

THEMENBLATT Vertrauensdienste

procilon Lösungen für eIDAS-Vertrauensdiensteanbieter



- ✓ Konformität entsprechend der Spezifikationen der eIDAS-Verordnung
- ✓ Vollständige Public Key Infrastructure
- ✓ Nach Common Criteria EAL 4 + evaluiert
- ✓ Minimierung von Sicherheitsrisiken

EU-Vertrauenssiegel für qualifizierte Vertrauensdiensteanbieter

Die Herausforderung

Digitale Transformation aktiv gestalten

Digitale Transformationen lösen herkömmliche Verwaltungs- und Geschäftsprozesse ab. Mit eIDAS stellt die europäische Gesetzgebung sicher, dass die genutzten Werkzeuge und Lösungen die notwendige Vertrauenswürdigkeit, Nachvollziehbarkeit und Beweissicherheit haben werden. Damit wird ein erheblicher Beitrag zur Standardisierung der Informationssicherheit bei digitalen Transformationen geleistet. Es bietet sich die Chance, Vertrauen und Transparenz in täglichen, IT- unterstützten Arbeitsabläufen herzustellen. Nur das wird Akzeptanz bei Nutzern finden.

Standardisierung in EU-Binnenmarkt

Laut der eIDAS-Verordnung sind „Vertrauensdiensteanbieter von Diensten zur Erstellung, Überprüfung und Validierung von elektronischen Signaturen, elektronischen Siegeln oder elektronischen Zeitstempeln und die Bewahrung von, diese Dienste betreffenden, elektronischen Signaturen, Siegeln oder Zertifikaten.“ Darüber hinaus zählen die Zustellung elektronischer Einschreiben sowie die Erstellung, Überprüfung und Validierung von Zertifikaten für die Website-Authentifizierung dazu.



eIDAS Regelungen/Anwendungsfälle

Identitäten	Zertifikate
	elektronische Ausweise
Vertrauensdienste	elektronische Siegel
	elektronische Zeitstempel
	Website-Authentifizierung
	elektronische Zustelldienste
	Bewahrungsdienste

Mindestmaß an Informationssicherheit

Für Anbieter von Vertrauensdiensten ist es wichtig, ein Mindestmaß an Informationssicherheit einzuhalten. Grundsätzlich lassen sich die angebotenen Dienste in drei Gruppen zusammenfassen:

- Vertrauensdienste ohne Akkreditierung (nicht qualifizierte Vertrauensdienste)
- Vertrauensdienste mit Akkreditierung (qualifizierte Vertrauensdienste)
- Vertrauensdienste innerh. geschlossener Systeme

Vertrauensdienste innerhalb geschlossener Systeme werden von der Gesetzgebung nicht weiter berührt und unterliegen eigenen Compliance-Anforderungen. Die erstgenannten beiden Formen bieten Vertrauensdienstleistungen gegenüber Dritten auf dem Markt an, deshalb sind sie dazu verpflichtet, technische und organisatorische Maßnahmen zur Minimierung von Sicherheitsrisiken zu ergreifen.

Besondere Maßnahmen für qualifizierte Anbieter

Für Anbieter qualifizierter Vertrauensdienste bestehen komplexe Sicherheitsanforderungen. So ist die Erbringung qualifizierter Vertrauensdienste der jeweiligen nationalen Aufsichtsbehörde mitzuteilen und deren Konformität von einem akkreditierten Prüfer bestätigen zu lassen. Beispielsweise definieren die Mitglieds-

THEMENBLATT Vertrauensdienste

procilon Lösungen für eIDAS-Vertrauensdiensteanbieter

staaten gemeinsam kryptographische Algorithmen und Schlüssellängen. Die nationalen Aufsichtsbehörden überprüfen deren Konformität. Für Vertrauensdiensteanbieter ist daher der Einsatz von bereits auf hohem Niveau geprüfter Produkte für ihre Dienste empfehlenswert. Damit wird die Grundlage für ihr Informationssicherheitskonzept gelegt.

Die Lösung

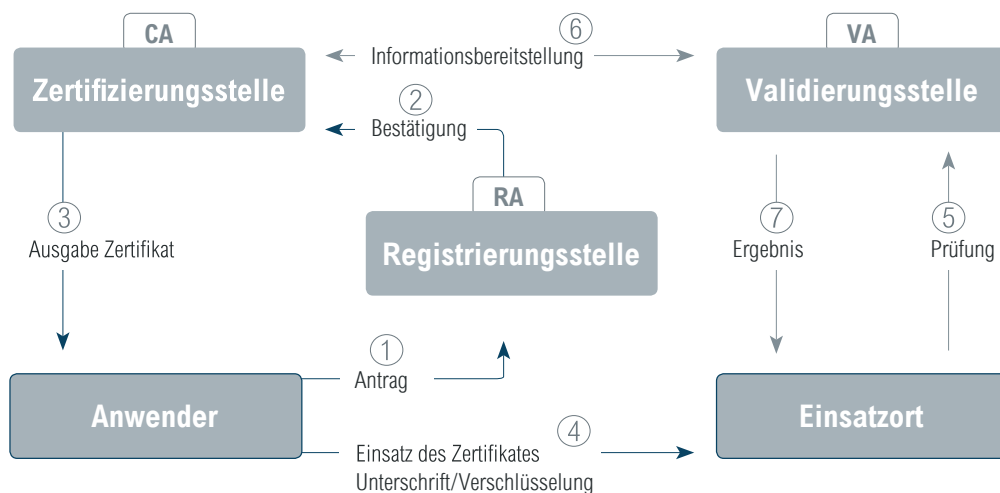
Komplexe Anforderungen benötigen standardisierte sowie zertifizierte Lösungen. Mit Produkten der proNEXT Familie ist procilon in der Lage, dies mit optimal aufeinander abgestimmten Einzelkomponenten zu realisieren. Die Einsatzmöglichkeiten reichen

Zur Integration wird eine REST-Schnittstelle (API) zur Verfügung gestellt, die anderen Applikationen erlauben, die gewünschten Funktionen aufzurufen.

proNEXT Security Manager bietet eine zentrale Identitätsverwaltung für alle Zugänge, Ressourcen und Repositories.

Mit der proNEXT Suite liefert procilon eine modulare Sicherheitssoftware, welche verschiedene Aufgaben rund um sichere elektronische Kommunikation, Identitäten und PKI abbildet. Die Architektur aller Lösungsbausteine ist eine Java Enterprise Anwendung auf einem gehärteten Linux System.

Der proNEXT Archive Manager ist ein beweiswerterhaltendes IT-System für archivierte Dokumente mit qualifizierter Signatur und ermöglicht die rechtskonforme Langzeitarchivierung nach



dabei von der Signaturanwendung über Authentisierungsprozesse bis zur schnellen Erzeugung von Zertifikaten. Insbesondere für eIDAS-Szenarien wie elektronische Ausweise, qualifizierte Signaturen, Siegel und Zeitstempel, aber auch für Website-Authentifizierung und Bewahrungsdienste stellt procilon optimale Lösungen bereit.

Alle Produkte sind nach Common Criteria in der Prüfstufe EAL 4+ mit AVA VAN.5 (vollständige Missbrauchsanalyse und hohes Angriffspotential) auditiert und zertifiziert. Bestandteil der Prüfung ist ein Integritätsschutz-Mechanismus, der die jeweilige proNEXT-Installation vor unbemerkten Manipulationen schützt. proNEXT Secure Framework ist eine vollständige Signaturanwendungskomponente zur Erstellung und Prüfung elektronischer Signaturen und ist konform zu den technischen Spezifikationen der eIDAS-Verordnung. Es besitzt keine eigene Benutzeroberfläche (User Frontend), sondern ist als Integrationskomponente für Fachapplikationen konzipiert. Damit kann der Anwender die Signaturfunktionalitäten aus seinem Arbeitsumfeld heraus nutzen.

technischer Richtlinie des BSI-TR 03125. Das Produkt ist dem entsprechend BSI-zertifiziert. Die Komponente BNotK TrustCenter 2.0 ist eine PKI-Lösung mit den Subsystemen CA, OCSP, CRL und TSS zur Erstellung qualifizierter Zertifikate und Zeitstempel.

Kontakt

procilon GROUP
Leipziger Straße 110
04425 Taucha
+49 34298 48 78-31
anfrage@procilon.de
www.procilon.de

