



Hash-Safe

Long-term signature archive for permanent preservation of the evidence value for qualified signatures according to § 17 of the German Digital Signature Ordinance (SigV)

The Challenge

Documents, which must be kept for periods of time that exceed the expected validity of the signature or the hash algorithms, must be stored in a timely manner in order to **preserve the evidence value**. To ensure the integrity and authenticity of the documents, they must be **signed again** before the algorithm expires in accordance with **§ 17 SigV** and provided with a **qualified timestamp**. However, since the amount of data doubles every year on average, renewing the signature for every single document is neither acceptable as far as costs are concerned nor technically feasible in a reasonable amount of time.

The Solution

To solve this problem, all the signature data must be **consolidated** during the archiving process. In addition, **hash trees** are generated, which represent the data for a particular day, month or year. Within the hash trees, evidence value can be permanently maintained based on cryptographic processes.

The main service provided by Hash-Safe is the consolidation of stored data for preserving signatures.

Verification Workstation

Hash-Safe includes all the functions necessary for consolidating and verifying your signature data. The management of these functions is done at a verification workstation. To map the requirements of different industries, the rules for signature preservation can be generally formulated as you wish. Hash-Safe allows the verification of a signed document at any time based on the establishment and proof of an integrity chain according to RFC 4998 (Evidence Record Syntax). For storage times over 30 years, certification chains can be stored in their entirety and provided locally for verification purposes.

DMS and Archive Management

The signature data are saved separately parallel to the documents being saved in a DMS or archive system. **Hash-Safe does not replace a DMS or archive system!** In conjunction with the archive system, Hash-Safe requests the required source data **promptly and automatically from** the archive or DMS system.

This enables documents to be preserved even after the expiration of the underlying hash algorithms for the documents.

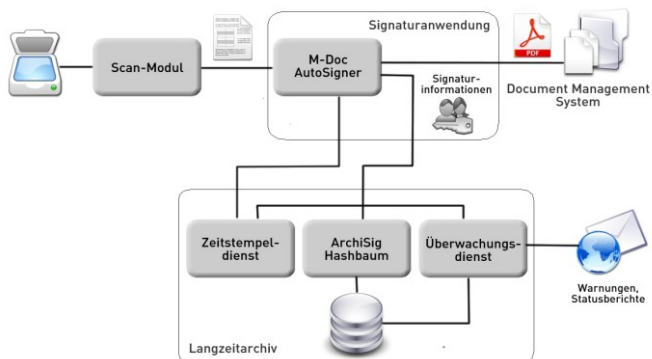
Guarantee of probative evidence

- Social Benefits Offices Archives
- Booking data
- Electronic decisions
- Electronic verdicts
- Electronic invoices

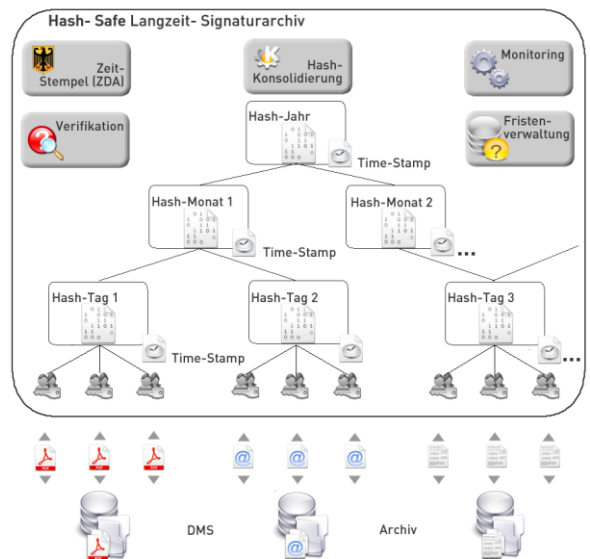
Features

- Open interface architecture
 - Directory-based
 - Web Services (SOAP)
 - E-Mail Proxy (SMTP)
 - Secure FTP
 - Database interfaces ...
- Use of timestamps by accredited Trust Centers
 - Authentidate AG
 - Deutsche Post Com
 - D-Trust

Linking to an archive or DMS



Hash-Safe Workflow



Related Products

- **Office-Signer** – for Windows-desktop based signatures, timestamps and verification without any transactional fees. Direct integration into Windows Explorer and Microsoft Office / OpenOffice.
- **M-Doc AutoSigner DataCenter Edition** – for qualified, automatic and server-based mass signatures without any transactional fees. Available for Windows and Linux.
- **M-Doc AutoVerifier DataCenter Edition** – server-based verification of signatures and certificate information without any transactional fees. Available for Windows and Linux.

Contact and Ordering

08 – 510 605 60

SignGuard Europe AB
Stockholm
Drottninggatan 61
S-111 21 Stockholm
Phone: +46 (0)8 510 605 60

info@SignGuard.se
www.SignGuard.se