Efficient management and issuance of digital certificates

Certificate Service Manager (CSM) – managed PKI platform

Advantages at a glance

1. Fast – certificates made available in a matter of seconds
2. Central – certificate stock managed at the company
3. Flexible – assignment of finely graded user authorizations
4. Automated – seamless integration into existing workflows thanks to an API interface

Certificates have become a natural part of digital processes at companies and on the Internet

They can be used in a vast range of ways, such as to exchange data securely on the Internet using data encryption, to warrant the identity of communication partners and to digitally sign files or e-mails. Companies that use various certificates need a fast request process to enable them to act quickly and to manage certificates in a clear-cut manner. D-TRUST's Certificate Service Manager (CSM) is a Web-based managed PKI solution for managing and requesting certificates and for user administration. You can manage everything on a single platform. This reduces the cost and time needed to manage a company's many digital certificates. Following initial verification, high-quality certificate products will be made available in a matter of seconds in an automated process. This means that you can control your organization's certificates at all times.

The solution and its components

Central management mechanisms

The CSM, a Web-based certificate management platform, is used to process certificate requests and to manage verification data and certificates via one account. Access to the Web portal is secured by an SSL and smart card certificate. This ensures maximum security. One or more authorised persons ('operators') within the company have access to this account. They are responsible for the data stored there as well as for the final release of certificate requests. The advantage of this is that all activities are managed from one account and centrally monitored. Any number of organisations can be created for each account. This is ideal for large companies who have to manage certificates for many sub-organisations. Depending on the organizational structure, different levels of user authorization can be assigned to the account and the organizations.

Immediate issuance of very different types of certificates

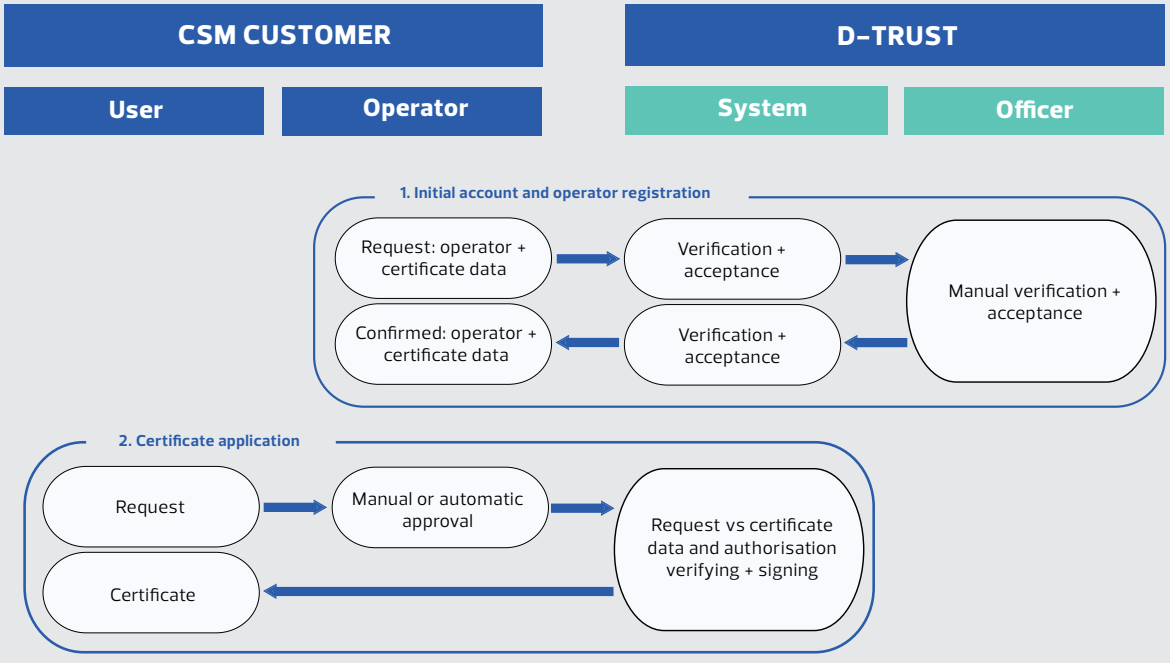
Using the CSM, all request and verification data for all certificates required in the future can already be sent before the actual request is made. The required verification and the purchase process take place in advance. This means direct access is available to many different types of certificates:

The Certificate Service Manager (CSM) is a managed PKI service for organisations that apply for multiple certificates annually.

- SSL/TLS certificates according to the Organisation Validation (OV) or Extended Validation (EV) standard
- DV SSL products
- Qualified website certificates according to the eIDAS Regulation
- S/MIME certificates for digital signing and encryption of e-mails and for authenticating users and devices in networks
- Machine certificates for securing communication between machines or objects with organisational affiliation
- personal certificates, which are issued in accordance with the technical guideline TR-03145 certified by the Federal Office for Security and Information Technology (BSI). A solution for companies, authorities and classified institutions "classified information – for official use only" (VS-NfD).

All that is needed to apply for a certificate on the basis of the data pre-checked by the TSP is request data, such as the company name or domain name. Depending on how the operator has configured the account, the certificate can also be created in an automated process and then billed later on an invoice.

CERTIFICATE SERVICE MANAGER (CSM)



Ver. 11/2020