

Archival  
of Documents of  
the Electronic Record Procedure  
(eANV)

Consist ITU  
Environmental Software GmbH  
23.02.2009

According to the Ordinance on Waste Recovery and Disposal Records, electronic documents need to be provided with qualified electronic signatures which must be archived according to legal regulations.

The documents have a retention period of at least eight years. The retention period results from a term of up to five years for records of proper waste management and the minimum registration period for registered documents of three years as specified in the Ordinance on Waste Recovery and Disposal Records (Sec. 25 (1)). Moreover, the documents are also commercial letters, which according to the German Commercial Code (HGB Sec. 257) are subject to an archival obligation of ten years.

According to the provisions of the Digital Signature Act (SigG) and Digital Signature Ordinance (SigV) proper archival involves the conservation of validity of electronic signatures

## 1 Modawi Solution

Since conservation of the validity of signatures cannot be restored without limitation at a later date, the Modawi solution includes a long-term archive for signatures as required by ArchiSig. The signature server SecPKI included in the Modawi scope of service automatically archives all signatures it signs or verifies as required by ArchiSig. Regular re-signing of the roots of the hash trees with qualified timestamps ensures the integrity of the archived signatures. The necessary qualified timestamps must be issued by a trust center or another suitable timestamp service.

At receipt of documents, Modawi ensures that the signatures received are verified and thus entered into the signature archive.

Documentation of the validity of signatures can already be generated with the current version using the appropriate tools, and/or the certification information can be provided as an Evidence Record (as specified in RFC 4998). A check of "old" signatures is thus also possible for third parties. Of course, the Modawi solution can also verify "old" signatures on that basis. Future Modawi versions will also conveniently offer the generation of evidence documents through the Modawi interface.

However, the BMU interface doesn't yet specify the exchange of these evidence records precisely, so that adjustments will probably be necessary.

Since the documents in waste management are already in XML format, an additional XML container as specified in ArchiSafe is not required.

Modawi provides a comprehensive solution for the processing and archival of electronically signed documents, and we are more than happy to assist in its application.

## 2 Background information

### 2.1 Archival of electronically signed documents

For the archival of electronically signed documents, the documents must be stored securely and the signatures must be archived.

The signature archive fulfills three tasks:

- 1) Documentation of the signature certificate validity at the time of receipt
- 2) Conservation of signature validity by means of re-signing with qualified timestamps
- 3) Generation of certification that the signature was valid throughout the archival period (proof of integrity)

Signature archival must first document that the signature was created with a valid signature certificate. Since trust centers only give information about the current status of the certificates issued, it is also necessary to check a received signature and its certificate as quickly as possible and to document that check. In practice, what is saved in the signature archive is the result of the certificate check received in signed form with a timestamp from the trust center (a signed OCSP response).

More powerful computers and advances in cryptanalysis make signatures less secure over time. The signature consists of a hash value over the document and the encryption of the hash value with the signer's private key.

A signature archive then uses re-signing with current encryption functions and timestamps to ensure that the integrity of the original signature can be verified. However, if the hash function becomes insecure, the hash values over the documents must also be renewed.

The possibility of insecurity of the hash function is very unlikely with the SHA256 hash function used today, and due to the absence of any suitable alternative, it is currently not possible to protect against it. New hash functions are under development, but they won't be ready before 2012. It will also be more cost-effective to consider suitable processes for securing signatures only after a significant insecurity has been shown (notification by the Federal Network Agency (BNetzA) on crypto algorithms). It is very probable that it will not be necessary to rehash every document, but that larger blocks can be formed. The prerequisite for any securing project is a signature archive of valid signatures stored separately from the document archive.

## 2.2 Solution approaches

For the archival of signed documents, the market currently offers different solution approaches: The ArchiSig concept, the ArchiSoft software by SIT, and the ArchiSafe project.

In 2004, a process was presented in the context of the ArchiSig project for conserving signatures very efficiently. Hash values are stored along with the OCSP responses (certificate checks) in so-called "hash trees", and the values contained are themselves also secured with hash values. The tree structure means that only the roots of the hash trees need to be re-signed with timestamps. This allows signatures to be retained for many documents with just a few timestamps. The process is supported by legal opinion ("Legal opinion on the Signature Law compliance of the standardization suggestion 'Long-Term Conservation of Electronic Signatures for the ISIS-MTT specification of June 30, 2004' (ArchiSig) of July 20, 2004" by Dr. Alexander Roßnagel). The ArchiSig concept is also used in the Modawi solution.

The Fraunhofer Institute for Secure Information Technology (SIT) has used ArchiSig to develop the ArchiSoft software package.

ArchiSafe is a project of the Physikalisch Technische Bundesanstalt (PTB), which has produced a process for the long-term archival of documents (including electronically signed documents). Documents suitable for long-term archival (TIFF, PDF/A, text) are archived with metadata in XML containers, and signatures are stored with ArchiSig. Besides signature archival, the project also addresses the fact that the long-term conservation of the documents must be ensured. This is the reason for restricting the system to the use of a few suitable formats. Furthermore, the official requirements defined in the DOMEA concept for electronic files are also taken into consideration. In 2008, ArchiSafe also published a protection profile for such systems with the Federal Office for Information Security (BSI). However, to date no system has been shown to have been tested using it.