TeleTrusT/VOI-Informationstag "Elektronische Signatur und Vertrauensdienste"

Berlin, 23.09.2021

Vertrauliche digitale Daten richtig aufbewahren

Stefanie Peter, procilon GmbH

Themengebiete in diesem Vortrag

AGENDA

- Vertrauenswürdigkeit technischer Systeme
- Herausforderungen und Einflussfaktoren
- Technische Richtlinie TR-03125
- Technische Lösungen

Begriffsdefinition

VERTRAUEN

Vertrauen, als die Hypothese künftigen Verhaltens, die sicher genug ist, um praktisches Handeln darauf zu gründen, ist als Hypothese ein mittlerer Zustand zwischen Wissen und Nichtwissen […].

(Georg Simmel, dt. Philosoph und Soziologe, Untersuchungen über die Formen der Vergesellschaftung)

VERTRAUENSWÜRDIGKEIT

Trustworthiness – Definitionen auf der Seite des NIST (National Institute of Standards and Technology)

The attribute of a person or enterprise that provides confidence to others of the qualifications, capabilities, and reliability of that entity to perform specific tasks and fulfill assigned responsibilities.

Computer hardware, software and procedures that— 1) are **reasonably secure from intrusion and misuse**; 2) provide a **reasonable level of availability, reliability, and correct operation**; 3) are **reasonably suited to performing their intended functions**; and 4) adhere to **generally accepted security procedures.**

The degree to which an information system (including the information technology components that are used to build the system) can be expected to **preserve the confidentiality, integrity, and availability** of the information being processed, stored, or transmitted by the system across the full range of threats. **A trustworthy information system is a system that is believed to be capable of operating within defined levels of risk despite the environmental disruptions, human errors, structural failures, and purposeful attacks that are expected to occur in its environment of operation.**

Was ist mit Archivierung gemeint?

ARCHIVIERUNG

Gabler Wirtschaftslexikon

- kontrollierte und systematische langfristige Speicherung von Dokumenten und Daten.

Problemkontext

- Langfristige Speicherung von Dokumenten und Daten in digitaler Form
- Zugreifbarkeit digitaler Daten und Nachweisbarkeit der Unveränderthеit über lange Zeiträume
- Löschung digitaler Daten nach Ablauf der Aufbewahrungsfrist
- Aktualisierung digitaler Daten, wenn erforderlich
- Langfristige Prüfbarkeit elektronischer Sicherheitsmerkmale (Signaturen, Zeitstempel, Hashwerte etc.)

Bedrohungslage

INFORMATIONSSICHERHEIT

Heterogene Bedrohungslage beständig hoch

- Abfluss vertraulicher Informationen
- Datenmanipulationen
- Systemmanipulationen
- Ransomware
- Angriffe auf die Verfügbarkeit von Systemen und Informationen

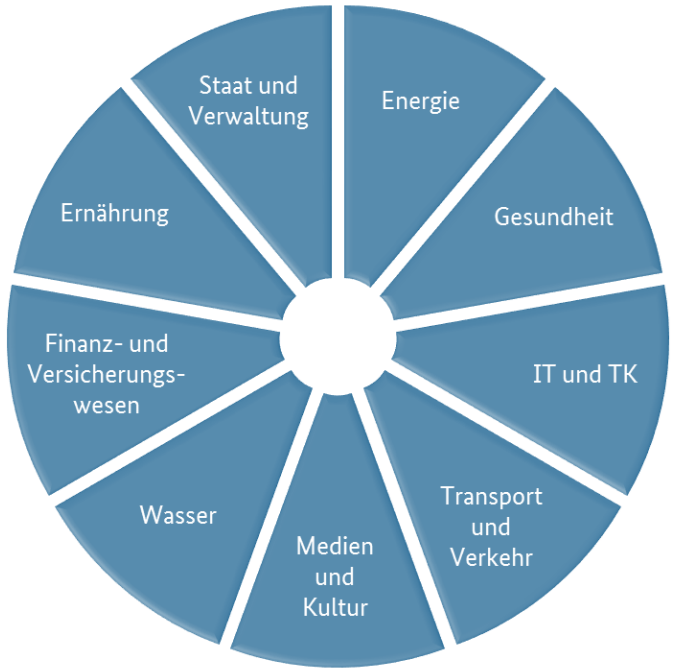
Anforderungen und Einflussfaktoren

SICHERHEITSANFORDERUNGEN

Integrität	Prüfbarkeit der Unveränderthеit übermittelter / gespeicherter Daten
Vertraulichkeit	Zugriff nur für berechtigte Subjekte (Nutzer, technische Systeme)
Verfügbarkeit	Zugriff innerhalb zugesicherter Antwortzeiten
Authentizität	Nachweisbarkeit des Ursprungs übermittelter und gespeicherter Daten

GESETZLICH UND BRANCHENSPEZIFISCH

- Kaufmännisch: §§ 239, 257 HGB, GoBS, GdPDU
- Branchenspezifische Anforderungen, z. B. KRITIS



Quelle: kritis.bund.de

Auditierung: Zugriffsprotokollierung

Schriftformerfordernis: Elektronische Signaturen

Aufbewahrungsfristen: Vorgegebene Mindestzeiträume

Löschung: sicheres Löschen digitaler Daten

Zugriffskontrolle: Beschränkung des Datenzugriffs

ALTERUNG KRYPTOGRAFISCHER VERFAHREN

Beispiel: Elektronische Signaturen

- Zertifikatslaufzeiten und Gültigkeitsmodelle
- Eignung kryptografischer Algorithmen und Schlüssellängen (Rechenleistung und Quantencomputer)
- Verfügbarkeit von Gültigkeits- und Sperrinformationen
- Aufbewahrungszeitraum elektronischer Dokumente ggf. wesentlich länger

Sicherheit kryptografischer Algorithmen bei Verfügbarkeit Quantencomputer

Kryptografischer Algorithmus	Schlüssel-Typ	Verwendung	Auswirkungen
AES	Symmetrischer Schlüssel	Verschlüsselung	Längere Schlüssellänge notwendig
SHA-2, SHA-3	N/A	Hash-Funktionen	Längere Ausgaben erforderlich
RSA	Öffentlicher Schlüssel	Signaturen, Schlüsselaushandlung	Nicht mehr sicher
ECDSA, ECDH (Elliptische Kurven)	Öffentlicher Schlüssel	Signaturen, Schlüsselaushandlung	Nicht mehr sicher
DSA (Finite Felder)	Öffentlicher Schlüssel	Signaturen, Schlüsselaushandlung	Nicht mehr sicher

IT-SYSTEMLANDSCHAFT UND INTEGRATION

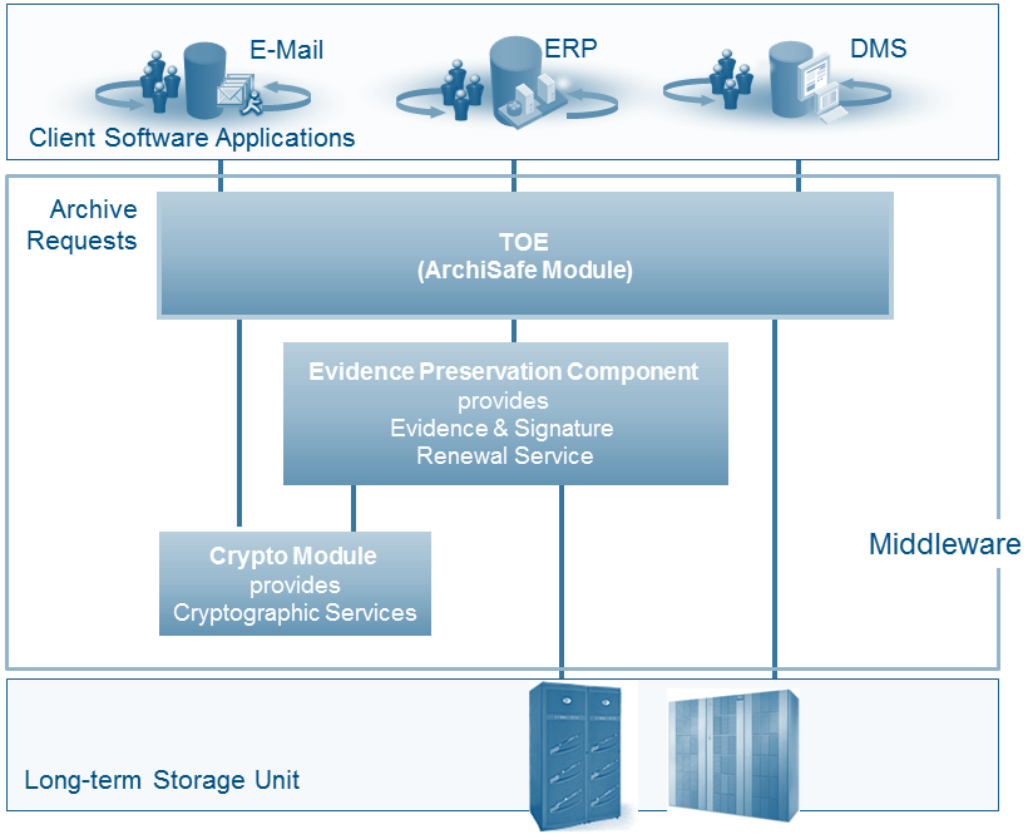
Herausforderungen

- Kryptografie und IT-Sicherheit i. d. R. fern von der ursprünglichen Fachdomäne
- Sicherheits- und Fachanforderungen ergeben im Zusammenspiel komplexe Szenarien
- Komplexität ist ein wesentlicher Kostentreiber in der Lösungsrealisierung

Ziele

- Standardisierung der Verfahren und Schnittstellen
- Schwache Kopplung und hohe Kohäsion der beteiligten Systeme

DIE ARCHISAFE-IDEE



Übersicht

- Schwache Kopplung externer Systeme
- Identifikation zu archivierender Objekte anhand der Garderobenmarke (AOID, Archive Object Identifier)
- Selbstbeschreibende Archivobjekte (AIP, **a**rchival **i**nformation **p**ackage)
- Zugriffskontrolle auf archivierte Objekte

Quelle: Common Criteria Protection Profile für an ArchiSafe Compliant Middleware for Enabling the Long-Term Preservation of Electronic Documents

TECHNISCHE RICHTLINIE TR-03125

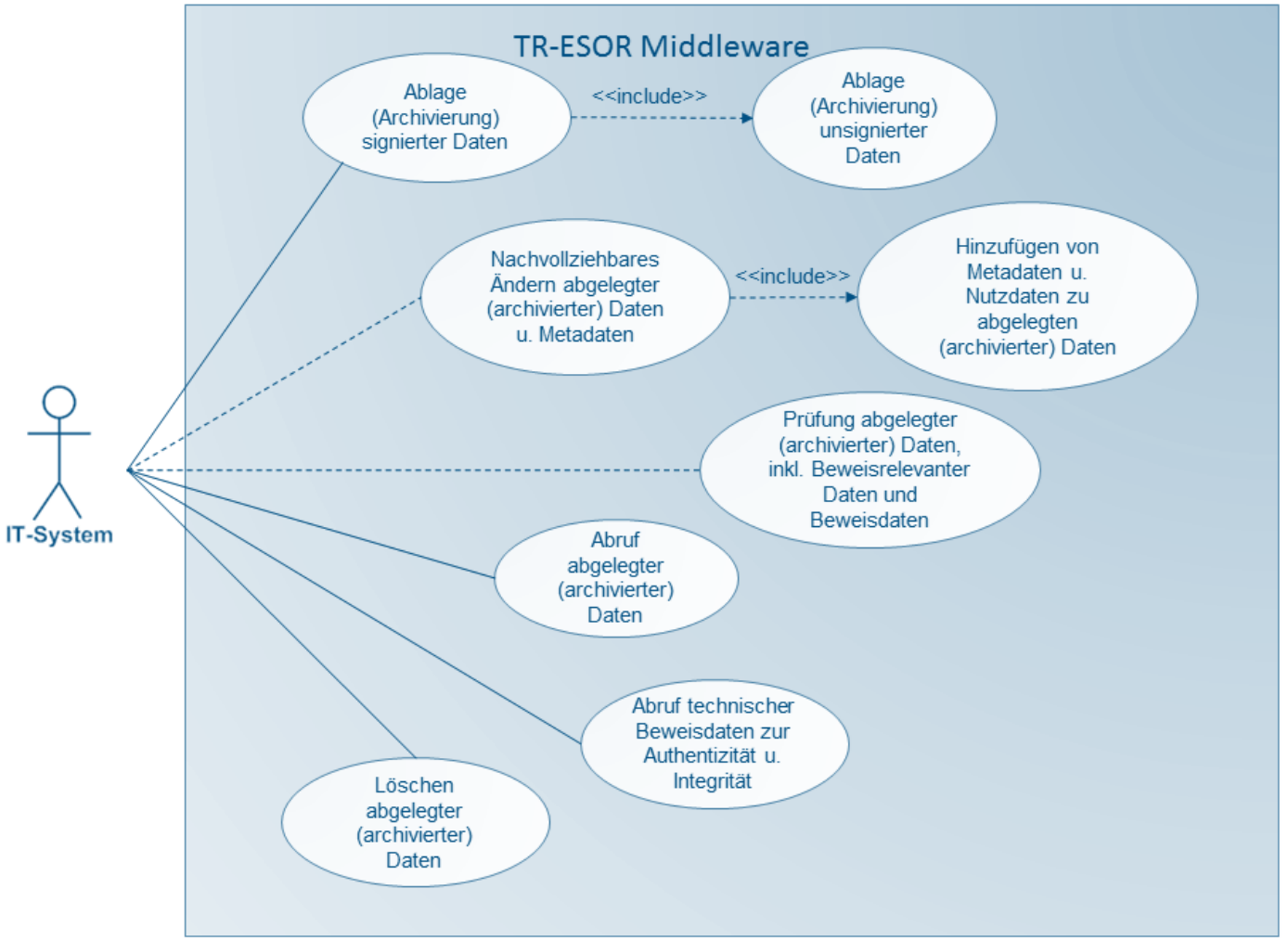
Aspekt	Bedeutet
Modularität	Modulare Systembestandteile für die Konzepte ArchiSafe (Archivobjekte), ArchiSig (Signaturerneuerung), Kryptografie (Kryptografische Basisdienste)
Schnittstellen	Schnittstellenvorgaben für standardisierte Produkte
Verifikationsreport	Prüfung der Archivdatenobjekte
Profilierung	Profile für Bundesbehörden und Industrie
Testspezifikationen	Konformitätstests und Zertifizierung technischer Lösungen

TECHNISCHE RICHTLINIE TR-03125

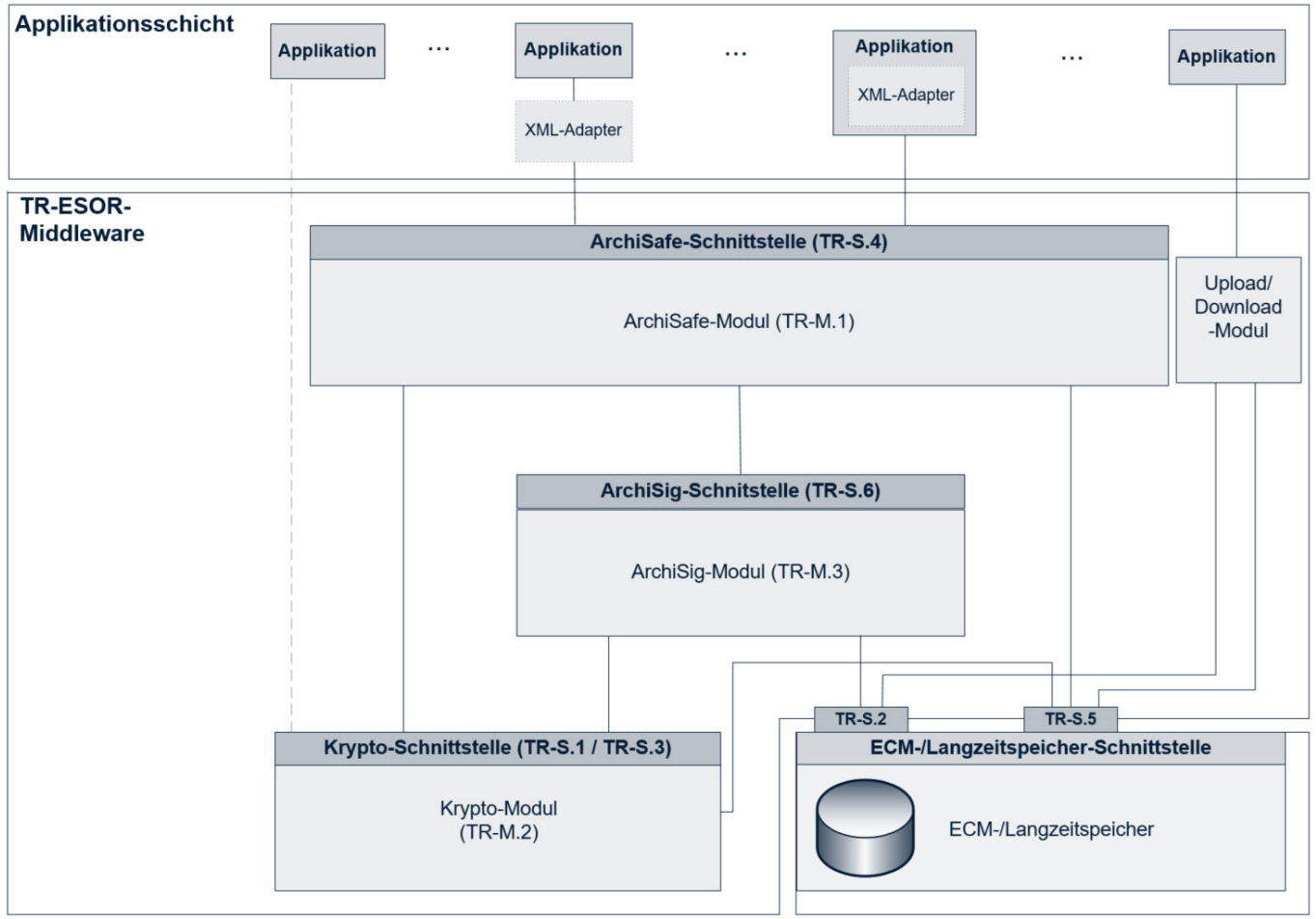
Building Blocks vertrauenswürdiger Langzeitarchive

Aspekt	Bedeutet
ArchiSafe	• Schnittstellenabstraktion • Abstraktion des Archivierungsformats (selbst beschreibendes Archiv) • Zugriffskontrolle • Zugreifbarkeit
ArchiSig	• Signaturerneuerung und Befähigung für den Erhalt des Beweiswerts elektronisch signierter Daten
Kryptografie	Vertrauenswürdige kryptografische Implementierungen, u. a. • Signaturprüfung • Hashwertberechnungen • Zufallszahlen • Anbindung Vertrauensdiensteanbieter

ANWENDUNGSFÄLLE

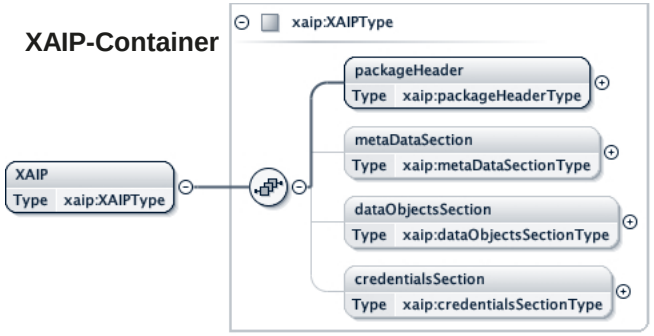


MODULARITÄT

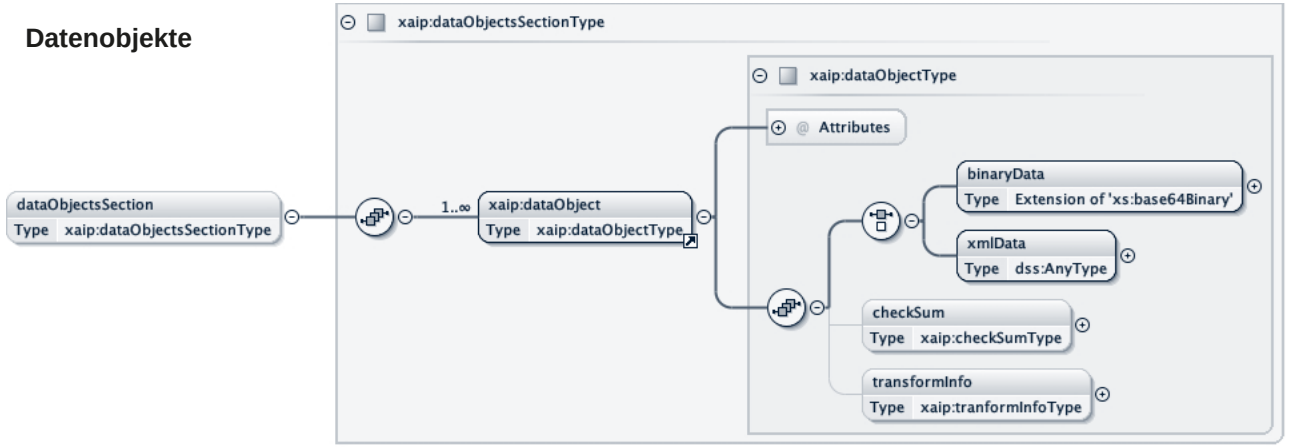


DATENSTRUKTUREN

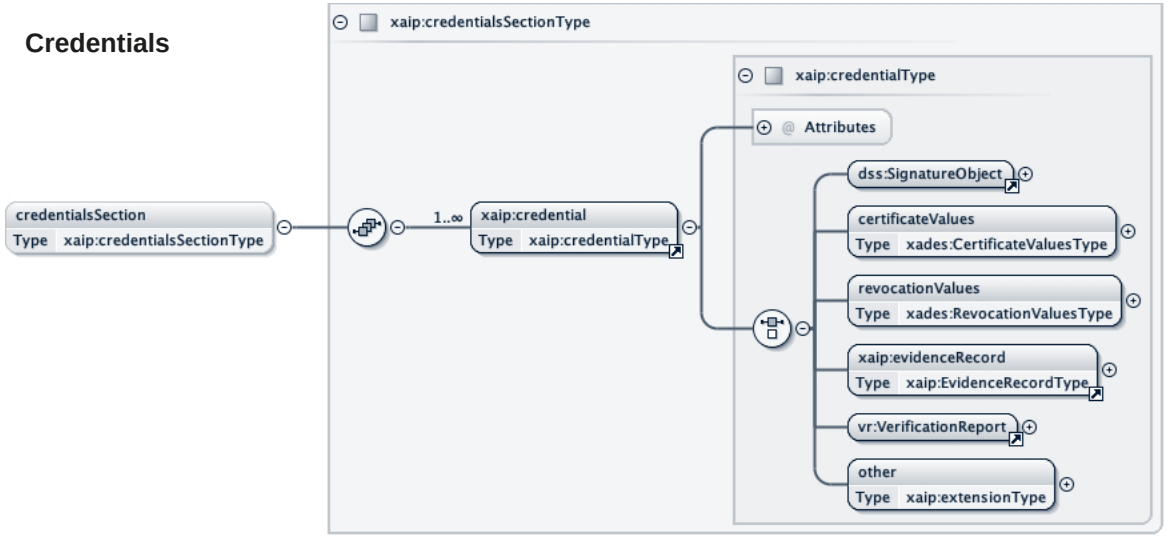
XAIP-Container



Datenobjekte



Credentials



SPEZIFISCHE PROFILE – VERSCHLÜSSELTE DOKUMENTE

- Vertraulichkeit der Dokumente vom Arbeitsplatz bis ins Archiv durchsetzen
- Erweiterung des XAIP-Schemas
- Handhabung der Zugriffsberechtigungen auf kryptografischer Ebene durchgesetzt
- Im Ergebnis: kryptografische Separation archivierter Daten als zusätzlicher Schutz

procilon Lösung

PRONEXT ARCHIVE MANAGER

- beinhaltet alle Komponenten, die für eine revisionssichere Ablage insbesondere qualifiziert signierter Dokumente sowie die Erhaltung der Gültigkeit von Signaturen und elektronischen Siegeln nach eIDAS benötigt werden

- bietet sämtliche kryptografischen Erweiterungen, die zur Sicherstellung der Beweiskraft elektronischer Dokumente entsprechend §71a der Zivilprozessordnung notwendig sind.

- kann über Archive hinaus auch in Dokumenten-managementsysteme und/oder eAktenlösungen integriert werden und

- ist **gemäß technischer Richtlinie** zertifiziert

VIELEN DANK

für Ihre Aufmerksamkeit

procilon GROUP
Leipziger Straße 110
04425 Taucha bei Leipzig

Telefon: 034298 4878-10
E-Mail: anfrage@procilon.de

www.procilon.de