

Signature Check Server

Version 2.8.0

Usage & field of application

The AuthentiDate Signature Check Server enables fully automatic, large-scale verification of qualified signatures of documents, invoices and all other electronically signed objects. The verification takes place in compliance with the legal requirements of the Signature Law, the current Sales Tax Law and EU Signature Directive.

Each recipient of electronically signed documents requires easily usable tools in order to verify signatures and thus the authenticity of the data. In the case of electronic invoices, the recipient, provided that he is entitled to deduct input tax, is even legally obliged to carry out signature verification (GDPdU). The verification in this case must be documented and archived by means of an electronic report (verification log).

Functional description

The AuthentiDate Signature Check Server is available as an automatic signature verification server for high data volumes or for individual requirements. The signature verification server is used for the integration of signature verifications in automated processes. The signature verification server uses the AuthentiDate Signature Check Webservice in the background. All configurations and processes relevant to signature verifications thus take place centrally, automatically and transparently.

The Signature Check Server is installed on a server and integrated into the respective IT environment via standard interfaces.

For integration via SMTP/Email the Signature Check Server has a standalone mail server component for centralized, large-scale processing of incoming emails that contain signed documents – e.g. electronic invoices – as an attachment. In this case, a signature verification

report is generated for documents and signatures that are attached to an email. This is added to the respective email as an additional attachment.

Configurable incoming and outgoing directory structures are used as interfaces for the file-based integration of the signature verification server. The files to be verified are placed in the respective incoming directories. These files plus a signature verification report are provided via corresponding outgoing directories. Aborted verifications are communicated via an error report and can be assigned via the file name of the respective signature, for example.

If integrated, signed PDF or PDF/A documents are verified, the verification reports can be attached as a separate file, or alternatively, can also be integrated directly into the verified, signed document i.e. attached to the original document. This simplifies the processing for the recipient because the original document, signature and

verification report are summarized in a PDF or PDF/A file.

The dynamic and modular architecture of the AuthentiDate Signature Check Server has very powerful internal process policies. These policies make it possible to replicate very different process, forwarding and processing constellations in an extremely flexible manner. Thus, for example, sender and recipient could be notified automatically in case a signature is incorrect. Similarly, powerful policies are provided for the email and file interface as well as for system and transaction events.

The verification of signatures and the corresponding signature algorithms are performed according the algorithm assessment guidelines defined by the German Network Agency (Bundesnetzagentur) in 2009. The assessment result is included in the verification reports.



**Range of functions and services**

- ▶ Verification of signatures generated by AuthentiDate signature components (verification of signatures of other providers on request)
- ▶ Signature algorithm assessment based on the German Network Agency specification from 2009
- ▶ Flexible connection to existing infrastructures via standard protocols (SMTP, NFS, FTP, SMB, WebDAV)
- ▶ Dedicated log file for the evaluation of invoice and transaction information
- ▶ Secure authentication of email servers sending e-mail to the signature verification server by means of SMTP-AUTH (SMTP-based connection)
- ▶ Policy-based processing of all kinds of documents and processing results for verification
- ▶ Secure transmission of data via STARTTLS/HTTPS
- ▶ Configurable signature verification levels
- ▶ High-performance signature verification through parallel processing
- ▶ Verification of
 - associated signatures (Common PKI)
 - integrated PDF signatures according to Adobe Reference Standard PDF Version 1.7.
 - integrated PDF/A signatures according to PDF/A Standard Version 1b
- ▶ Sample templates for verification reports in German, English and French. Additional languages are available on request
- ▶ Optional: Integration of virus/malware scanners when SMTP is used as supply source
- ▶ Optional: Integration of database systems for the storage of accounting and transaction information.
- ▶ Optional: Customization of the verification reports by means of templates
- ▶ A complete list of supported certificate issuers is available upon request.

Standards and interfaces

- Signature Application Component compliant with German Signature Law (SigG)
- SMTP, NFS, FTP, SMB, WebDAV
- SMTP-AUTH,
- Certificate format X.509v3 (qualified)
- Common PKI V. 1.1, V. 2.0

System requirements

- Minimum hardware requirements: Intel Xeon processor 2.0GHz; min. 512MB; 40GB HD
- Operating systems supported:
 - Red Hat Enterprise Linux Version 5
 - SuSE Linux Enterprise Server 10 and 11
- Software: Java Runtime Environment Version 1.6 (32 or 64 Bit)
- TCP/IP network connection depending on integration type
- Outgoing HTTPS connection to the Internet
- Access to AuthentiDate Signature Check Webservice (central signature verification)

Delivery content

- The software, license key and documentation are delivered by data carrier or electronically by email or FTP.
- Installation and setting up of the system, incl. the operating system, can only be carried out by AuthentiDate or by authorized partners.

Related products

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