PRODUKTBLATT

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 Nutzungs-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 und -partnerinnen 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 Nutzendenadministration 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.

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 Zwei-Faktor-Authentifizierung gesichert. Das sorgt für maximale Sicherheit. Eine oder mehrere autorisierte Personen („Operatoren") innerhalb der Organisation 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:

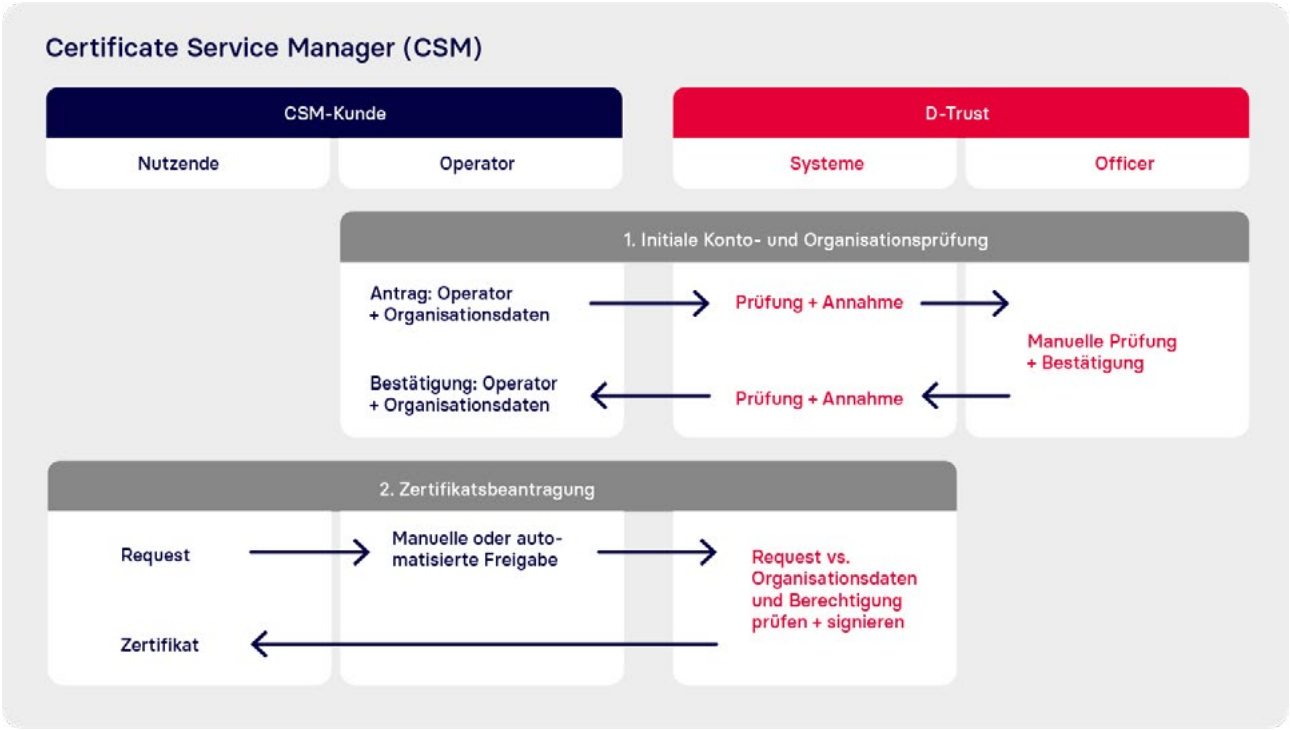
- TLS-Zertifikate nach dem Standard „Organization Validation (OV)" oder „Extended Validation (EV)"
- DV-SSL-Produkte
- Qualifizierte Website-Zertifikate nach der eIDAS-Verordnung
- S/MIME-Zertifikate für digitales Signieren und Verschlüsseln von E-Mails und für die Authentifizierung von Nutzenden und 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 in der Informationstechnik (BSI) zertifiziert sind. Eine Lösung für Unternehmen, Behörden und Institutionen mit Geheimhaltungsstufe „Verschlusssache – Nur für Dienstgebrauch" (VS-NfD).

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

Automatisierung durch die Kombination aus CSM und CLM

Was ist ein CLM?
Das CLM (Certificate Lifecycle Management) sorgt für die effiziente und fehlerfreie Verwaltung von Zertifikaten über den gesamten Lebenszyklus. Dazu gehört auch die automatische Verteilung und das Erneuern ablaufender Zertifikate.
Der Certificate Service Manager (CSM) stellt als Managed-PKI-Lösung die Grundlage zur Beantragung digitaler Zertifikate, für Statusabfragen und zur Sperrung bereit.
Alternativ zu einem CLM kann der Bezug von TLS-Zertifikaten für Server auch über das vom CSM unterstützte Protokoll ACME automatisiert werden.

Wichtig: Durch Automatisierung stärken Sie die IT-Sicherheit, optimieren Prozesse und gewährleisten langfristige Compliance und Verfügbarkeit. Dies gilt insbesondere für neue Rahmenbedingungen wie kürzere Zertifikatslaufzeiten und Kryptoagilität.



D-Trust GmbH | Kommandantenstraße 15 | 10969 Berlin | Germany
Tel.: +49 (0)30 25 93 91-0 | info@d-trust.net | www.d-trust.net