

Scan Signature Module

contains certified signature appliance component SLMBC 3.0.20

Usage & field of application

The Scan Signature Module enables legally compliant, large-scale generation and verification of qualified electronic signatures in document recording (scan process).

Through the use of qualified electronic signatures it is possible to replicate paper documents and their digital images in scan processes subject to corresponding legal requirements. This replication offers scan solution providers an enhanced field of application in which legal security is required for scanned data.

The concept of the Scan Signature Module allows providers of scan solutions to integrate qualified electronic signatures into the existing software components at low cost and to preserve the existing processes and base technologies to the greatest possible extent. Additionally, existing customers can use the enhanced functionality through a migration to a new software release of the scan application without making extensive changes to the established processes.

The Scan Signature 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, the integration of module functionality into existing software products is possible with little effort and 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 case of very high transaction volumes by means of a state machine-based job management system.

The Scan Signature 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). Accordingly, the requirements for qualified signatures stipulated for products by the German Signature Act are met.

Functional description

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

Signature cards can be grouped so as to be client related or signature-purpose related. Signature cards are identified here with the aid of the certificate regardless of the chip card terminals connected and assigned to the configured groups. The number of chip card terminals and signature cards used is virtually only limited by the performance limits of the underlying system.

It is also possible to pre-configure the compulsory use of attribute certificates that can limit the signature value to the application case for documenting the change in media from paper to electronic format.

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 possible to fall back optionally 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 is also minimized by a caching mechanism. During caching, the Scan Signature Module tests whether any applicable status information is already available. This normally increases the processing speed significantly during the verification of large volumes of signatures.


Range of functions and services

- ▶ Large-scale generation of qualified and advanced signatures for the documentation of the change in media from paper to electronic format
- ▶ Large-scale verification of qualified and advanced signatures
- ▶ Client related or signature-purpose related grouping of signature cards
- ▶ Support of qualified attribute certificates
- ▶ 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)
- ▶ Chip card terminal-based dialog for the activation of signature cards
- ▶ Documentation of the test results via Evidence Records
- ▶ Variable configuration of the test depth in the verification process
- ▶ Batch-related archiving of signature cards according to technical BSI guideline (BSI-TR-03115)
- ▶ License-dependent transaction volumes per time interval
- ▶ 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)
- USB port for the connection of chip card terminals
- Signature cards compliant with Signature Law according to DIN-NI 17.4 and with support of the Open Card Framework (OCF)
- OCSP, 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 is only restricted to the following Windows and UNIX operating system platforms due to legal requirements:
 - Microsoft Windows XP, ServicePack 2 (SP2) 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)
- Interfaces: USB port per chip card terminal connected

- Chip card terminals: Reiner SCT, Cherry SmartBoard xx44, Smart Terminal ST-2xxx, SCM Microsystems
- SPR 532
Chip cards: versions of TeleSec signature cards PKS-Card, E4KeyCard, E4NetKeyCard and the D-Trust multcard, confirmed by the Signature Law
- Transparent network connection to the directory service 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.

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

V.009