

PRODUKTVERGLEICH

Elektronische Siegel in der Anwendung

Fernsiegeldienst seal-me, Siegelkarten und Qualified Seal ID

Elektronische Siegel sichern Herkunft und Integrität von Daten

Die eIDAS-Verordnung regelt europaweit den Einsatz von Vertrauensdiensten, darunter den von elektronischen Siegeln. Jene Siegel entsprechen den Firmenstempeln und Behördensiegeln in der analogen Welt.

Technisch gewährleisten sie die Herkunft und Integrität von digitalen Dokumenten. Für jeden Empfänger eines elektronisch gesiegelten Dokuments ist z.B. über kostenfrei verfügbare PDF-Reader jederzeit prüfbar, auf welche Organisation ein Vertrauensdiensteanbieter (VDA) wie D-Trust das Zertifikat ausgestellt hat. Zudem lassen sich Manipulationen an Dokumenten schnell erkennen.

In der Praxis bedeutet das für den Nutzer ein rechtssicheres und medienbruchfreies Siegel von Dokumenten. Bei allen durch D-Trust angebotenen Siegeln, also beim Fernsiegeldienst seal-me, den Siegelkarten und auch bei der Qualified Seal ID, kommen qualifizierte Zertifikate zum Einsatz, die über die EU Trusted List prüfbar sind.

Siegelkarten

Siegelkarten gelten als sichere Siegelerstellungseinheit für qualifizierte Siegel im Sinne der europäischen eIDAS-Verordnung. Das Siegel wird hier mit dem privaten Schlüssel auf einer Siegelkarte berechnet – in Kombination mit einem Lesegerät, einer Siegelsoftware und der Siegel-PIN.

Qualified Seal ID

Die Qualified Seal ID wird als nach eIDAS qualifiziertes Zertifikat ebenfalls durch den Vertrauensdiensteanbieter ausgestellt. Siegelzertifikat und Schlüssel werden als Softtoken auf einem von der Organisation selbst gewählten Schlüsselspeicher oder in einer sicheren Serverumgebung abgelegt und genutzt.

Fernsiegeldienst seal-me

Das jüngste Produkt aus der D-Trust Siegelfamilie ermöglicht das qualifizierte elektronische Siegeln ohne zusätzliche Komponenten, also fernausgelöst. Das Siegel wird in diesem Fall mit dem privaten Schlüssel auf einer sicheren Hardwareeinheit (HSM) im D-Trust Rechenzentrum ausgelöst. Als zweiter Faktor dient eine Kombination mit dem Softtoken der Qualified Seal ID.

Unterscheidung

Die jeweilige Speicherung und Verwendung des privaten Siegelschlüssels bewirkt, dass über Siegelkarten und den Fernsiegeldienst seal-me der D-Trust qualifizierte elektronische Siegel erzeugt werden. Über eine Qualified Seal ID werden fortgeschrittene elektronische Siegel auf Basis von qualifizierten Zertifikaten erstellt.

Unabhängig vom gewählten Siegelverfahren gilt:

- **Schutz von Integrität und Authentizität:**

Technische Schutzmaßnahmen auf hohem Niveau sorgen dafür, dass elektronische Dokumente manipulationssicher sind und die siegelnde Organisation stets eindeutig identifizierbar ist.

- **Rechtssicherheit:**

Die eIDAS-Verordnung verleiht den elektronischen Dokumenten vor Gericht einen starken Beweiswert – und das im gesamten europäischen Raum.

| Produkte im Vergleich | Fernsiegeldienst seal-me | Siegelkarten | Qualified Seal ID |
|-----------------------------------|--|--|---|
| eIDAS-Bezeichnung | Qualifizierte elektronisches Siegel nach eIDAS | Qualifizierte elektronische Siegel nach eIDAS | Fortgeschrittene elektronische Siegel auf Basis eines qualifizierten Zertifikats nach eIDAS |
| Preismodell | Jährliche Zertifikatskosten und transaktionsabhängige Pakete | Einmaliger Kartenpreis (Gültigkeit 3 Jahre) | Jährliche Zertifikatskosten |
| Antragsverfahren | Zur Bestellung stellt Ihnen unser Vertrieb gerne die Unterlagen zur Verfügung (vertrieb@d-trust.net) | Bestellung über das D-Trust-Portal (vereinfachte und individuelle Antragsverfahren für Behörden/Unternehmen möglich) | Bestellung über den Certificate Service Manager (CSM) oder Partner |
| Lieferung | Freischaltung der Zertifikate auf dem HSM bei D-Trust & Anbindung im eigenen Fachverfahren | Lieferung der Karte per Einschreiben | Lieferung eines Softtokens oder Zertifikats |
| Zusatzkomponenten | Workflowkomponente oder Fachverfahren mit Möglichkeit zur API-Anbindung | Kartenlesegerät und Siegelsoftware notwendig | Keine zusätzliche Hardware notwendig |
| Speicherort des Schlüssels | Schlüsselspeicher im D-Trust Rechenzentrum | Schlüsselspeicherung auf der Siegelkarte (sicherer Speicherort) | Softtoken, Schlüsselspeicherung von der Organisation gewählt |
| Sicherheit | 2-Faktor- Authentifizierung (Account & Qualified Seal ID) | 2-Faktor-Authentifizierung (Karte und PIN) | Passwort bei Softtoken |
| Verfügbarkeit | Nutzung nur online möglich, Einbindung in virtualisierte Umgebung möglich | Nutzung offline möglich | Nutzung offline möglich, Einbindung in virtualisierte Umgebung möglich |

Anwendungsbereiche

Das elektronische Siegel schließt eine Lücke in der digitalen Kommunikation. Es überführt Behördensiegel und Unternehmensstempel rechtsverbindlich und europaweit anerkannt ins digitale Zeitalter.

Es gibt dabei Fälle, in denen ein qualifiziertes Siegel vom Gesetzgeber oder von anderen Instanzen gefordert ist. Zu diesen Fällen zählt auf EU-Ebene die Anwendung der Produktdatenbank zu Energielabeln (EPREL). Auf nationaler Ebene sind qualifizierte Verfahren im Bereich der elektronischen Vergabeverfahren oder beim ersetzenden Scannen (TR-RESISCAN) gefordert.

Sobald Unternehmen in einem dieser Bereiche ihre digitalen Unterlagen siegeln, muss beachtet werden, dass ein qualifiziertes Siegel nach eIDAS-Verordnung zum Einsatz kommt.

Fazit

Egal ob fernausgelöst mit Siegelkarte oder Qualified Seal ID – wichtig bleibt für jedes Siegel, dass damit ein einfacher Weg zur Absicherung von elektronisch versandten Dokumenten zur Verfügung steht. Elektronische Siegel verhindern für alle Nutzer sichtbar Manipulationen am Dokument und identifizieren die siegelnde Organisation eindeutig.