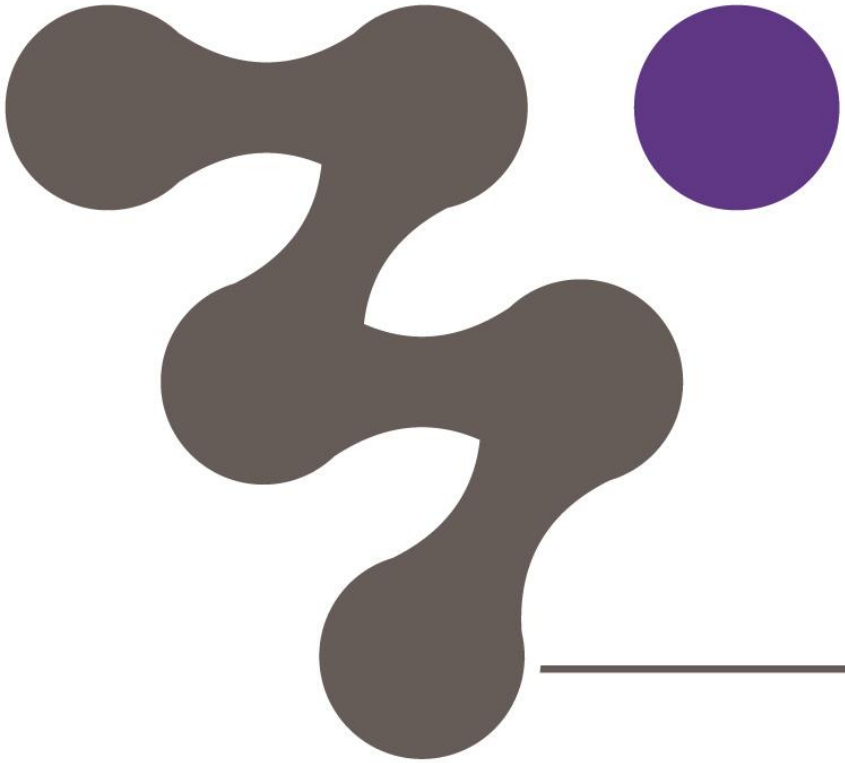
FP mentana claimsoft

OfficeSigner



VER- UND ENTSCHLÜSSELUNG VON
SENSIBLEN PERSONENBEZOGENEN DATEN

WARUM EIGENTLICH DER EINSATZ DES OFFICESIGNERS?

WO WIRD DER OFFICESIGNER EINGESETZT?

IHR NUTZEN IST IHR VORTEIL

DER OFFICESIGNER UND SEINE MERKMALE IM ÜBERBLICK:

FEATURE

SYSTEMVORAUSSETZUNGEN:

Betriebssysteme

Windows 2008 Server

Windows 2012 Server

Windows Vista SP1

Windows 7

Windows 8

Linux
Verschiedene Derivate möglich, empfohlen
wird zurzeit Debian , mind. 6.0

Mindestanforderung an die Hardware

Empfohlen wird ein separater Server mit Windows Server 2008 (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 gegen Trustcenter

Schnittstellen

Input Modul:

Eingang der signierten Dokumente ins Archiv:
Das vorhandene Archiv stellt dem HashSafe 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. folgende Attribute in einem Datensatz gespeichert:
- 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 HashSafe abgelegt. Die Signaturdaten werden parallel zu den Dokumenten und separat in einem DMS- oder Archivsystem gespeichert. HashSafe ersetzt kein DMS- oder Archivsystem! Im Zusammenspiel mit dem Archivsystem fordert HashSafe 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.

Retrieval Modul:

Abruf der Dokumente aus dem Archiv zur Nachberechnung/Prüfung:

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.

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