

eArchive Module

contains certified signature appliance component SLMBC 3.0.20

Usage & field of application

The AuthentiDate eArchive Module enables legally compliant, large-scale verification of qualified signatures within Archive and Document Management Systems.

An essential feature here is conformity with the standards X.509v3 (qualified) and Common PKI 1.1 and 2.0. As a result of this, external signatures, i.e. signatures generated by third-party applications, can be verified with a high degree of security.

The eArchive Module has been specially developed for the purpose of integration into other software products. Owing to its service-oriented architecture (SOA) the module can be used easily and on the basis of all current program languages. The module integration is done using regular software development interfaces. Consequently, module functionality can be integrated into

existing software products with little effort and with the greatest possible flexibility in comparison with existing software architectures and base technologies.

The module also ensures secure and proper data processing even in the event of very high transaction volumes by means of a state machine-based job management system.

The eArchive Module is a software component that can be operated locally or on a separate computer system in the local network. It is based on the "AuthentiDate SLM Base Component" that complies with the Signature Law. The software was tested by an independent test center accredited to do so by the federal office for information security (BSI). An approval center authorised by the federal network agency then issued the appropriate certification in accordance with the signature act



(SigG). The requirements for qualified signatures stipulated for products by the German Signature Act are met accordingly.

Functional Description

The AuthentiDate eArchive Module is used for large-scale verification of qualified signatures in compliance with the requirements of the Signature Law - proven by a certification based on the German Signature Law.

Large-scale verification of qualified signatures takes place in configurable test depths. The result of the verification of a signature is returned to the invoking application as a so-called "Evidence Record" in the form of an XML document. After saving and archiving this XML document, signature verifications can be documented easily and in a form that is readable for a long period of time. All relevant certificates and verifications pertaining to the existence and lock status are provided upon request. These verifications and certificates can be used

for archiving. In the event of later re-verification, it is optionally possible to fall back on the archived verifications and certificates instead of retrieving this information again online. This aspect is particularly relevant in the long-term storage management of signed data.

Depending upon the selected test depth, the number of online directory service accesses required are also minimized by a caching mechanism. During caching, the eArchive Module tests whether any applicable status information is already available for the certificates that are to be verified. This normally increases the processing speed significantly during the verification of large volumes of signatures.

The requirement and verification of qualified time stamps is fully supported.

This includes the verification of separate time stamps as well as those embedded in signature containers as proof at the time of signature generation. In this way, the re-signing of signatures and thus the long-term validity of signatures is supported.

The implementation of a system for long-term storage of electronically signed documents in accordance with the internationally recognized ETSI-standard (ETSI TS 101 733) is possible, too. The eArchive Module can also verify signatures and timestamps of other electronic archiving systems which use for example ERS or ArchiSig to store long-term evidence records.

**Range of functions and services**

- ▶ Large-scale verification of qualified signatures in Archive- and Document Management Systems
- ▶ Support of qualified attribute certificates
- ▶ Support of qualified time stamps – separate and embedded in signatures
- ▶ Support of associated and integrated signatures (TIFFv6, PDF)
- ▶ Support of parallel and countersignatures
- ▶ Transaction security and data security by means of scalable job management (one state machine per job)
- ▶ Documentation of the test results via Evidence Records
- ▶ Variable configuration of the test depth in the verification process
- ▶ Product ist certified to comply with German Signature Law (SigG)

Standards and interfaces

- Signature Law:
SigG certification has been issued on 17.08.2009.
Manufacturer's declaration of the signature application components (SLMC) used was published by the Federal Network Agency in the Official Journal 02/2010 on Jan 27, 2010.
- Certificate format X.509v3 (qualified), Common PKI V. 1.1, V. 2.0
- Signature format Cryptographic Message Syntax (CMS), either as separate file or included in file (only TIFF, PDF)
- OSCP, LDAP, RFC3161
- Support of RSA 2048, SHA256, SHA-384 and SHA-512

System requirements

- Minimum hardware requirements: Intel Pentium processor 3.0GHz; min. 1GB RAM; 100 GB HD
- Operating systems: the module is platform independent from a technical point of view and runs in the Java Runtime Environment 1.4.2. Manufacturer's support is restricted to the following operating system platforms and versions :
 - Microsoft Windows XP, ServicePack 3 (SP3) or higher,
 - Microsoft Windows 2003 Server ServicePack 1 (SP1) or higher,
 - Red Hat Enterprise Server (kernel versions, 2.6.9 or higher),
 - Suse Enterprise Server (kernel versions, 2.6.9 or higher)
- Transparent network connection to the directory service and time stamp authority of the certification authority (OCSP, LDAP, RFC3161)

Delivery contents

- The software and documentation are delivered on CD or electronically by email/FTP.
- The license key is delivered electronically by email.

Related products

- Signature Check Server
- Signature Check Webservice
- eBilling Connector for SAP

* The certification requires specific hardware and software components. Details are available in the certification report.

V.008