secunet
eID PKI Suite

Universal security framework and trust anchor

for the digital world

secunet.com

Business processes are mostly represented electronically and confidential information is sent over open, Internet-based platforms.

For trust-based relationships to function well in the modern world, confidentiality and data integrity must be safeguarded at all times. A Public Key Infrastructure (PKI) provides the best solution: PKIs can be used to safeguard user authentication, such as during electronic tax returns, software updates in electronic devices and vehicles, as well as the integration of intelligent electric meters into the communication networks. The secunet eID PKI Suite has been proven in a variety of applications as a reliable security framework, it is modular to adapt to specific customer demands and its CA kernel is also certified in accordance with Common Criteria EAL 4+.

One PKI for every need:

Based on the extensive know-how from more than 350 projects and more than 20 years of experience in the field of PKI design and implementation, secunet has developed the eID PKI Suite as a turnkey solution for application scenarios of all kinds and sizes. These include the issuing of employee ID cards, secure email, VPN and remote access, smart card logon as well as the authentication of software updates in computers, electronic systems and vehicles.

The secunet eID PKI Suite is universally applicable and based on a modular approach: The individual software modules combine to a powerful complete system or complement existing system architectures, when implemented individually. The eID PKI Suite is also a reliable basis for applications with special security requirements. The CA kernel (C^2K), certified according to Common Criteria EAL 4+, is a quality label for the high level of security "Made in Germany". Independently from the modules used, the secunet eID PKI Suite can always be integrated easily, quickly and economically. As a proven software product, the eID PKI Suite is developed at a continuous rate and thanks to its intuitive user interface, it reduces administration and operation efforts.

Certificate-based solutions, implemented simply and securely

Process control via individual workflows

In the secunet eID PKI Suite each process stage, such as issuing a certificate, is controlled by so-called workflows across all modules. Thanks to script-supported implementation, these workflows can be adapted to customers' needs, for instance by means of the two-man rule, to secure process stages that are particularly relevant to security.

Freely configurable certificate profiles

The properties of certificates and Certificate Revocation Lists (CRLs) are defined in so-called profiles. Various attributes within these profiles can be combined flexibly according to customer requirements, for instance in accordance with RFC 5280 and Common PKI. The secunet eID PKI Suite also supports Card Verifiable (CV) certificates as a compact certificate format for use in applications with low processing power such as smart cards or simple electronic devices.

Support of Key Recovery and Key Escrow

During encryption, a (permanent) lost key also results in the loss of the archived data – this is why a backup copy of the secret key parts is often essential in many applications. For each certificate request, the eID PKI Suite generates keys, which should be then available to Key Recovery or Key Escrow in the connected Hardware Security Module (HSM). These are secured cryptographically and saved in the database.

Smart card personalization

The secunet eID PKI Suite also includes a component for the personalization of smart cards. In addition to optical and electronic personalisation, it can also create PIN letters and cover letters for the cardholder; Layouts and texts can be freely configured. The personalisation system can be used both centralised and decentralised.

Benefits

- Flexibility from a configurable workflow engine, certificate profiles and publishing regulations
- "Made in Germany" quality: Certified version available (CC EAL 4+)
- Investment protection by using a constantly updated product

Technical properties

Administration of all PKI components via secured Web Frontend
Full automation of the entire process via interfaces connected to the certificate management: EST, CMP, ACME,CMC, SCEP, Smart Meter or customized web service interfaces
Validation Authority with OCSP and CRLs (revocation lists)
Certified CA Kernel (C^2K) in accordance with Common Criteria EAL 4+ (Protection Profile CIMC V1.5)*
Connection to various HSMs
CV certificates for Industry 4.0, particularly for the automotive industry
Supported operating systems: Windows Server, SUSE Linux Enterprise Server, Red Hat Enterprise Linux
Supports docker based microservice deployment
Databases: PostgreSQL, Oracle, MS-SQL
Integration into monitoring systems via SNMP and Prometheus metrics

*Certificate number BSI-DSZ-CC-1144-2021; for the certification report, please visit the BSI homepage (www.bsi.bund.de; Topics/Certification/Certified Products).

More than 20 years of PKI-experience

1997 SINA®

Based on a broad concept outlined by the German Federal Office for Information Security (BSI), secunet developed the Secure Inter-Network Architecture SINA which enables the protected processing, storage, transfer and also a full audit trail of classified information and other sensitive data between 1999 and 2002. The SINA portfolio comprises a growing family of modular components which are designed to be secure in a variety of application scenarios, and whose functionality is constantly being extended – currently there are over 35,000 components in operation worldwide.

ELSTER

On behalf of the Bavarian State Office for Taxes, secunet implemented the security platform for the Elster Online portal which supports the authentication, encryption and electronic signature for web applications via certificate-based processes. The security platform meets the highest security requirements and is being further developed and customised by secunet to meet new requirements on a continual basis since 2002. As a result of these processes, convenient, new online portals now exist for virtually all tax-related areas, including tax declarations, tax cards, income tax and tax account inquiries.

OFFICE OF CITIZENSHIP AND MIGRATION AFFAIRS

In the context of developing a passport and migration information system the Latvian Office of Citizenship and Migration Affairs (OCMA) has also renewed the existing public-key infrastructure for electronic passports and new national identity documents. As a result of the implemented secunet eID PKI Suite, the new system allows for both issuing electronic identity documents as well as their verification during border control and at Latvian consulates all over the world. Latvia has the technological capacity to process new-generation passports since 2012.

2020 CLAAS

CLAAS has launched the project "Security@CLAAS". The aim was to establish a comprehensive guideline for the implementation of cyber security in the product development of CLAAS. On the infrastructure side, it was necessary to set up a new public key infrastructure (PKI). This acts as a trustworthy CLAAS instance and thus lays the foundation for the protection of networked agricultural machinery against unauthorised access and manipulation. The PKI provides all central cryptographic functions, such as the generation of keys and electronic certificates or the calculation of digital signatures.

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

More information:
secunet.com/en/pki

secunet eID PKI Suite x.509_EN_06/21