DATENBLATT **proNEXT Secure Framework 2.0**

Signaturanwendungskomponente

- ✓ Erstellung qualifizierter oder fortgeschrittener Signaturen für Einzeldokumente oder Dokumentenstapel
- ✓ Erzeugung einer qualifizierten elektronischen Signatur mit einer sicheren Signaturerstellungseinheit (SSEE)
- ✓ Prüfung von elektronischen Zertifikaten, Signaturen, Zeitstempeln und Evidence Records
- ✓ Integration in Fachapplikationen über REST Schnittstelle (API)
- ✓ Prüfung von zu signierenden Dokumenten auf aktive oder versteckte Inhalte

Standardisierte Sicherheit von Anfang an

Das proNEXT Secure Framework ist eine vollständige Signaturanwendungskomponente zur Erstellung und Prüfung elektronischer Signaturen. Neben der marktüblichen Herstellererklärung gegenüber der Bundesnetzagentur, welche die Einhaltung der Anforderungen des Signaturgesetzes (SigG) und der Signaturverordnung (SigV) bestätigt, ist das procilon Produkt nach Common Criteria in der Prüfstufe EAL 4+ mit AVA VAN.5 (vollständige Missbrauchsanalyse und hohes Angriffspotential) durch den TÜV-IT auditiert und zertifiziert.

Das proNEXT Secure Framework ist in der Lage, in Übereinstimmung mit den Festlegungen der eIDAS-Verordnung alle Zertifikate der EU Trusted Lists of Certification Service Providers (TSL) zu prüfen.
Die verwendeten Algorithmen zur Signaturerstellung und -prüfung werden zur Sicherung deren Aktualität stetig mit dem Algorithmenkatalog des BSI abgeglichen. Ein Integritätsschutz-Mechanismus ermöglicht die Konsistenzprüfung der proNEXT Secure Framework Installation und schützt so vor Manipulation.
Anwender der Komponente können einzelne oder mehrere Dokumente einer Signaturkarte zuführen, welche die kryptografischen Operationen zur Signaturerstellung ausführt. Es können Dokumente in verschiedenen elektronischen Formaten im Single- oder Batch-Modus verarbeitet werden.
Das proNEXT Secure Framework besteht aus den Komponenten Management Subsystem (MS) als zentraler Dienst und dem Operations Subsystem (OS) als Client-Komponente. Das OS wird zur Generierung von Hash-Werten, zur Prüfung von Dokumenten und zur Kommunikation mit Smartcards verwendet.
Das MS wird als Dienst, z.B. aus einem zentralen Rechenzentrum bereit gestellt. Hier werden Zertifikatsinformationen gesammelt, Prüfberichte erstellt und Audit-Logs geschrieben. Darüber hinaus werden alle für die Signaturanwendung notwendigen Informationen und Konfigurationen für das OS bereit gestellt. Das sind z. B. Karten- und Lesertypen, zugelassene Vertrauensanker, Online-Gültigkeitsprüfungen gegen Vertrauensdienste, HSM etc. Beide Subsysteme sind sicher über TLS gekoppelt.

Unterstützte Signaturtypen

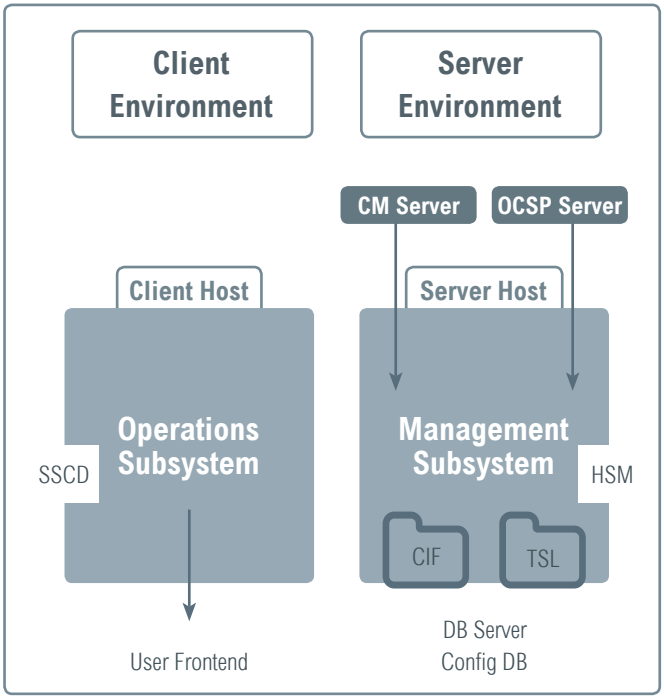
- Eingebettete Signaturen
- Abgestzte Signaturen
- PDF inline Signatur

Ideale Integrationsmöglichkeiten

Das proNEXT Secure Framework besitzt keine eigene Benutzeroberfläche (User Frontend), sondern ist als Integrationskomponente für Fachapplikationen konzipiert. Damit kann der Anwender die Signaturfunktionalitäten aus seinem Arbeitsumfeld heraus nutzen. Zur Integration wird eine REST-Schnittstelle (API) zur Verfügung gestellt, die anderen Applikationen erlaubt, die oben genannten Funktionen aufzurufen. Die Erstellung von fortgeschrittenen oder qualifizierten elektronischen Signaturen sowie deren Validierung wird für einzelne oder mehrere Dokumente ermöglicht, ebenso ihre Integration in Fachapplikationen über externe Schnittstellen.

DATENBLATT **proNEXT Secure Framework 2.0**

Signaturanwendungskomponente



Trusted Checker API (TCR API)

Diese Schnittstelle wird dazu benutzt, die zu signierenden Dokumente an den Trusted Checker zu übermitteln. Es wird geprüft, ob die Konformität zu einem vordefinierten Format gegeben ist und ob aktive oder versteckte Inhalte enthalten sind.

Smartcard Operations API (SCO API)

Die Schnittstelle wird benutzt, um alle erforderlichen Informationen der angeschlossenen sicheren Signaturerstellungseinheit (SSEE) zu ermitteln, die für den Start des Signaturprozesses notwendig sind.

Digest Operations API (DOS API)

Diese Schnittstelle dient dem Start der Signaturerzeugung und der Signaturprüfung sowie der Generierung von Hash-Werten und der Entschlüsselung von Dokumenten. Über diese Schnittstelle können auch qualifizierte Zeitstempel bezogen werden.

Operations Security API (OS API)

Über diese Schnittstelle wird der Selbsttest des Operations Subsystems gestartet. Dabei werden alle Binär- und Konfigurationsdateien des Operations Subsystems geprüft.

User Notifications

Diese Schnittstelle dient dazu, den Anwender über den bevorstehenden Start der Signaturerstellung oder den Abbruch des Signaturprozesses zu informieren.

Das proNEXT Secure Framework ist in die procilon Produktfamilien proDESK, proGOV und proNEXT zur Signaturanwendung und -prüfung eingebettet.

Empfohlene Systemvoraussetzungen

Client Umgebung:

- Microsoft Windows 7/10
- Apple Mac OS X 10
- Ubuntu Desktop 14.04 LTS
- Oracle Java SE Runtime Environment 8 with Java Cryptography Extension (JCE) Unlimited Strength Jurisdiction Policy Files for JDK/JRE 8

Sichere Signaturerstellungseinheit:

- G&D STARCOS 3.4 Health QES C1
- G&D STARCOS 3.5 ID ECC C1
- G&D STARCOS 3.5 ID ECC C1R
- TCOS 3.0 Signature Card Version 2.0 Release 1

Bestätigte Kartenleser:

- ReinerSCT cyber Jack e-com 3.0 (USB)
- ReinerSCT cyber Jack RFID standard (USB) V 1.2
- ReinerSCT cyber Jack RFID komfort (USB) V 2.0
- ReinerSCT cyber Jack secoder smartcard reader, V 3.0
- Cherry SmartTerminal ST-2xxx smartcard reader, V 6.01

(Nutzung nur mit Windows oder Linux Betriebssystemsystem)

Kontakt

procilon GROUP
Leipziger Straße 110
04425 Taucha

+49 342 98 48 78-31
anfrage@procilon.de
www.procilon.de

SecurITy made in Germany
Trust Seal www.teletrust.de/itsmig