz).

Das 1984 gegründete Unternehmen Nexus ist ein unabhängiger Hersteller von IT-Security-Standardprodukten. Zu den Kunden gehören große Unternehmen und namhafte Behörden weltweit.



Nexus Technology GmbH
Kantstrasse 13 · D-10623 Berlin
phone: +49 (0)30 20614150
www.nexus-safe.com

TeleTrust warnt vor den Konsequenzen aus EU-Expertenbericht zu elektronischer Rechnungslegung

TeleTrust begrüßt grundsätzlich den Report der EU-Expertengruppe zur elektronischen Rechnungslegung (E-Invoicing). Der Verband steht bereit, sich an der europaweiten Diskussion der Ergebnisse zu beteiligen. Die Expertengruppe hatte einen „Minimalkonsens“ auf Basis des European Electronic Invoicing Frameworks (EEIF) empfohlen, der „interne Kontrollen“ nach zukünftiger Definition der einzelnen Mitgliedsstaaten vorsieht.

Der deutsche Sicherheitsverband warnt jedoch vor den Konsequenzen einer Umsetzung der Empfehlungen aus dem aktuellen Report: Das verständliche Bestreben nach europaweiter Einigung auf Basis eines „kleinsten gemeinsamen Nenners“ würde zwangsläufig die Sicherheit und Rechtsverbindlichkeit der elektronischen Rechnungslegung unterlaufen. TeleTrust plädiert deshalb dafür, das deutsche Modell der qualifizierten elektronischen Signatur zur Basis der weiteren Überlegungen zu machen.

Die Empfehlungen der Expertengruppe könnten schnell zu einzelstaatlichen Teillösungen führen, die entgegen der Idee des europäischen Wirtschaftsraums laufen. Dies bedeutet ein wesentlich höheres Investitionsrisiko und zusätzlichen Aufwand für alle international tätigen Unternehmen. Insbesondere kleine und mittelständische Unternehmen (KMU) werden durch den Ersatz der elektronischen Signatur durch „interne Kontrollen“ genötigt, sich auf zahllose unterschiedliche Anforderungen und

Verfahren einzustellen. Dies benachteiligt besonders kleinere Unternehmen, da der Aufwand in der Regel für diese Unternehmen nicht wirtschaftlich darstellbar ist. Insgesamt stark betroffen von dieser eventuellen Neuregelung sind alle KMU als Rechnungsempfänger.

In Deutschland, Spanien, Italien und zehn weiteren Mitgliedsstaaten der Europäischen Union bewährt sich das Modell der qualifizierten elektronischen Signatur als Basis der elektronischen Rechnungslegung bereits seit Jahren und wird täglich in Millionen von Vorgängen eingesetzt. Diese Lösung stellt zudem sicher, dass sämtliche Anforderungen der zuständigen Behörden auch in allen anderen EU-Staaten grenzen- und branchenübergreifend gewährleistet sind sowie Authentizität und Integrität einer elektronischen Rechnung europaweit gewahrt werden.

Die EU-Rechnungsrichtlinie von 2006 ist in den vergangenen Jahren in immer mehr EU-Staaten erfolgreich umgesetzt worden. Eine Vielzahl von Unternehmen aller Größen und Branchen praktiziert seit Jahren grenzüberschreitend sicheres E-Invoicing mit elektronischen Signaturen. Hierfür sind zahlreiche Signaturverfahren von unterschiedlichen Herstellern und Dienstleistern am Markt verfügbar und praktisch erprobt. Mehrere TeleTrust-Mitglieder wie AuthentiDate mit dem eBilling Signature Server oder secunet mit multisign haben entsprechende Lösungen im Portfolio. ■

Einsturzgefahr!

Passgenaue IT-Sicherheit macht Ihren Erfolg stabil.

Schützen Sie Ihre wichtigsten Werte. IT-Sicherheit ist der Wegbereiter für eine intakte IT-Infrastruktur und alle Prozesse. Setzen Sie mit secunet auf die richtige Karte: Wir unterstützen Sie mit Expertise und Weitblick bei der Realisierung anspruchsvoller IT-Sicherheitslösungen.

secunet

www.secunet.com

IT-Sicherheitspartner der
Bundesrepublik Deutschland



Anwendungsbereiche elektronischer Signaturen

Elektronische Signaturen wurden in Deutschland erstmals 1997 mit dem Signaturgesetz geregelt. Im Jahre 2001 erfolgte eine Überarbeitung der gesetzlichen Regelungen aufgrund der EG-Richtlinie über elektronische Signaturen. Seither unterscheidet man in Deutschland drei Grundformen elektronischer Signaturen: Die einfachste Form einer elektronischen Signatur ist die Namensunterschrift, beispielsweise in einer E-Mail die in den meisten E-Mail-Programmen auch so bezeichnete „Signatur“. Fortgeschrittene Signaturen entsprechen dem, was beispielsweise das Programm pgp (Pretty Good Privacy) bietet. Ausführlich im Gesetz geregelt ist die qualifizierte elektronische Signatur, welche die höchste Sicherheit im Hinblick auf Authentizität und Integrität gewährleistet. Eine Variante davon ist gegeben, wenn der Zertifizierungsdiensteanbieter von der Bundesnetzagentur akkreditiert ist und damit nachgewiesen hat, dass er die Vorgaben des Signaturgesetzes (SigG) erfüllt.

Mittlerweile gibt es mehrere Anbieter qualifizierter elektronischer Signaturen in Deutschland. Trotz dieser vorhandenen Infrastruktur und der langen Geschichte des Signaturgesetzes in Deutschland bleibt die praktische Anwendung von qualifizierten elektronischen Signaturen noch immer hinter den Erwartungen zurück.

Wichtige Impulse zur Verbreitung wurden durch die Verpflichtung der Notare zur elektronischen Einreichung von Anträgen bei den Registergerichten und der Rechtsanwälte zur elektronischen Einreichung von Mahnbescheiden gegeben. Weitere Impulse zur Anwendung qualifizierter elektronischer Signaturen können sich aus

den E-Card-Projekten des Bundes ergeben (etwa elektronischem Personalausweis, ELENA und Gesundheitskarte), die mit Funktionen zur qualifizierten elektronischen Signatur ausgestattet sind.

Kontraproduktiv dürfte die Initiative des Bundesinnenministeriums zu DE-Mail und Bürgerportalen wirken: Mit DE-Mail wird letztlich ein anderer Weg gesucht, Authentizität und Integrität elektronischer Nachrichten, insbesondere im Internet, sicherzustellen. Die fehlende Bereitschaft in Bevölkerung und Wirtschaft, Aufwand und Kosten für elektronische Signaturen auf sich zu nehmen, wird sicher nicht dadurch gesteigert, dass zum gleichen Zweck nun ein anderes Mittel zur Verfügung gestellt werden soll.

Eine mögliche Schlüsselanwendung für die qualifizierte elektronische Signatur kann die elektronische Rechnung sein: Verschiedene Untersuchungen haben gezeigt, dass die Umstellung von der gewohnten Papier-Rechnung auf elektronische Rechnungen für die Unternehmen erhebliches Einsparpotenzial mit sich bringen kann. Neben den Kosten für Papier, Druck und Porto ist insbesondere der Verwaltungsaufwand bei Absender und Empfänger erheblich.

Tatsächlich ist zu beobachten, dass immer mehr Unternehmen auf elektronische Abrechnungen setzen. Für den Empfänger ist die Möglichkeit zum Vorsteuerabzug aus elektronischen Rechnungen jedoch nur gegeben, wenn diese mit qualifizierten elektronischen Signaturen versehen sind. Elektronische Dokumente sind von sich aus leicht zu kopieren, zu verändern und zu verfälschen – qualifizierte elektronische Signaturen sind geeignet, Authenti-



TURAYA™

TrustedObjects Manager
Trusted Security Management

TrustedVPN
Trusted Communication Channels

TrustedServer
Trusted Services Provisioning

TrustedDesktop
Trusted Work Environments

- **TURAYA™ Security Kernel**, providing Trusted Computing support with
 - Trusted Boot
 - Hardware Security-Anchor
 - Remote Attestation
 - Sealed Storage

- **Foolproof Configuration and Operation Management**
 - Trusted Virtual Domains
 - Enterprise-Wide Policy Enforcement

Sirrix AG
security technologies

info@sirrix.com

www.sirrix.com

zität und Integrität von Rechnungen sicherzustellen und damit den Missbrauch von Rechnungen und dem Vorsteuerbetrug entgegenzuwirken.

Im aktuellen Report der EU-Expertengruppe zur elektronischen Rechnungslegung (E-Invoicing) werden Empfehlungen ausgesprochen, wie die Akzeptanz der elektronischen Rechnung in Europa weiter verbessert werden kann: Positiv daran ist die Zielsetzung, in Europa einheitliche Vorgaben für elektronische

Rechnungen zu gewährleisten. Auch der Versuch, die elektronische Rechnung nicht komplizierter und aufwändiger zu machen als die Rechnung auf Papier, ist zu begrüßen. Jedoch ist davor zu warnen, die qualifizierte elektronische Signatur als Sicherheitsmerkmal elektronischer Rechnungen aufzugeben und stattdessen alleine „interne Kontrollen“ nach zukünftiger Definition der einzelnen Mitgliedsstaaten vorzuschreiben. In Deutschland, Spanien, Italien und zehn weiteren

EU-Mitgliedsstaaten bewährt sich das Modell der qualifizierten elektronischen Signatur als Basis der elektronischen Rechnungslegung bereits seit Jahren, wird täglich in Millionen von Vorgängen eingesetzt und sollte nicht durch ein unsicheres System ersetzt werden. ■

Rechtsanwalt Dr. Thomas Lapp ist Regionalbeauftragter Frankfurt/Main im DAV-IT und Leiter der TeleTrust-AG „Rechtliche Aspekte“

TELETRUST Deutschland e. V.

www.teletrust.de

Der IT-Sicherheitsverband TELETRUST Deutschland wurde im Jahr 1989 gegründet, um verlässliche Rahmenbedingungen für den vertrauenswürdigen Einsatz von Informations- und Kommunikationstechnik zu schaffen. Er entwickelte sich zu einem Kompetenznetzwerk mit derzeit rund 100 Mitgliedern aus Industrie, Wissenschaft und Forschung sowie öffentlichen Institutionen. TELETRUST betreibt Arbeitsgruppen zu aktuellen Themen, beteiligt sich an öffentlichen Projekten (z.B. dem „Netzwerk Elektronischer Geschäftsverkehr“), äußert sich zu politischen und rechtlichen Fragen, organisiert Messen und Messebeteiligungen (insbesondere „ISSE“ und „RSA“) und ist Träger der „European Bridge CA“ (Bereitstellung von Public-Key-Zertifikaten für sichere E-Mailkommunikation) sowie des Zertifikates „TELETRUST Information Security Professional“ (T.I.S.P.). Hauptsitz des Verbandes ist Berlin.

Vorstand:

Prof. Dr. Norbert Pohlmann
(Vorsitzender)

Michael Leistenschneider
(Stellvertretender Vorsitzender)

Dr. Rainer Baumgart

Ammar Alkassar

Geschäftsführer:

Dr. Holger Mühlbauer
holger.muehlbauer@teletrust.de
Tel.: + 49 30 / 40 05 43 06

Bundesgeschäftsstelle Berlin:

TELETRUST Deutschland e.V.
Chausseestraße 17
10115 Berlin
Tel.: + 49 30 / 40 05 43 10
info@teletrust.de
www.teletrust.de

Ekkehard Diedrich (Referent)
ekkehard.diedrich@teletrust.de
Tel.: + 49 30 / 40 05 43 10

Marion Gutsell (Assistenz)
marion.gutsell@teletrust.de
Tel.: + 49 30 / 40 05 43 10

Pressekontakt:

Sebastian Thümmel
index Agentur für strategische
Öffentlichkeitsarbeit und Werbung GmbH
Zinnowitzer Str. 1, 10115 Berlin
Tel.: +49 30 / 390 88-190
s.thuettel@index.de
www.index.de

Regionalgeschäftsstelle Nord-West:

c/o OTARIS GmbH
Frank Bittner
Fahrenheitstraße 1
28359 Bremen
frank.bittner@teletrust.de
Tel.: +49 421 / 22 08 120

TELETRUST-Projekte, Leiter und Koordinatoren

TELETRUST-Projekt „European Bridge CA“

Prof. Bernhard Esslinger, Deutsche Bank
Dr. Guido von der Heide, SIEMENS

Die European Bridge-CA (EB-CA) ermöglicht eine sichere und authentische Kommunikation zwischen Unternehmen und öffentlicher Verwaltung. Dabei werden die Public-Key-Infrastrukturen der einzelnen Organisationen miteinander verknüpft.

TELETRUST-Projekt „T.I.S.P.“

(TELETRUST Information Security Professional)

Christoph Weinmann, securvo GmbH

Das TISP-Zertifikat ist das erste Expertenzertifikat im Bereich der Informationssicherheit, das speziell auf den europäischen Raum abgestimmt ist und die dort verbreiteten Standards und Gesetzgebungen berücksichtigt.

Projekt „Netzwerk Elektronischer Geschäftsverkehr (NEG)“

Ekkehard Diedrich, TELETRUST

Hans-Joachim Bierschenk, Bierschenk Consulting
Harald Kesberg, Kesberg Consulting

Noch immer ist das Know-how bei kleinen und mittelständischen Unternehmen in puncto Informationssicherheit eher unterdurchschnittlich ausgeprägt. Konkrete Hilfestellung will in diesem Zusammenhang eine Veranstaltungsreihe im Rahmen des Begleitprojektes zu NEG unter Beteiligung von TELETRUST bieten. Unter dem Motto „Unternehmer lernen von Unternehmern“ wird eine Reihe regionaler „Stammtische“ bundesweit organisiert.

TELETRUST-Arbeitsgruppen, Leiter und Koordinatoren

TELETRUST-AG „Juristische Aspekte“

RA Dr. Thomas Lapp, DAV-IT

TELETRUST-AG „Gesundheitstelematik“

Dr. Christoph Goetz, KVB

TELETRUST-AG „SICCT“

Jürgen Atrott, TÜV-IT

TELETRUST-AG „Öffentlichkeitsarbeit“

Dr. Kai Rathke, secunet

TELETRUST-AG „Sichere elektronische Geschäftsprozesse“

Stephan Wappler, IBM

TELETRUST-AG „PKI“

Andrea Klenk, mtG AG

TELETRUST-AG „Elektronische Identitäten“

Prof. Dr. Helmut Reimer

TELETRUST-AG „SOA Security“

Dr. Bruno Quint, Corisecio GmbH

TELETRUST-AG „Trusted Computing“

Christian Stübke, Sirrix AG

TELETRUST-AG „Biometrie“

Prof. Christoph Busch, Fraunhofer IGD

Regionalvertretung Nordwest TeleTrust Deutschland e.V.

OTARIS
Interactive Services

EINFACH SICHER!



OTARIS entwickelt kundenspezifische client- und webbasierte Softwarelösungen, die sich durch einfache Bedienbarkeit, optimal abgestimmte Sicherheitskonzepte und Zuverlässigkeit auszeichnen.

- IT-Security
- Business Intelligence
- Software development
- Mobile Business

OTARIS Interactive Services GmbH
Fahrenheitstraße 1
28359 Bremen
Tel: +49 421 2208 120
www.OTARIS.de

Besuchen Sie uns auf der CeBIT Halle 6, D42

Anzeige

Mitglieder bei TELETRUST Deutschland e.V.

Stand: März 2010

@bc – Arendt Business Consult
 ABDA
 accessec GmbH
 Applied Security GmbH
 Atos Origin GmbH
 atsec information security GmbH
 AUCONET GmbH
 AuthentiDate International AG
 BCC Unternehmensberatung
 Bierschenk Consulting
 BioID GmbH
 bos – bremen online services GmbH & Co. KG
 Brainloop AG
 Bromba GmbH
 Bundesamt für Sicherheit in der Informationstechnik (BSI)
 Bundeskriminalamt Wiesbaden
 CCV Deutschland GmbH
 certgate GmbH
 Cognitec Systems GmbH
 Computas Gisela Geuhs GmbH
 Computer Communication Networks GmbH
 Corisecio GmbH
 CROSS MATCH Technologies GmbH
 DATEV eG
 DE-CODA GmbH
 DERMALOG Information Systems GmbH
 Deutsche Bank AG
 Deutscher Genossenschaft-Verlag eG
 Deutscher Sparkassenverlag GmbH
 DFN – Verein zur Förderung eines Deutschen
 Forschungsnetzes e.V.
 Dr. Fehr GmbH
 FH Gelsenkirchen, Institut für Internet-Sicherheit if (is)
 Fraunhofer Institut für Biomedizinische Technik - BMT
 Fraunhofer Institut für Graphische Datenverarbeitung - IGD
 Fraunhofer Institut für Sichere Informationstechnologie - SIT
 GAD – Gesellschaft für automatische Datenverarbeitung eG
 Gemalto GmbH
 Glück & Kanja Consulting AG
 HID Global GmbH
 HYPERCOM GmbH
 INFORA GmbH
 International School of IT-Security – isits AG
 ITSG – Informationsstechnische Servicestelle der
 Gesetzlichen Krankenkassen GmbH
 Kassenärztliche Bundesvereinigung
 Kassenärztliche Vereinigung Bayerns
 Kassenzahnärztliche Bundesvereinigung
 Kesberg Consulting
 KOBIL Systems GmbH
 Mentana-Claimsoft AG
 media transfer AG (mtG)
 Microsoft Germany GmbH
 NEC Deutschland GmbH

NetSys.IT GbR
 Nexus Technology GmbH
 Nimbus Technologieberatung GmbH
 NXP Semiconductors Germany GmbH
 Onlinehelp24
 OTARIS GmbH
 PAV Card. GmbH
 PGP Deutschland AG
 Psylock GmbH
 QGroup GmbH
 qSkills GmbH & Co. KG
 Rohde & Schwarz SIT GmbH
 SAP AG & Co. KG
 SCM Microsystems GmbH
 Secardeo GmbH
 Secaron AG
 securvo Security Consulting GmbH
 secrypt GmbH
 secunet Security Networks AG
 Secusmart GmbH
 Siemens AG
 SignCard GmbH & Co. KG
 Sirrix AG
 SOFTPRO GmbH
 TC TrustCenter AG
 Teleca Systems GmbH
 Totemo AG
 TÜV Informationstechnik GmbH
 VOICE.TRUST AG
 ZF Electronics GmbH

Einzelmitglieder:

Stephan Wappler, Axel Leitner, Heiko Kirsch

Ehrenmitglieder:

Dietrich Kruse, Dr. Karl Rihaczek, Prof. Dr. Helmut Reimer

Assoziierte Mitglieder:

AWW – Arbeitsgemeinschaft für wirtschaftliche
 Verwaltung e.V.
 CAST e.V.
 DAV IT – Arbeitsgemeinschaft Informationstechnologie
 im Deutschen Anwaltverein (DAV) e.V.
 eco
 GDD e.V.
 LSEC – LEADERS IN SECURITY
 NIFIS – Nationale Initiative für Informations- und
 Internet-Sicherheit e.V.
 SIBB
 SILICON TRUST
 VSWM – Verband für Sicherheit in der Wirtschaft
 in Mitteldeutschland
 VOI – Verband Organisations- und
 Informationssysteme e.V.

Identitätsmanagement mit Governikus®

Das elektronische Identitätsmanagement mit dem neuen Personalausweis realisiert die bos KG als Komponente der bewährten Sicherheitsmiddleware

Bereits frühzeitig begann das auf E-Government und E-Business spezialisierte IT-Unternehmen aus Bremen eine Lösung sowohl server- als auch clientseitig für einen gesicherten Identitäts- und Altersnachweis mit dem neuen Personalausweis zu konzipieren. Die Identitätsmanagementlösung der bos KG basiert auf dem eCard-API-Framework und wird modularer Bestandteil von Governikus® sein.

Das Identitätsmanagement mit Governikus bietet sämtliche Funktionen, die zum Identitäts- und Altersnachweis mit dem neuen Personalausweis benötigt werden. Die Governikus-Komponente eID-Server sorgt für sichere Identitäts- und Altersnachweise mit dem neuen Personalausweis, verwaltet die Berechtigungszertifikate sowie die zugehörigen kryptografischen Schlüssel und verarbeitet Sperrlisten. Die Komponente eID-Client zeigt im Gegenzug das sog. Berechtigungszertifikat der Organisation an, die den Personalausweis auslesen möchte und ermöglicht dem Personalausweisinhaber das An- oder Abwählen der aus dem neuen Personalausweis angeforderten Datenfelder – vor allem aber sichert sie die Kommunikation zwischen dem neuen Personalausweis und dem eID-Server über das eCard-API-Framework.

bremen online services GmbH & Co. KG | Am Fallturm 9 | D-28359 Bremen
Telefon: +49 421 204 95-0 | E-Mail: sales@bos-bremen.de



**bremen
online services**

Unabhängig davon wird die gesamte bos-Produktpalette den neuen Personalausweis als qualifizierte Signaturkarte zeitnah unterstützen, sobald dieser von den entsprechenden Stellen dafür freigegeben wurde.

Die bos KG auf der CeBIT 2010

Über nähere Einzelheiten zu Governikus und das Identitätsmanagement informiert die bos KG auch anlässlich der CeBIT 2010 (02.-06.03.2010).

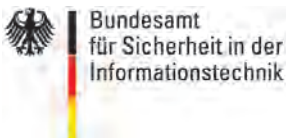
Besuchen Sie uns im Public Sector Parc

in Halle 9, Stand B70/1
und als Kooperationspartner am Stand des BMI (B60).
Wir freuen uns auf Sie!

www.bos-bremen.de



**HANNOVER
2.–6.3.2010
cebit.com**



Bundesamt für Sicherheit in der Informationstechnik (BSI)

Halle 11, Stand B 46

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) wurde am 1. Januar 1991 gegründet und gehört zum Geschäftsbereich des Bundesministeriums des Innern. Das BSI ist eine unabhängige und neutrale Stelle für Fragen zur IT-Sicherheit in der Informationsgesellschaft. Als Behörde ist sie damit im Vergleich zu sonstigen europäischen Einrichtungen einzigartig. Derzeit sind dort mehr als 500 Mitarbeiter mit dem Schwerpunkt Informatik, Physik und Mathematik beschäftigt. Seinen Hauptsitz hat das BSI in Bonn.

Mit der rasanten Fortentwicklung der Informationstechnik entstehen in fast allen Bereichen des Alltags neue IT-

Anwendungen – und damit auch immer neue Sicherheitslücken. Je abhängiger der Mensch von der Informationstechnik wird, desto mehr stellt sich die Frage nach deren Sicherheit. Unsere Gesellschaft ist stärker als zuvor durch Computerversagen, -missbrauch oder -sabotage bedroht. Bisher kann nicht ausreichend sichergestellt werden, dass die Informationstechnik das tut, was sie soll, und nichts tut, was sie nicht soll. Weil die Probleme in der Informationstechnik so vielschichtig sind, ist auch das Aufgabenspektrum des BSI sehr komplex: Das BSI untersucht Sicherheitsrisiken bei der Anwendung der Informationstechnik und entwickelt Sicherheitsvorkehrungen. Es informiert über Risiken und Gefahren beim Einsatz der Informationstechnik und versucht Lösungen dafür zu finden. Dies beinhaltet die Prüfung und Bewertung der IT-Sicherheit von IT-Systemen, einschließlich deren Entwicklung in Kooperation mit der Industrie. Auch bei technisch sicheren Infor-

mations- und Telekommunikationssystemen können Risiken und Schäden durch unzureichende Administration und Anwendung entstehen. Um diese Risiken zu minimieren beziehungsweise zu vermeiden, wendet sich das BSI an eine Vielzahl von Zielgruppen: Es berät Hersteller, Vertreiber und Anwender von Informationstechnik. Darüber hinaus analysiert es Entwicklungen und Trends in der Informationstechnik.

Bundesamt für Sicherheit in der Informationstechnik

Postfach 200363
53133 Bonn
Telefon: 0228 99 9582-0
Telefax: 0228 99 9582-5400
Homepage: <http://www.bsi.bund.de>

Hier abonnieren

Diese Leser profitieren vom Informationsdienst IT-Grundschutz

- IT-Leiter
- Administratoren
- Sicherheitsbeauftragte
- Bezieher der IT-Grundschutzkataloge
- Datenschutzbeauftragte
- IT-Security-Officer zum schnellen Überblick

SecuMedia

Der Verlag für
Sicherheits-Informationen

Postfach 12 34, 55205 Ingelheim
vertrieb@secumedia.de
Tel. +49 6725 9304-0



IT-Grundschutz

Der Informationsdienst „IT-Grundschutz“ ist eine ideale aktuelle Ergänzung zu den IT-Grundschutz-Katalogen. Der monatlich erscheinende Informationsdienst liefert Neues zu Rechtsprechung, Technik, Anwendungen und Trend-Themen - leicht verständlich und praxisnah.

gratis: Probeseiten und News unter: www.grundschutz.info

Jahresabonnement **Informationsdienst IT-Grundschutz:**

Inland 98,00 € / Ausland 116,10 € inkl. MwSt. und Versandkosten

Koppelabopreis für <kes>-Abonnenten: Inland 76,00 € / Ausland 84,53 € / Schweiz: 130,00 SFr (inkl. MwSt. und Versandkosten)



Die IT-Security-Messe

Nürnberg

19.-21. Oktober 2010

*Erleben Sie mit der it-sa in Nürnberg
vom 19.-21. Oktober 2010 eine Messe,
die sich exklusiv auf das Thema
IT-Sicherheit konzentriert*

- Lösungen zu Informations-Sicherheit, Storage- und Netzwerksicherheit, Datenschutz, Hardware-Sicherung, Security-Awareness
- Non-Stop-Vortragsprogramm auf drei großen Foren mit Kurzreferaten, Podiumsdiskussionen und Live-Demos
- Guided Tours von unabhängigen Consultants
- Topic-Routen zu Trendthemen, Basis-Lösungen
- Seminare, Security-Tagungen, Workshops

Jetzt informieren: www.it-sa.de

SecuMedia Verlags-GmbH
Postfach 12 34, 55205 Ingelheim
Telefon +49 6725 9304-0
Fax +49 6725 5994

Manches soll immer ein Rätsel bleiben ...

**Rohde & Schwarz SIT – Ihr Partner für
sichere Sprach- und Datenkommunikation**

- Sicherheits- und Kryptographielösungen
„Made in Germany“
- Höchste zivile und militärische Zulassungen
- Jahrzehntelange Kryptoerfahrung

www.sit.rohde-schwarz.com

Besuchen Sie uns auf der
CeBIT 2010 in Hannover
2. bis 6.3.2010
Halle 11 / Stand D46



ROHDE & SCHWARZ

Sind Sie verantwortlich für die IT-Sicherheit?

<kes> liefert alle relevanten Informationen zum Thema IT-Sicherheit – sorgfältig recherchiert von Fachredakteuren und Autoren aus der Praxis.

In jeder Ausgabe finden Sie wichtiges Know-how, Hinweise zu Risiken und Strategien, Lösungsvorschläge und Anwenderberichte zu den Themen:

Internet/Intranet-Sicherheit

Zutrittskontrolle

Virenbabwehr

Verschlüsselung

Risikomanagement

Abhör- und Manipulationsschutz

Sicherheitsplanung

Elektronische Signatur und PKI

<kes> ist seit 20 Jahren die Fachzeitschrift zum Thema Informations-Sicherheit - eine Garantie für Zuverlässigkeit.

<kes>-online

<kes>-Leser können neben der Print-Ausgabe auch <kes>-online unter www.kes.info nutzen. Hier finden Sie ohne Zugangsbeschränkung, das Thema der Woche, viele interessante Links, Stichwort-Lexikon IT-Security-Begriffe, Verzeichnis relevanter Veranstaltungen und außerdem aktuelle Artikel zum Probelesen.

Abonnenten erhalten zusätzlich ein Passwort mit dem sie Zugriff auf alle aktuellen Artikel und auch auf das Online-Archiv erhalten.

PROBEHEFT-ANFORDERUNG

☐ **ja**, bitte schicken Sie mir gratis und unverbindlich ein Exemplar der <kes> - Die Zeitschrift für Informations-Sicherheit zum Probelesen zu.

Es kommt nur dann ein Abonnement zustande, wenn ich es ausdrücklich wünsche.

Das Abonnement beinhaltet ein Passwort zur Nutzung des Abo-Bereichs auf www.kes.info

Datum

Zeichen

Unterschrift

FAX an +49 6725 5994

Lieferung bitte an

SecuMedia Verlags-GmbH
Abonnenten-Service
Postfach 12 34
55205 Ingelheim

Telefon Durchwahl

Jetzt Probeheft anfordern!

