Fraunhofer
SIT

FRAUNHOFER INSTITUTE FOR
SECURE INFORMATION TECHNOLOGY

*Fraunhofer Institute for Secure Information Technology SIT*

*Contact:*
*Dipl.-Inform. Michael Herfert*
*Rheinstrasse 75*
*64295 Darmstadt, Germany*

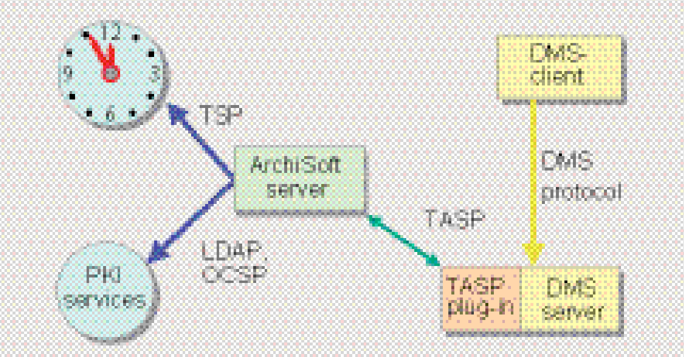
*Telephone: 0 61 51 8 69-329*
*Fax: 0 61 51 8 69-322*
*michael.herfert@sit.fraunhofer.de*
*www.sit.fraunhofer.de/archisoft*

# ARCHISOFT

## LONG-TERM ARCHIVAL OF DIGITAL DOCUMENTS

Electronic business processes in industry and public administration depend on documents with secure and permanent digital signatures – as a basic precondition of paperless yet audit-compliant processing.

The statutory retention periods for this kind of document are often extremely long, for example 30 years in the German public health system. The same requirement applies to the digital signatures; unfortunately, however, these are liable to expire or »fade« if they were created using techniques that have since become obsolete and are no longer sufficiently secure. In the event of a dispute, a signature can lose its cryptographic probative value when the case is taken to court. By preserving the quality of signatures – and hence of the documents in which they are contained – »ArchiSoft« ensures that they continue to be accepted as valid legal evidence.



*ArchiSoft interacts optimally with document management systems.*

ArchiSoft, the software package developed by Fraunhofer Institute SIT, updates signatures as and when necessary before they become outdated. The fact that it can be integrated in a DMS (document management system) makes it particularly good value for money: instead of signing every single document, it bundles existing documents in a tree together with their signatures and assigns them a new, shared signature that is more difficult to crack than the individual signatures. This internationally accepted method has been defined in the RFC 4998 standard in collaboration with SIT.

Even conservative estimates admit to a cost-cutting factor of 2000 as a result of bundling; in practice, the figure is likely to be higher still. ArchiSoft is also available as a service or as a mail server component for companies without a DMS.

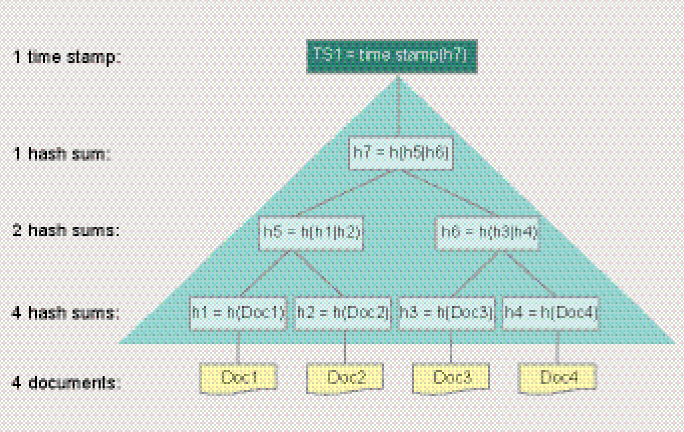
### Professional software package

The ArchiSoft package ensures that digital signatures can be reliably used as evidence for several decades to come, regardless of whether they belong to your own documents or to those of your business associates. ArchiSoft is written in Java and therefore runs on all popular platforms. SIT markets ArchiSoft together with commercial partners who provide the necessary support and hotline for this professional software product.

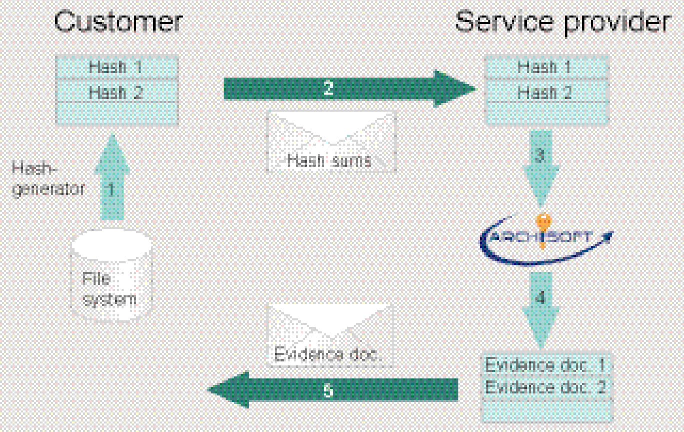
### Easy integration into DMS

ArchiSoft can be connected to almost any DMS in a few easy steps. All that is required is a small plug-in, which is very simple to

06/2010



*The time stamps assigned by ArchiSoft can also be shared by several documents – an important cost saving.*



*ArchiSoft is also available as a service for companies that are unwilling to install the software themselves.*

program, at the DMS server end. This plug-in communicates with the ArchiSoft server using the TASP (Trusted Archive Service Protocol) protocol. As soon as the DMS server has confirmed to ArchiSoft that a particular document exists, it can strike »faded« signatures from its list of potential problems – from now on, ArchiSoft takes over control of the complete cycle.

### ArchiSoft as a service

If your company is unwilling to invest in its own ArchiSoft server, you can still reap the benefit by purchasing ArchiSoft as a service from a SIT partner. The principle is simple: you create hash sums of your files and send them to the server. With ArchiSoft's help, the server then builds the hash trees that are needed to generate evidence documents. These evidence documents are subsequently returned to the user.

Using SIT's verification application, you can prove the validity of your documents from the evidence documents and the originals to which they belong. The judge in a court of law or an external expert can also reconstruct a document's probative value independently of the user. All evidence is based on cryptographic arguments. The chain of proof is consequently much stronger than it would be if the proper functioning of certified systems were to be taken as the sole foundation for a signature's authenticity.

### ArchiSoft as a mail server component

It also makes sense to use ArchiSoft for unsigned documents. ArchiSoft guarantees audit compliance without the need for special, expensive hardware. By integrating it in a mail server, you can make your mail archives audit-proof for only a modest investment.

### Time stamps protect signatures

ArchiSoft protects signatures by integrating time stamps. External time stamp servers are used by the system for this purpose. However, ArchiSoft does not procure a separate time stamp for each document – that would be totally inefficient – but rather builds a »tree« from a large number of documents, in which the root represents all documents. A time stamp is only required for the root, in other words for the complete document package. Since the root consists of a hash sum, the content of documents signed in this way is absolutely invisible to the operator of the time stamp server. The costs for the time stamp are thus also negligible. ArchiSoft accordingly authenticates the validity of digitally signed documents by extracting standardised evidence documents from the tree.

### Old signatures no longer considered secure

With effect from March 31, 2008, the validity of all signatures created with 1024 bit keys expired. This measure was announced by the German Federal Network Agency in an official publication.

Old signatures produced up until the end of 2007 using signature cards in conformity with the German Digital Signature Act are now considered to be »cryptographically faded«. The Signature Act, however, states that signatures must be renewed if they are to retain their probative value. ArchiSoft renews them for you – cheaply and efficiently. If you haven't already done so, you would be well advised to update your digital signatures with ArchiSoft at the earliest opportunity.

## SYSTEM REQUIREMENTS

**CPU:**
recommended Intel Core 2 Duo with 2.0 GHz

**Main memory:**
recommended at least 2 GB

**Hard disk:**
at least 110 MB for installation

**Operating systems:**
Windows Server 2008, Windows Server 2003, Windows XP Professional, Windows Vista, Linux, Solaris

Java Runtime Environment:

Java Runtime Environment (JRE) version 5 or 6 is required

**Databases:**
Microsoft SQL Server 2008, Microsoft SQL Server 2005, Microsoft SQL Server 2000, Oraces 9i, Oracle 10g, MySQL 5, PostgresSQL 8, in principle every database with JDBC interface

**Interfaces:**
Java API and web service interface to document management systems and archives respectively

**Timestamp services:**
RFC3161 (TSP) compliant timestamp services, optional authentification via HTTP(S) or CMS signature