

Digitale Zertifikate effizient verwalten und ausstellen

Certificate Service Manager (CSM) – Managed-PKI-Plattform



Ihre Vorteile

01

Schnell

Bereitstellung der
Zertifikate innerhalb
weniger Sekunden

02

Zentral

Verwaltung des
Zertifikatsbestands
im Unternehmen

03

Flexibel

Vergabe von fein
abgestuften Benutzer-
berechtigungen

04

Automatisiert

Nahtlose Integration
in bestehende
Workflows durch
API-Schnittstelle

Zertifikate sind aus den digitalen Prozessen von Unternehmen sowie aus dem Internet nicht mehr wegzudenken

Die Bandbreite ihrer Einsatzmöglichkeiten ist umfangreich. Sie werden z. B. genutzt, um den Austausch von Informationen über das Internet per Datenverschlüsselung abzusichern, die Identität von Kommunikationspartnern zu gewährleisten und Dateien oder E-Mails digital zu signieren. Unternehmen, die diverse Zertifikate in ihrer Organisation nutzen, stehen vor der Herausforderung, durch einen schnellen Beantragungsprozess agil zu handeln und Zertifikate übersichtlich zu verwalten.

Der Certificate Service Manager (CSM) der D-Trust ist eine webbasierte Managed-PKI-Lösung zur Verwaltung, Beantragung und Benutzeradministration von Zertifikaten. Managen Sie alles über eine einzige Plattform – das reduziert Aufwand, Kosten und Zeit, die mit der Verwaltung von vielen digitalen Zertifikaten im Unternehmen verbunden sind. Nach initialer Prüfung stehen hochwertige Zertifikatsprodukte innerhalb weniger Sekunden automatisiert zur Verfügung. So haben Sie 24/7 die Kontrolle über den Zertifikatsbestand innerhalb Ihrer Organisation.

Der Certificate Service Manager (CSM) ist ein Managed-PKI-Service für Organisationen, die jährlich mehrfach Zertifikate beantragen.

Die Lösung und ihre Bestandteile

Zentrale Verwaltungsmechanismen

Der CSM als webbasierte Zertifikatsmanagement-Plattform dient der Bearbeitung von Zertifikatsanfragen sowie der Verwaltung von Prüfdaten und Zertifikaten über ein Konto. Der Zugang zum Webportal wird mittels SSL- und Smartcard-Zertifikat gesichert. Das sorgt für maximale Sicherheit. Eine oder mehrere autorisierte Personen („Operatoren“) innerhalb des Unternehmens haben Zugriff auf dieses Konto. Sie sind verantwortlich für die dort hinterlegten Daten sowie die endgültige Freigabe von Zertifikatsanfragen. Der Vorteil: Alle Aktivitäten werden von einem Account verwaltet und zentral überwacht. Je Konto können beliebig viele Organisationen angelegt werden. Dies ist ideal für Großunternehmen, die Zertifikate für viele Unterorganisationen verwalten müssen. Entsprechend der Organisationsstruktur können verschiedene abgestufte Benutzerberechtigungen für das Konto und die Organisationen vergeben werden.

Sofortiges Ausstellen von unterschiedlichsten Zertifikatstypen

Mithilfe des CSM lassen sich sämtliche Auftrags- und Prüfdaten für alle zukünftig benötigten Zertifikate bereits vor dem Zeitpunkt der eigentlichen Beantragung übermitteln. Erforderliche Überprüfungen und der Einkaufsprozess finden im Vorfeld statt.

Dadurch besteht direkter Zugriff auf die unterschiedlichsten Zertifikatstypen:

- SSL/TLS-Zertifikate nach dem Standard „Organization Validation (OV)“ oder „Extended Validation (EV)“
- DV SSL Produkte
- Qualifizierte Websitezertifikate nach der eIDAS-Verordnung
- S/MIME-Zertifikate für digitales Signieren und Verschlüsseln von E-Mails und für die Authentifizierung von Benutzern und Geräten in Netzwerken
- Maschinenzertifikate für die Absicherung der Kommunikation von Maschinen oder Objekten mit Organisationszugehörigkeit
- Personenzertifikate die nach der technischen Richtlinie TR-03145 des Bundesamts für Sicherheit und Informationstechnik (BSI) zertifiziert sind. Eine Lösung für Unternehmen, Behörden und Institutionen mit Geheimhaltungsstufe „Verschlussache – Nur für Dienstgebrauch“ (VS-NfD)

Zur Zertifikatsbeantragung werden nur noch Requestdaten wie Name des Unternehmens oder Domainname benötigt. Die Zertifikatserstellung kann auch vollständig automatisiert werden. Die Abrechnung erfolgt dann bequem im Nachgang per Rechnung.

