secunet
eID PKI Suite

Universelles Sicherheitsgerüst und Vertrauensanker

für die digitale Welt

secunet.com

Geschäftsprozesse werden zunehmend elektronisch abgebildet, vertrauliche Informationen über offene, internetbasierte Plattformen ausgetauscht.

Damit Vertrauensbeziehungen im modernen Alltag funktionieren, müssen Vertraulichkeit und Integrität von Daten jederzeit gesichert sein. Eine Public Key Infrastruktur (PKI) ist hierfür die optimale Lösung: Mit PKIs werden sowohl die Nutzer-Authentifizierung wie z. B. bei der elektronischen Steuererklärung, Softwareupdates in elektronischen Geräten und Fahrzeugen oder die Einbindung intelligenter Stromzähler in Kommunikationsnetze gesichert. Die secunet eID PKI Suite bewährt sich in den unterschiedlichsten Anwendungen als verlässliches Sicherheitsgerüst, passt sich modular dem jeweiligen Kundenbedarf an und ihr CA-Kernel ist zudem nach Common Criteria EAL 4+ zertifiziert.

Eine PKI für jeden Bedarf:

Basierend auf dem umfangreichen Know-how aus über 350 Projekten und mehr als 20 Jahren Erfahrung im Bereich PKI-Design- und Implementierung hat secunet die eID PKI Suite als schlüsselfertige Lösung für Anwendungsszenarien aller Art und Größe entwickelt. Dazu zählen sowohl die Ausgabe von Mitarbeiterausweisen, sichere E-Mail, VPN und Remote Access, Smartcard-Anmeldung als auch die Authentisierung von Softwareupdates in Rechnern, elektronischen Systemen und Fahrzeugen.

Die universelle Einsatzfähigkeit der secunet eID PKI Suite basiert auf ihrem modularen Ansatz: Die einzelnen Softwarebausteinen ergeben zusammen ein leistungsstarkes Gesamtsystem oder ergänzen, einzeln implementiert, bestehende Systemarchitekturen. Auch für Anwendungen mit besonderen Sicherheitsanforderungen ist die eID PKI Suite eine zuverlässige Basis. Der nach Common Criteria EAL 4+ zertifizierte CAKernel (C^2K) ist ein Testat für die hohe Sicherheit „Made in Germany“. Unabhängig davon, welche der Bausteine zum Einsatz kommen, lässt sich die eID PKI Suite immer einfach, schnell und kostengünstig integrieren. Als bewährtes Softwareprodukt wird die eID PKI Suite fortlaufend weiterentwickelt und reduziert durch eine intuitive Benutzerführung den Aufwand für Administratoren und Operatoren.

Zertifikatsbasierte Lösungen einfach und sicher umgesetzt

Prozesssteuerung durch individuelle Workflows
Bei der secunet eID PKI Suite wird jeder Prozessschritt, wie z. B. die Ausstellung eines Zertifikats, über sogenannte Arbeitsabläufe modulübergreifend gesteuert. Durch die skriptunterstützte Umsetzung der Arbeitsabläufe können diese kundenspezifisch angepasst werden, wie z. B. durch Ergänzung des Vier-Augen-Prinzips zur Absicherung besonders sicherheitsrelevanter Prozessschritte.

Frei konfigurierbare Zertifikatsprofile
Die Eigenschaften von Zertifikaten und Certificate Revocation Lists (CRLs) werden in sogenannten Profilen definiert. In diesen Profilen können verschiedenste Attribute, wie beispielsweise nach RFC 5280 und Common PKI, flexibel nach Kundenwunsch kombiniert werden. Die secunet eID PKI Suite unterstützt auch Card Verifiable (CV) Zertifikate als kompaktes Zertifikatsformat für den Einsatz in Anwendungen mit geringer Rechenleistung wie Smartcards oder einfachen elektronischen Geräten.

Unterstützung von Key Recovery und Key Escrow
Bei der Verschlüsselung führt der (dauerhafte) Verlust des Schlüssels gleichzeitig zum Verlust der archivierten Daten – für viele Anwendungen ist eine Sicherungskopie der geheimen Schlüsselteile daher meist unverzichtbar. Bei der secunet eID PKI Suite werden im angebundenen Hardware Security Module (HSM) Schlüssel für einen Zertifikatsantrag erzeugt, die für Key Recovery bzw. Key Escrow zur Verfügung stehen sollen. Diese werden kryptografisch abgesichert in der Datenbank gespeichert.

Smartcard-Personalisierung
Die secunet eID PKI Suite enthält eine Komponente zur Personalisierung von Smartcards. Diese kann neben der optischen und elektronischen Personalisierung auch PIN-Briefe und Anschreiben für den Karteninhaber erstellen; Layouts und Texte lassen sich hierbei frei konfigurieren. Das Personalisierungssystem kann sowohl zentral als auch dezentral eingesetzt werden.

Vorteile

- Flexibilität durch konfigurierbare Workflow-Engine, Zertifikatsprofile und Veröffentlichungsregeln
- Qualität „Made in Germany“: Zertifizierte Version verfügbar (CC EAL 4+)
- Investitionsschutz durch den Einsatz eines kontinuierlich gepflegten Produktes

Technische Eigenschaften

Administration aller PKI-Komponenten über geschütztes Web-Frontend
Vollautomatisierter Gesamtprozesses durch Schnittstellen zum Zertifikatsmanagement: EST, CMP, ACME,CMC, SCEP, Smart Meter oder Kundenspezifische Webservice-Schnittstellen
Validation Authority mit OCSP und CRLs (Sperrlisten)
CA Kernel (C^2K) zertifiziert nach Common Criteria EAL 4+ (Protection Profile CIMC V1.5)*
Anbindung verschiedener HSMs
CV-Zertifikate für Industrie 4.0, insbesondere für die Automobilindustrie
Unterstützte Betriebssysteme: Windows Server, SUSE Linux Enterprise Server, Red Hat Enterprise Linux
Unterstützt Microservice-Deployment auf Docker-Basis
Datenbanken: PostgreSQL, Oracle sowie MS-SQL
Einbindung in Monitoring-Systeme über SNMP und Prometheus-Metriken

*Zertifizierungskennnummer BSI-DSZ-CC-1144-2021; den Zertifizierungsreport finden Sie auf der Homepage des BSI (https://www.bsi.bund.de/SharedDocs/Zertifikate_CC/CC/Netzwerk_und_Kommunikationsprodukte/1144.html)

Über 20 Jahr PKI-Kompetenz

1997 SINA®

Im Auftrag und auf Basis eines Grobkonzeptes des BSI hat secunet zwischen 1999 und 2002 die Sichere Inter-Netzwerk Architektur SINA entwickelt, die der sicheren Bearbeitung, Speicherung und Übertragung von Verschlusssachen (VS) sowie anderen sensiblen Daten dient. SINA umfasst eine wachsende Familie von modularen Komponenten zur Absicherung verschiedenster Anwendungsszenarien, deren Funktionalität stetig erweitert wird – mittlerweile sind weltweit mehr als 35.000 Komponenten im Einsatz.

ELSTER

secunet hat im Auftrag des Bayerischen Landesamtes für Steuern die Sicherheitsplattform für das ElsterOnline-Portal realisiert. Diese erfüllt hohe Sicherheitsanforderungen und wird seit 2002 kontinuierlich von secunet weiterentwickelt. Die Lösung unterstützt Authentisierung, Verschlüsselung und elektronische Signatur für Webanwendungen über zertifikatsbasierte Verfahren. Der Einsatz dieser Verfahren öffnet neue komfortable Online-Wege für nahezu alle steuerrelevanten Bereiche, wie z. B. Steueranmeldungen, Lohnsteuerkarte, Einkommensteuer und Steuerkontoabfrage.

OFFICE OF CITIZENSHIP AND MIGRATION AFFAIRS

Mit der Entwicklung eines Pass- und Migrationssystems hat das lettische Amt für Staatsbürgerschaft und Migrationsangelegenheiten die vorhandene Public Key Infrastruktur (PKI) für elektronische Reisepässe und neue elektronische Ausweise erneuert. Mit Implementierung der secunet eID PKI Suite können elektronische Identitätsdokumente ausgestellt sowie bei der Grenzkontrolle und in den lettischen Botschaften weltweit verifiziert werden. Lettland kann damit technisch bereits seit 2012 mit den Pässen der neuesten Generation umgehen.

2020 CLAAS

Das Management von CLAAS hat das Projekt „Security@CLAAS“ ins Leben gerufen, dessen Ziel es war, eine übergreifende Richtlinie zur Umsetzung von Cyber Security in der Produktentwicklung zu etablieren. Auf Infrastruktur-Seite war es dafür notwendig eine neue Public-Key-Infrastruktur (PKI) aufzubauen. Diese fungiert als vertrauenswürdige CLAAS-Instanz und legt somit den Grundstein für den Schutz von vernetzten Landmaschinen vor unerlaubtem Zugriff und Manipulation. Die PKI stellt dabei alle zentralen kryptografischen Funktionen, wie z.B. die Generierung von Schlüsseln und elektronischen Zertifikaten oder die Berechnung von digitalen Signaturen, zur Verfügung.

secunet Security Networks AG
Kurfürstenstraße 58 · 45138 Essen
T +49 201 5454-0 · F +49 201 5454-1000
info@secunet.com · secunet.com

Weitere Informationen:
www.secunet.com/pki

secunet eID PKI Suite x.509_DE_06/21