FP/digital

100% eSIEGEL READY

FP HashSafe

Beweiswerterhaltende Archivierung von signierten Dateien im bestehenden Archiv nach TR-ESOR

Auch nach der neuen EU-Verordnung eIDAS verlieren Signaturen immer wieder ihre Sicherheitseignung. So sind signierte Dateien oder Dokumente in Ihrem Archiv zwar immer noch gültig signiert, aber die Hashwert- und die Verschlüsselungsalgorithmen werden als potenziell unsicher eingestuft und verlieren ihren Beweiswert.

Wie schon bei dem Algorithmen- und Hashwertwechsel 2007/2008 geistert dann das Gespenst der Nachsignatur durch die Archivwelt. Jede Datei nachzusignieren, ist oft allein durch die Größe des Archivs nicht machbar.

SecurITy made in Germany
Trust Seal
www.teletrust.de/itsmig

Mit dem auch in der Technischen Richtlinie BSI TR-03125 (TR-ESOR) „Beweiswerterhaltung kryptographisch signierter Dokumente“ des BSI aufgenommenen Archi-Sig-Verfahren lassen sich auch große signierte Aktenbestände im Laufe ihres Lebenszyklus in ihrem Beweiswert erhalten und überwachen. Dieses Verfahren ist als Stand der Technik sowohl im eGovernment- und im eHealth- als auch im eJustice-Gesetz benannt.

Im HashSafe wird für alle Dokumente eines Tages ein sogenannter Tages-Hashbaumknoten berechnet und mit einem qualifizierten Zeitstempel gesichert. Dasselbe Verfahren wird auf den Monats- und Jahresknoten angewendet. Bei einem Hashwert- oder Algorithmenwechsel können mit nur einem qualifizierten Zeitstempel pro Jahr die Signaturen beweiskräftig erhalten werden. Die dafür notwendige Neuberechnung der Hashwerte führt der HashSafe eigenständig durch.

Der sogenannte Evidence Record erlaubt es, pro Dokument einen gerichtsverwertbaren Datensatz zu generieren. Damit ist die Beweiskraft Ihrer signierten Dokumente auch für sehr lange Aufbewahrungszeiten von z. B. 110 Jahren gesichert. Die Integritätssicherheit der Dokumente in Ihrem Langzeitarchiv wird durch den HashSafe noch erhöht.

In der TR-ESOR ist dieses Verfahren festgehalten und der HashSafe Cert wurde nach BSI TR-03125 vom BSI zertifiziert.

Der HashSafe arbeitet mit Ihrem DMS/ECM-System zusammen und überwacht automatisch im Hintergrund die archivierten Signaturen.

Durch die Installation unseres HashSafe wird Ihr Datenbestand langfristig und beweiskräftig geschützt.

Die Anforderungen der Europäischen Datenschutz-Grundverordnung (DSGVO) für verlangte und geplante Löschfristen werden vollumfänglich erfüllt.

Archivierung mit Siegel und Beweiskrafterhaltung

// Langzeitarchiv für qualifizierte und fortgeschrittene Signaturen unter Windows oder Linux, parallel zu einem beliebigen bestehenden Archiv („Signaturarchiv“)

// Zertifiziert nach BSI TR-03125 „Beweiswerterhaltung kryptographisch signierter Dokumente“

// TR-ESOR-konform

// Unsignierte Dateien sind problemlos in die Hashwertberechnung aufnehmbar.

// Basiert auf ArchiSig-/Archi-Safe-Standards und Vorschriften der eIDAS für Bewahrungsdienste

// Überwachungsdienst verifiziert kontinuierlich die Integrität des Archivs (Gültigkeitsmodelle werden regelbasiert definiert)

// Anbindung an DMS/ECM und Langzeitarchiv per SOAP oder Archiv-API

// Signaturformate wie PKCS#7 (extern und eingebettet) und PDF werden unterstützt.

// Export des Beweispfades eines beliebigen Dokuments (Evidence Record Syntax gemäß RFC 4998)

// Gesichert durch qualifizierte Zeitstempel

// Erhaltung der Signaturen für lange Aufbewahrungszeiten, z. B. Elektronische Patientenakte, technische Unterlagen, Prüfprotokolle oder auch kommunales Langzeitarchiv

// Lösung zum Thema Beweiswerterhaltung von qualifizierten Signaturen (Bewahrdienste nach eIDAS) auch für Dienstleister

Ablauf der Langzeitspeicherung von Signaturen im TR-ESOR-konformen HashSafe

1. Anbindung mit SOAP-Schnittstelle
2. Signierte Daten werden ins DMS/ECM importiert.
3. Nach Zuordnung einer ID durchlaufen die Dokumente den HashSafe.
4. Signaturprüfung ohne Erstellung Verifikationsprotokoll (Verifikation lässt sich durch die Anbindung eines Auto-Verifier für die Performance-Erhöhung abschalten)
5. Prüfergebnis (OSCP-Abfrage) und Zertifikatsinformationen werden in der Datenbank gespeichert (Datum und Uhrzeit der Signaturerstellung, Dateiname, Seriennummer des unterzeichnenden Zertifikats, Gültigkeitszeitraum des unterzeichnenden Zertifikats, die Zertifikatskette des Signaturzertifikats, alle OCSP-Antworten des Trustcenters, Art und Schlüssellänge des verwendeten Signaturverfahrens und des verwendeten Hashverfahrens, SHA-256-Hashwerte des Ausgangsdokuments sowie eindeutige Dokumenten-ID des Dokuments).
6. Die Dokumente selbst verbleiben im Archiv.
7. Tages-, Monats- und Jahresknoten werden gebildet und durch qualifizierte Zeitstempel gesichert.
8. Bei Ablauf der Gültigkeit der Algorithmen wird in der Baumstruktur ein neuer Hashwert berechnet und durch einen neuen Zeitstempel mit neuer Gültigkeit pro Jahr gesichert.

Die Erstellung eines Evidence Record kann konfiguriert werden. Die Dokumente werden nicht einzeln nachsigniert.

Die **FP Digital Business Solutions GmbH** bietet seit mehr als 20 Jahren intelligente Lösungen für Unternehmen und Behörden zur Bearbeitung von analogen und elektronischen Dokumenten und zur rechtssicheren Kommunikation, einschließlich digitaler Signaturen, nach höchsten Sicherheitsstandards. Wir sind unter anderem ISO/IEC-27001-zertifiziert.

Zertifiziert
ISO 9001
ISO 14001
ISO/IEC 27001
ISO/IGZ 27001
ISO 45001
ISO 50001

Das zeichnet uns aus – unsere Auszeichnungen und Kooperationen:

BUNDESDRUCKEREI · Security made in Germany · Swisscom Trust Services · DATEV Marktplatz PREMIUM PARTNER · Software Hosted in Germany · Klimabeitrag

FP/digital

FP Digital Business Solutions GmbH / Trebuser Straße 47, Haus 1 / 15517 Fürstenwalde
Mehr Informationen finden Sie unter **fp-dbs.com**. Gerne beraten wir Sie persönlich unter **Telefon +49 30 364440-300**.

www.linkedin.com/company/fpdigitalbusinesssolutions/ // www.facebook.com/fpdigitalbusinesssolutions // www.xing.com/pages/fp-digital-business-solutions-gmbh