



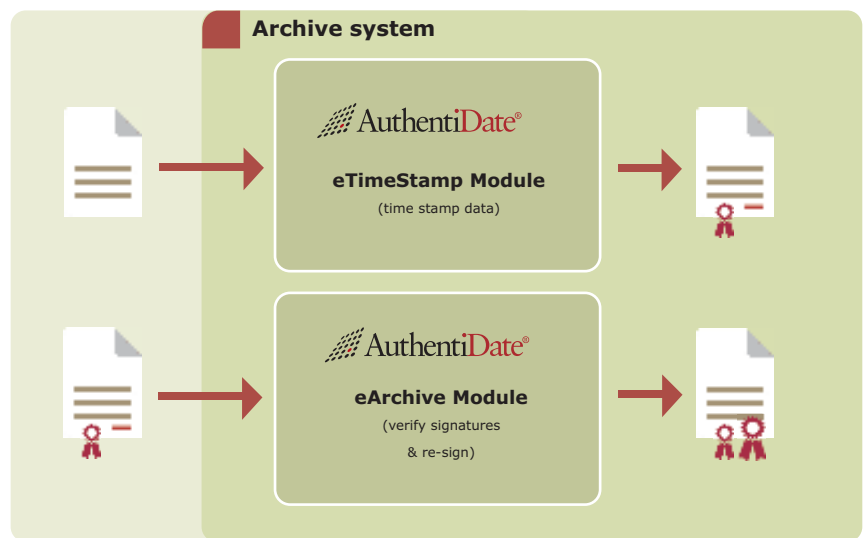
Legally binding long-term archiving

Signatures & time stamps for supplementing archive systems in accordance with the European ETSI standard

The business process

The archive system has a central role in many companies and authorities. Data must be stored safely for a long period and must be quickly retrievable at the same time. This is particularly necessary for data that has already been signed in other processes.

Qualified time stamps enable data to be archived in compliance with legal requirements for long periods in a legally secure manner. Retention periods of more than 30 years can also be replicated.



The implementation

AuthentiDate products supplement archive systems with various functions depending on the requirement.

■ Re-signing

Stored data in the archive system that has already been signed is re-signed here with a qualified time stamp. Re-signing with time stamps is mandatory by law if the algorithms become weak during signing. Without re-signing it would no longer be possible to guarantee that previously generated signatures are protected 100 percent against manipulation. The re-signing takes place automatically and transparently for the users.

■ Verifying

Signatures can be verified automatically in the archive system during the storage of the signed data. The result of the signature verification is stored automatically together with the signed data. Errors detected during the signature verification are reported immediately and automatically to ensure optimal quality of the archived data.

■ Documenting

All kinds of data can be signed with qualified time stamps automatically and centrally in the archive system. While doing so, you can define when and what data should be frozen by the time stamp. It is then safely protected against unnoticed manipulation. This process is also realizable for log files during SOX processes, for example.



Products for this solution

can be used individually or in combination

- eArchive Module
- eTimeStamp Module

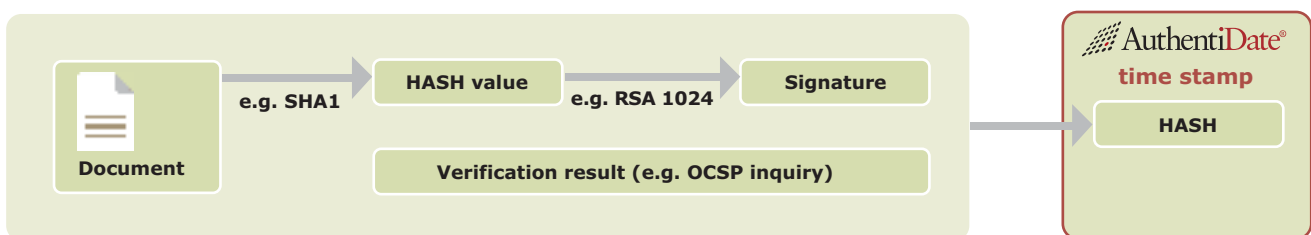


SOLUTION DESCRIPTION

Unlimited archive system functionality

by taking account of the European ETSI standard

Two different algorithms are always used for generating a signature. An algorithm is used for generating the hash value and another one is used for the encryption of the hash value. This produces the actual signature. AuthentiDate products have thus been designed in such a way that the signatures are automatically protected against one or both algorithms becoming weak during re-signing. Consequently, the archive system is only provided with one technical solution for all algorithm changes. This process was also defined in the European ETSI (European Telecommunication Standard Institute) TS 101 733 standard.



▪ Standard conformity

Through the application of the European ETSI standard, single files, including all associated elements (e.g. HASH values and signatures), can be deleted completely from the archives even after re-signing. Consequently, the archive system is not loaded by unnecessary data anymore. Each file is treated as an independent element. New files can be added and re-signed as well. The re-signed files can be verified at any time even without access to the archive system, e.g. by judges, auditors etc.

In addition to this, elements can be combined and thus the number of time stamps minimized, as defined in the ArchiSig concept, for example.

Profile

- ▶ **Automatic "re-signing" by a qualified time stamp as stipulated by law**
 - The use of legally compliant algorithms
 - Few time stamps are required owing to batch systems
- ▶ **AuthentiDate process takes account of the ArchiSig concept and the European ETSI (European Telecommunication Standard Institute) standard**
 - Extraction, complete deletion and addition of data even after re-signing
 - Re-signed data are added transparently to the existing archive structure
 - No additional expenditure if the HASH-algorithm becomes weak
- ▶ **Large-scale verification of personal signatures and/or time stamps in the archive**
- ▶ **Preinstalled and available on the current archive systems as standard**