PRODUCT SHEET

# Managing and issuing digital certificates efficiently

## Certificate Service Manager (CSM) Managed PKI Platform

### Advantages at a glance

01
**Fast**
certificates made available in a matter of seconds

02
**Central**
certificate stock managed at the company

03
**Flexible**
assignment of finely graded user authorizations

04
**Automated**
seamless integration into existing workflows thanks to an API interface

### Certificates have become a integral part of digital processes for companies and on the Internet

They can be used in a wide 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. Manage everything using a single platform - this reduces effort, costs and time associated with managing multiple digital certificates throughout the company. After an initial check, certificates are automatically available within a few seconds. This gives you 24/7 control over the number of certificates within your organisation.

Part of Bundesdruckerei group

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

## Central management

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 two-factor authentication. This ensures maximum security. One or more authorised persons ('operators') within the organisation 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 that 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 Organization.

**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:

- 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).

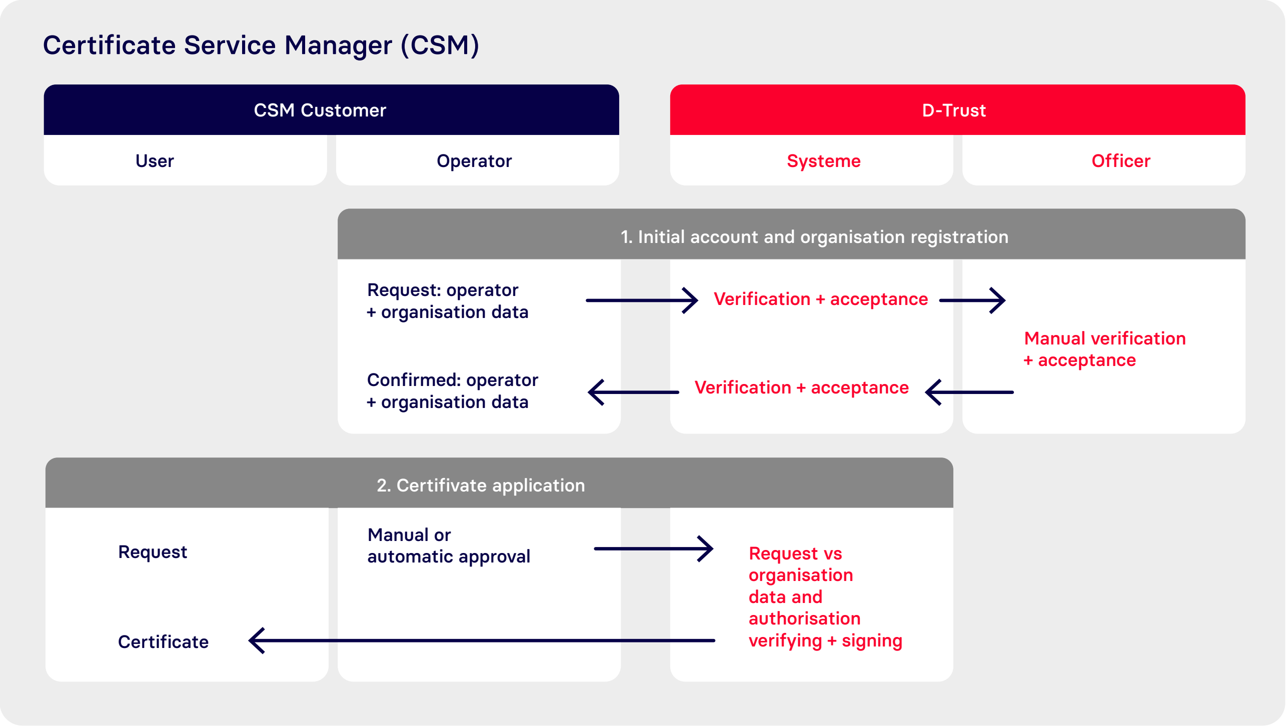
For the certificate application, no further information is required other than request data such as the name of the company or domain name. Certificate creation can also be fully automated. Invoicing then takes place afterwards by invoice.

## Automation through the combination of CSM and CLM

**What is CLM?**

CLM (Certificate Lifecycle Management) ensures the efficient and error-free management of certificates over the entire lifecycle. This also includes the automatic distribution and renewal of expiring certificates. As a managed PKI solution, the Certificate Service Manager (CSM) provides the basis for requesting digital certificates, for status queries and revocation.

Important: Automation strengthens IT security, optimize processes and ensure long-term compliance and and availability. This applies in particular to new framework conditions such as shorter certificate validity periods and crypto agility.



Certificate Service Manager (CSM)

CSM Customer
User
Operator
D-Trust
Systeme
Officer
1. Initial account and organisation registration
Request: operator + organisation data
Verification + acceptance
Manual verification + acceptance
Verification + acceptance
Confirmed: operator + organisation data
2. Certifivate application
Request
Manual or automatic approval
Request vs organisation data and authorisation verifying + signing
Certificate