

eSign Client Module

contains certified signature appliance component SLMBC 3.0.20

Usage & field of application

The eSign Client Module enables legally compliant generation and verification of qualified electronic signatures on any PC workstation.

Through the use of the AuthentiDate eSign Client Module, paper-based processes can be replicated electronically and still be legally binding. Consequently, costs can be reduced and approval and documentation processes accelerated.

By using qualified personal signatures with provider accreditation (based on a corresponding Smart Card) during the verification of the signature, it is possible to provide unequivocal and legally binding proof as to which person has signed a document. Since such signatures have to be verifiable for a period of 30 years due to legal regulations (Signature Law), such a process is also suitable for processes requiring long-term proof of approval.

The eSign Client 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 at any time by means of a state machine-based job management system. The eSign Client Module is a software component that can be operated on a PC workstation. 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 eSign Client Module is used for the generation and verification of qualified signatures on PC workstations in compliance with the requirements of the Signature Law - proven by a certification based on the German Signature Law.

The eSign Client Module is not a standalone software solution but a software component that enhances existing software products with functions for generating and verifying qualified signatures.

The eSign Client Module also allows parallel and countersignatures in order to meet the standard requirements of business processes. Parallel signing means that another person also signs data that has already been signed and thus an additional independent signature is connected with the data. Counter-signing means that another person countersigns the signature generated

previously and thus an additional, independent signature is connected with the data and the previous signature. Standard attribute certificates are also supported, e.g. for limiting the signature value.

The 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 is also minimized by a caching mechanism. During caching, the eSign client module tests whether any applicable status information is already available for the certificates that are to be verified. This normally increases processing speed significantly during the verification of large volumes of signatures.


Range of functions and services

- ▶ Generation of qualified signatures on PC workstations
- ▶ Verification of qualified signatures on PC workstations
- ▶ Support of qualified attribute certificates
- ▶ Support of qualified time stamps – 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)
- ▶ 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
- ▶ License-dependent transaction volumes per time interval, standard 250 signatures per day, 250 signature verifications per day, can be optionally extended
- ▶ 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 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)
- 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 content

- 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.008