Signaturlangzeitarchiv für dauerhafte Beweiswertsicherung qualifizierter Signaturen gemäß § 17 SigV

FUNKTIONSBESCHREIBUNG Beweiswertsicherung qualifizierter Signaturen

Hash-Safe ist eine ArchiSig-konforme und an TR-ESOR angelehnte Komponente, die die gespeicherten Signaturinformationen beweiswerterhaltend, auch über die Gültigkeit von Algorithmen hinaus, verwaltet. Der Hash-Safe wird dabei an ein bereits vorhandenes Archiv angebunden
Hash-Safe umfasst alle Funktionen zur Konsolidierung und Prüfung des

Signaturdatenbestandes.

Die Steuerung erfolgt über einen Verifikationsarbeitsplatz. Um die unterschiedlichen Branchen-anforderungen abbilden zu können, können die Regeln zur Signatursicherung weitgehend frei formuliert werden. Hash-Safe ermöglicht jederzeit die Prüfung eines signierten Dokuments unter Aufbau und Nachweis einer Integritätskette.

Es gibt zwei Schnittstellen zu berücksichtigen:
1. Input Modul: Eingang der signierten Dokumente ins Archiv
2. Retrieval Modul: Abruf der Dokumente aus dem Archiv zur Nachberechnung/Prüfung

Zu 1. Input Modul

Das vorhandene Archiv stellt dem Hash-Safe neu eingegangene Dokumente per SOAP-Aufruf oder ACSII/XML-Schnittstelle zur Verfügung. Dabei werden alle Signaturen selbst geprüft, wobei OCSP-Abfragen zwischengespeichert werden können, d.h. es wird vorab geprüft, ob mehrere Dokumente von einem Zertifikat unterschrieben wurden. Dieser Stapel an Dokumenten wird dann zusammen verifiziert, so dass am Ende nur eine OCSP- bzw. Sperrlistenabfrage benötigt wird.

Es werden u.a. folgenden Attribute in einem Datensatz abgespeichert:
- Datum und Uhrzeit der Signaturerstellung
- Dateiname
- Seriennummer des unterzeichnenden Zertifikates
- Gültigkeitszeitraum des unterzeichnenden Zertifikates
- Die Zertifikatskette des Signaturzertifikats
- Alle OCSP Antworten des Trustcenters
- Art und Schlüssellänge des verwendeten Signaturverfahrens
- Art und Schlüssellänge des verwendeten Hashverfahrens
- SHA-256 und SHA-512 Hash des Ausgangsdokumentes
- Eindeutige Dokumenten-ID des Dokuments im Archiv

Das signierte Dokument selbst wird **nicht** im Hash-Safe abgelegt. Die Signaturdaten werden parallel zu den Dokumenten in einem DMS- oder Archivsystem separat gespeichert. Hash-Safe ersetzt kein DMS- oder Archivsystem!
Im Zusammenspiel mit dem Archivsystem fordert Hash-Safe die erforderlichen Ursprungsdaten rechtzeitig und automatisch vom Archiv oder DMS System an. Sollte es keine Schnittstelle zu dem vorhandenen Archiv geben, wird diese in Zusammenarbeit mit dem Archivhersteller programmiert.

Zu 2. Retrieval Modul

Zwecks Berechnung neuer Hashwerte von bestehenden, signierten Dokumenten bei Ablauf von Hashalgorithmen oder bei Dokumentenprüfungen, muss ein lesender Zugriff auf das Archiv möglich sein. Über die gespeicherte Dokumenten-ID wird auf das entsprechende Dokument per SOAP-Aufruf lesend zugegriffen. Andere Schnittstellen sind möglich.

Verifikationsumgebung

Die Beweiswirkung von signierten Dokumenten kann nur dann garantiert werden, wenn die Dokumente jederzeit eine gültige Signatur tragen und dieser Umstand lückenlos nachweisbar ist. Derzeit können folgende Umstände dazu führen, dass die Gültigkeit einer Signatur aufgehoben wird:

- Die Eignung des verwendeten Hashwertverfahrens wird aufgehoben
- Die Eignung des verwendeten Verschlüsselungsverfahrens wird aufgehoben

Die Verwendungsdauer der entsprechenden Sicherungsmittel (Hashwertverfahren und Verschlüsselungsalgorithmus) wird von der Bundesnetzagentur festgelegt und jährlich in der „Übersicht über geeignete Algorithmen“ veröffentlicht.

Die erneute qualifizierte Signatur eines bereits signierten Dokumentes stellt keine weitere Willenserklärung dar, sondern ist reines Sicherungsmittel vorhandener Willenserklärungen. Daher ist es möglich, Dokumente, deren Signaturgültigkeit abläuft, mit einem qualifizierten Zeitstempel zu sichern.

Die Verifikationsumgebung selbst besteht aus drei Komponenten:

Zeitstempel-Dienst

Der Zeitstempeldienst kapselt sämtliche Zugriffe auf den Zeitstempelanbieter. Dabei können qualifizierte Zeitstempel von Trustcentern abrufen werden.

Hashbaum-Archiv

Das Hashbaum-Archiv ist die zentrale Komponente des Verifikationsservers. Es speichert die Signaturen und die im vorigen Abschnitt genannten Attribute in einer Datenbank. Die Lösung der Mentana verwendet als RDBMS standardmäßig PostgreSQL. Dieses Datenbanksystem unterstützt ein Hot-Backup, so dass der Betrieb der Signaturumgebung nicht vom Backup unterbrochen wird. Es können nach Absprache oder Notwendigkeit auch andere SQL-Datenbanken zum Einsatz kommen.

Innerhalb des Hashbaum-Archivs werden die gespeicherten Signaturen zu hierarchischen Strukturen zusammengefasst. Für jeden dieser Hashcontainer kann ein eindeutiger Hashwert bestimmt werden.

Die Zeiträume für das Bilden der Hashbaum-Knoten sind wie folgt definiert:

1. Die Blattebene bilden die Signaturen. Diese sind in der Datenbank gespeichert.
2. Die nächste Ebene wird tageweise gebildet. Für jeden Hashwert, der sämtliche Signaturen eines Tags zusammenfasst, wird ein qualifizierter Zeitstempel angefordert.
3. Ebene 3 wird monatsweise gebildet. Durch den Verzicht auf wöchentlich erstellte Container entstehen keinerlei Überlappungen im Gesamtansatz. Für jeden Monatshashwert wird ein qualifizierter Zeitstempel angefordert.
4. Als Jahres-Wurzelknoten des Hashbaumes wird der Hashwert über alle Hashwerte der Monatsebene gebildet.

Innerhalb der Datenbank werden unabhängige Jahresstrukturen gespeichert. Eine weitere Bündelung bis auf Jahrzehnte scheint in Anbetracht des minimalen Zugewinns nicht sinnvoll. Die Datenstrukturen werden auf Wunsch gerne offen gelegt.

Volumenabschätzung: Es fallen ca. 15-20 KByte pro Datensatz inkl. Binärbaumaufbau an. Dies ist bei der Planung der Hardware entsprechend zu berücksichtigen.

Revisions- /Administrationsarbeitsplatz: Über eine mitgelieferte Windowssoftware kann der Inhalt der Hashbaum-Datenbank angesehen / ausgelesen werden. Ein Export des Signaturpfades kann bis auf Dokumentenebene durchgeführt werden. In diesem Fall wird vom System ein den Prüfablauf beschreibendes Begleitdokument erzeugt und sämtliche Zeitstempel, beginnend bei der Dokumentensignatur bis zum Wurzelknoten, exportiert. Der Export geschieht in Form einer XML-Datei, die sich an den Vorgaben der ERS (Evidence Record Syntax) gemäß RFC 4998 orientiert oder per ASN.1 Standard..

Überwachungsdienst

Der Überwachungsdienst verifiziert in regelmäßigen Abständen den Inhalt des Hashbaum-Archivs. Das regelbasierte Überwachungssystem ist über ein Webfrontend konfigurierbar. Werden Dokumente erkannt, deren Signaturgültigkeit abläuft, wird ein Archivar über E-Mail informiert. Die fraglichen Dokumente können wahlweise auf jeder Stufe der Hierarchie automatisch erneut zeitgestempelt werden. Dabei werden sämtliche vorhergehenden Signaturen in den Prozess eingebunden. Wird ein Zeitstempel unterhalb des Wurzelknotens erneuert, so werden nach einer konfigurierbaren Zeit sämtliche darüber liegenden Knoten aktualisiert.

Die Überprüfung der Signaturen schließt eine Prüfung der Zertifikate gegenüber der PKI des ausstellenden Trustcenters unter Verwendung von CRL-Listen und OCSP-Anfragen ein.

Eine Revisions- bzw. Administrationsarbeitsplatzsoftware unter Windows ist Bestandteil des Hash-Safes. Damit können u.a. die Beweiswertpfade zu signierten Dokumenten abgerufen und der Hash-Safe komplett administriert werden.

Mindestanforderungen an die Hardware (Hash-Safe)

Empfohlen wird ein separater Server mit Windows Server 2003 (oder Linux).
Die Mindestanforderung an die Hardware ist:

- Prozessor: aktuelles Modell
- Festplatte(n): S-ATA oder SCSI, mind. 300 GB
- RAM: min. 4096 MB
- Internetzugang für OCSP Abfragen beim Trustcenter
- Proxy-Unterstützung

Systemvoraussetzungen:

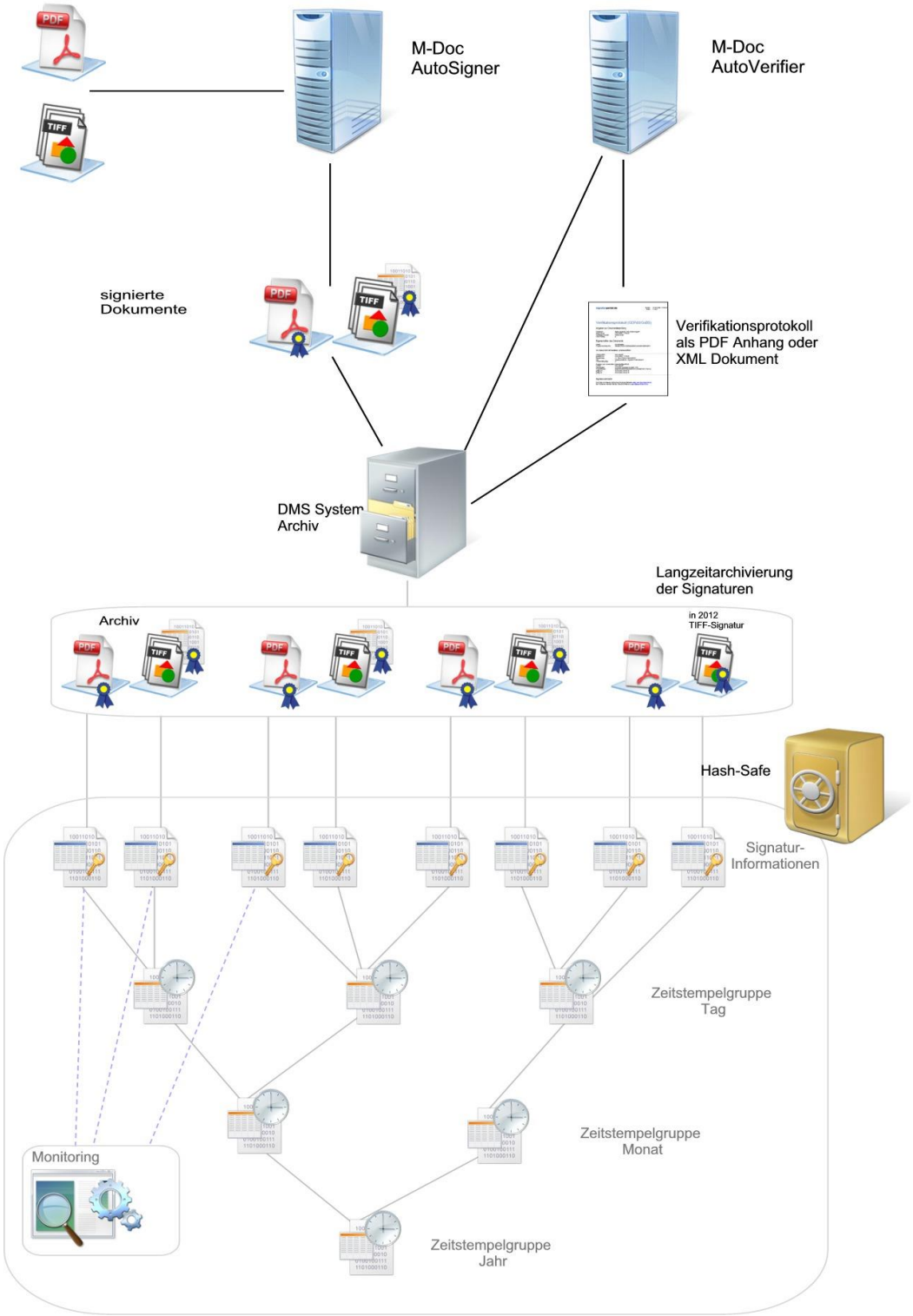
Betriebssysteme:

Windows

Windows 2008 Server
Windows 2012 Server
Windows Vista SP1
Windows 7
Windows 8

Linux

Verschiedene Derivate möglich,
empfohlen wird zurzeit Debian, min. 6.0



Mentana-Claimsoft GmbH
EIN UNTERNEHMEN DER FP-GRUPPE

Tel: +49 5063 / 2 77 44 - 0
Fax: +49 5063 / 2 77 44 - 50
E-Mail: vertrieb@mentana.de
De-Mail: vertrieb@mentana.de-mail.de
www.mentana-claimsoft.de
www.fp-demail.de

Hannover / Bad Salzdetfurth
Griesbergstr. 8
D-31162 Bad Salzdetfurth

Berlin / Fürstenwalde
Trebuser Str. 47 - Haus 1
D-15517 Fürstenwalde