Server.ID (TeleSec ServerPass)

1 INDRODUCTION

This document informs the user about the Server.ID (TeleSec ServerPass) service and, in addition to the Server.ID (TeleSec ServerPass) General Terms and Conditions, contains the obligations of the signatory.

By accepting this document, the signatory agrees to these terms and conditions of use.

2 PERFORMANCE COMPONETS

The standard Server.ID (TeleSec ServerPass) (incl. SAN/UCC (Multidomain)) variants meet the requirements of ETSI 319 411-1 policy OVCP.

All EV variants (EVCP) (incl. SAN (Multidomain)) meet the requirements of ETSI 319 411-1.

Server.ID EV (TeleSec ServerPass EV) (incl. SAN (Multidomain)) OCP-w also meet the requirements for qualified trust service providers (TSPs) or qualified trust services for website authentication in accordance with eIDAS Regulation (EU) No. 910/2014.

the eIDAS requirements for EU-qualified certificates and ETSI EN 319 411-2 policy QCP-w. ServerPass EV meets the requirements

The fulfillment of these requirements is certified annually by a DIN EN ISO/IEC 17065 accredited certification authority. In addition, an annual internal audit according to DIN EN ISO/IEC 19011 is carried out.

For all variants described here, the Certification Practice Statement (CPS Server.ID (TeleSec ServerPass)) apply.

2.1 Contact details

Address:

T-Systems International GmbH
represented by Deutsche Telekom Security GmbH
Trust Center & ID Security
Untere Industriestraße 20
57250 Netphen, Germany
Phone:

+49 1805 268 204 (landlines: EUR 0.14/minute, mobile networks: max. EUR 0.42/minute)

WWW: https://www.telesec.de

Email: telesec_support@t-systems.com

2.2 Accessibility of the revocation service (24/7)

WWW: https://serverpass.telesec.de/serverpass/ts/ee/login/displayLogin.html

Selectable revocation codes are:

- Not specified
- Key compromised
- Information in the certificate is out of date or incorrect
- Certificate is no longer required
- Cessation of operation

Server.ID (TeleSec ServerPass)

- Rights have been withdrawn (right to use the domain name expired)

Phone:

+49 1805 268 204 (landlines: EUR 0.14/minute, mobile networks: max. EUR 0.42/minute)

2.3 Accessibility of other services

- As a monthly average, the service portal and web server are available 98.0 percent of the time.
- As a monthly average, the LDAP directory service (CRL, ARL) is available at 98.0 percent of the time.
- As a monthly average, the online validation service (OCSP) is available 98.0 percent of the time.
- As a monthly average the email server is available 98.0 percent of the time.

2.4 Log events

Which data and events are recorded by whom and at which intervals is defined in the logging concept. In addition, rules are laid down that govern how long the log data is stored (currently for six weeks) and how it is protected against loss and unauthorized access. The requirements under ETSI EN 319 401 are implemented as part of this process.

2.5 Retention period for archived data

The following records and storage periods are stipulated:

- order documents, in particular information regarding certificate requests, their validation and the certificates resulting from this and revocations executed are retained for seven years after the certificate validity expires,
- in the case of Server.ID EV / EV SAN with QWAC (TeleSec ServerPass EV / EV SAN with QWAC) until the end of operation,
- audit and event logging data is archived in accordance with the current legal provisions.

2.6 Provisions for settling disputes

In the event of disputes, the parties shall come to an agreement taking into account any applicable laws, regulations, and agreements made.

Server.ID (TeleSec ServerPass)

3 OBLIGATIONS

The signatory (the customer, the certificate holder, or the authorized person) who applies for, manages, or operates one or more certificates for an end user or device undertakes:

- To provide proof, if required, that they may commission certificate requests on behalf of the customer (legal person).
- To provide proof of ownership or control of the domain(s) from the certificate request.
- To provide complete and correct information in the certificate request.
- To verify immediately after issuance that the certificate content matches the underlying order data.
- To use the issued certificate exclusively for its intended purpose and for authorized and legal purposes.
- Not to misuse the certificate and not to contradict the regulations the Certification Practice Statement (CPS) of the Server.ID (TeleSec ServerPass) service.
- To bear the legal consequences arising from non-fulfillment of the obligations described in the aforementioned CPS and to observe the specifications on the subject of certificate revocation.
- To use the keys and certificates only in the permitted applications. The application must comply with the key usages entered in the certificate.
- Not to use the certificate with applications or machines whose functions seem to be unknown, suspicious, or unreliable.
- To protect their private key appropriately and against unauthorized access by third parties.
- To genuinely act as the end user and not to perform any CA functions with their private key, such as signing certificates or revocation lists.
- Immediately revoke the end-user certificate in question or to have it revoked if the private key is lost, or if it is presumed to have been compromised or manipulated, if significant changes have been made to the details of the certificate, if its use has been discontinued, or in the case of presumed misuse.
- To cease immediately and permanently from using the private key if this key has been compromised.
- To stop using the certificate if it becomes known that the certificate of the certification authority has been compromised.

The current Certification Practice Statement (CPS) of the Server.ID (TeleSec ServerPass) service, along with previous versions of this document, are stored publicly at:

https://www.telesec.de/de/service/downloads/pki-repository/

4 RECOMMENDATION TO RELYING PARTIES

Relying parties must have sufficient information and knowledge to be able to evaluate the handling of certificates and their validation. The relying party is responsible for its own decisions regarding whether the information provided is reliable and trustworthy.

Every relying party should

- check that the information contained in the certificate is correct before using it;
- check that the certificate is valid by validating the entire certificate chain as far as the root certificate (certificate hierarchy) and checking the validity period and revocation information (CRLs or OCSP) of the certificate, amongst other things;
- use the certificate for authorized and legal purposes only in accordance with this CPS. T-Systems is not responsible for assessing the suitability of a certificate for a specific purpose;
- check the intended technical purposes, which are defined via the attributes "key usage" and "extended key usage" indicated in the certificate.

Relying parties must use appropriate software and/or hardware to check certificates (validation) and the associated cryptographic procedures.