FP | mentana claimsoft

ZERTIFIZIERT NACH TR-ESOR, DAUERHAFTE BEWEISWERTERHALTUNG

GRÜNDE FÜR DEN EINSATZ DES HASHSAFE

- Kryptografisch signierte Dokumente im Archiv müssen beweiswerterhaltend aufbewahrt werden
- „Ablaufende" Signaturen im digitalen Archiv müssen nachsigniert werden
- Evidence Record[1] (Beweispfade für digitale Signaturen) müssen für Gerichtsverfahren vorgehalten werden
- Nachsignatur ist zeitintensiv und vor Ablauf der Signaturen zeitlich oft nicht möglich
- Das Vorhalten der Zeitpunkte und die Organisation ist mehr als aufwändig
- BSI[2] TR-ESOR[3] Zertifizierung ist erforderlich
- lange Aufbewahrungszeiten von bis zu 110 Jahren sind erforderlich und somit auch die gültige Erhaltung der Signaturen
- Digitale Langzeitarchivierung nach rechtlichen Vorschriften erfüllen
- Verifikationsprotokolle innerhalb des Archivierungsprozesses erstellen

WO WIRD DER HASHSAFE EINGESETZT?

- Aufkündigung von Algorithmen und Hashwerten durch die Bundesnetzagentur
- Beweiswerthaltung des Archives
- Vorlage der Beweiswerterhaltung vor Gericht
- Bundesbehörden im Rahmen ihrer Aufbewahrungspflicht

IHR NUTZEN IST IHR VORTEIL

Automatisches Monitoring erspart Zeit, Geld und Nerven.

Für den Nachweis des Beweispfades wird der Evidence Record automatische erstellt, genau wie die „Nachsignatur".

Die durch das BSI zertifizierte Version erfüllt die rechtlichen Vorschriften für Bundesbehörden

Zusammenarbeit mit bestehenden DMS/ECM und Archiven sichert das Zusammenspiel der Komponenten.

DER HASHSAFE UND SEINE MERKMALE IM ÜBERBLICK:

- Erhaltung der Signaturen für lange Aufbewahrungszeiten
- Verifikation eingehender Signaturen und Zeitstempel mit erstelltem Prüfprotokoll
- Bildung von Hashbaumarchitektur nach ArchiSig
- Neuberechnung ablaufender Algorythmen > Hashwerte
- Erstellung der Evidence Record im RFC 4998 Standard (ASN.1[4])
- Signaturformate wie PKCS#7[5] (extern und eingebettet), PDF und TIFF werden unterstützt.
- Verwendung des „Data Structure for the Security Suitability of Cryptographic Algorithms (DSSC)" Formats (RFC 5698) um die Gültigkeit der Algorithmen zu ermitteln
- Schutz der Softwarekomponenten vor Manipulation
- Zertifiziert nach TR-ESOR

1 Nachweisdatei
2 Bundesamt für Sicherheit in der Informationstechnik
3 Technische Richtlinie für die Beweiswerterhaltung kryptographisch signierter Dokumente
4 Abstract Syntax Notation One (Abstrakte Syntaxnotation Eins)
5 Public Key Cryptography Standards

SYSTEMVORAUSSETZUNGEN:

Betriebssysteme

Windows 2008 / 2008 R2 Server
Windows 2012 / 2012 R2 Server
Windows Vista SP1
Windows 7
Windows 8.1
Windows 10

Mindestanforderung an die Hardware

- Festplatte: mindestens 300 GB
- RAM: mindestens 4096 GB
- Internetzugang für OCSP[6] Abfragen am Trustcenter und Abruf von Zeitstempeln
- Volumenabschätzung: pro Datensatz fallen ca. 13 KB an.

Benötigte Softwarekomponenten

- JAVA Runtime 1.8
- Apache Tomcat 7.0 oder höher
- PostgreSQL 9 oder höher oder Ocale 9i oder höher
- Für die HashSafe-GUI[7] .NET 4.0

Import von Dokumenten ohne Signatur

- Über globale Einstellung oder über Importschnittstelle
- Keine Verifikation
- Nur Hashwert-Berechnung

Importmöglichkeiten

- SOAP[8]

Importgeschwindigkeit

- Ca. 15.000 Dokumente mit einer Größe von 10 MB pro Stunde bei Verwendung von OCSP-Caching [9]und Unterschriften von 1 bis 2 Zertifikaten
- Ohne OCSP-Caching hängt die Importgeschwindigkeit von der Antwortzeit des OCSP-Responders ab.
- Synchrone Einlieferung

Aufteilung auf Organisationseinheiten

- Aufbau des Hash-Baums pro Organisationseinheit

Was passiert beim Import

- Verifikation der Signatur
- Prüfung des Zertifikats-Pfades

---

6 Online Certificate Status Protocol
7 Graphical User Interface (Grafische Benutzeroberfläche)
8 Simple Object Access Protocol
9 Zwischenspeicherung

- OCSP-Abfrage
- Berechnung der Hashwerte des Dokumentes und der Signatur (nur bei externen Signaturen)
- Speicherung in der Datenbank
- Erstellung eines XML[10]-Verifikationsreports und Ablage in der Datenbank
- Weiterleitung an das angebundene Langzeitarchiv
- Speicherung der AOID[11] aus dem Langzeitarchiv in der HashSafe Datenbank

Zertifikatspeicher

- Alle zur Verifikation benötigten Zertifikate müssen in den HashSafe importiert werden. Dazu gibt es eine SOAP-Schnittstelle. Alternativ kann die HashSafe-GUI verwendet werden.

Hash-Baum Aufbau

- Es gibt Tages-, Monats- und Jahresknoten
- Weitere Konten sind die Root- und Sub-Konten unterhalb der Tages-Knoten
- Automatische Erstellung des Konten beim Tageswechsel und zu Konfigurierbaren Zeitpunkten
- Auftragserstellung für Knotenerstellung per SOAP oder GUI
- Kann kein Zeitstempel angefordert werden, wird kein Tage, Monats- oder Jahres-Knoten erstell.
- Gleichzeitige Erstellung eines ASN.1 Tagesknotens (Erfordert zusätzliche Zeitstempel)

Neuberechnung

- Vor Ablauf des Zeitstempels (durch Ablauf des Hash-Algorithmus) wird ein neuer Zeitstempel mit neuem Hash-Algorithmus auf dem letzten Knoten angebracht.
- Vor Ablauf des Hash-Algorithmus des Dokumenten-Hashs muss das Dokument aus dem Langzeitarchiv angefordert und ein neuer Hash-Wert berechnet werden. Zusammen mit dem reduzierten Archivbaum wird dieser Hash-Wert in einen der nächsten Tages-Knoten integriert.
- Vorlaufzeit für Neuberechnung bei Algorithmen erfassbar

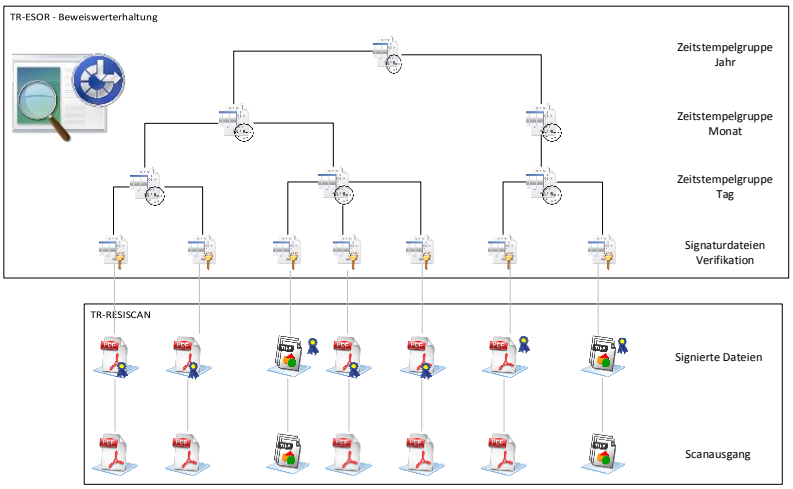
Zeitstempel

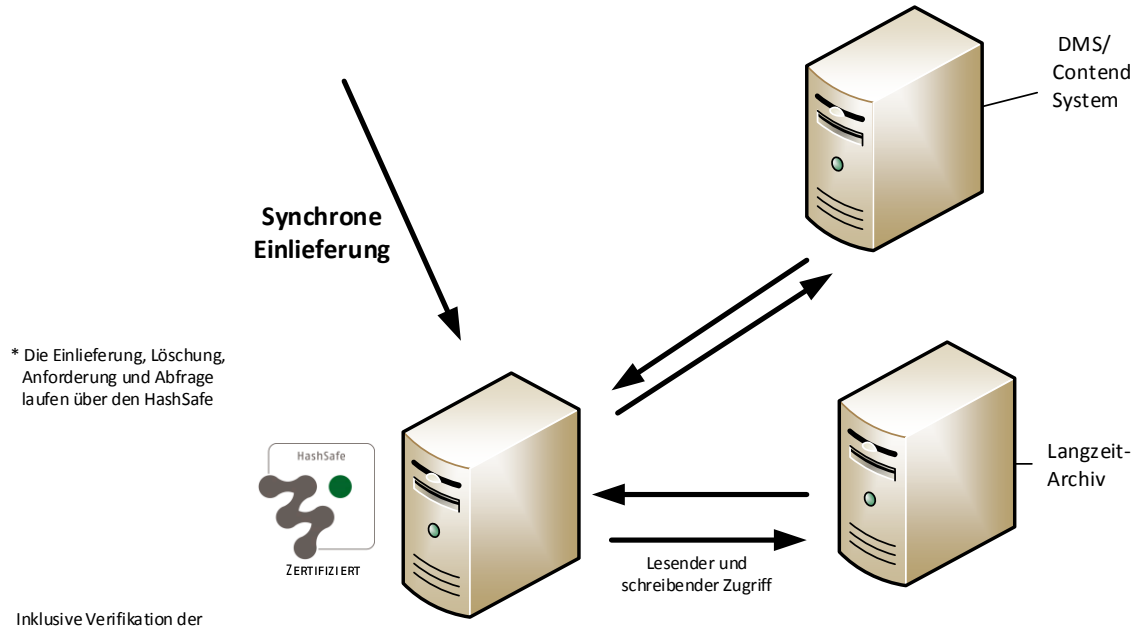
- Nur Zeitstempel des Signaturportals[12] werden unterstützt

10 Extensible Markup Language (erweiterbare Auszeichnungssprache)
11 Archivedataobject ID (ID des Archivdatenobjektes)
12 www.signaturportal.de

EINSATZ

EIN BEISPIELSZENARIO





Mentana-Claimsoft GmbH
EIN UNTERNEHEMEN DER FP-GRUPPE

Trebuser Str. 47 – Haus 1
D-15517 Fürstenwalde

Griesbergstr. 8
D-31162 Bad Salzdetfurth

Tel: +49 5063 / 27744-0
Fax: +49 5063 / 27744-50

vertrieb@mentana.de
vertrieb@mentana.de-mail.de

www.mentana-claimsoft.de