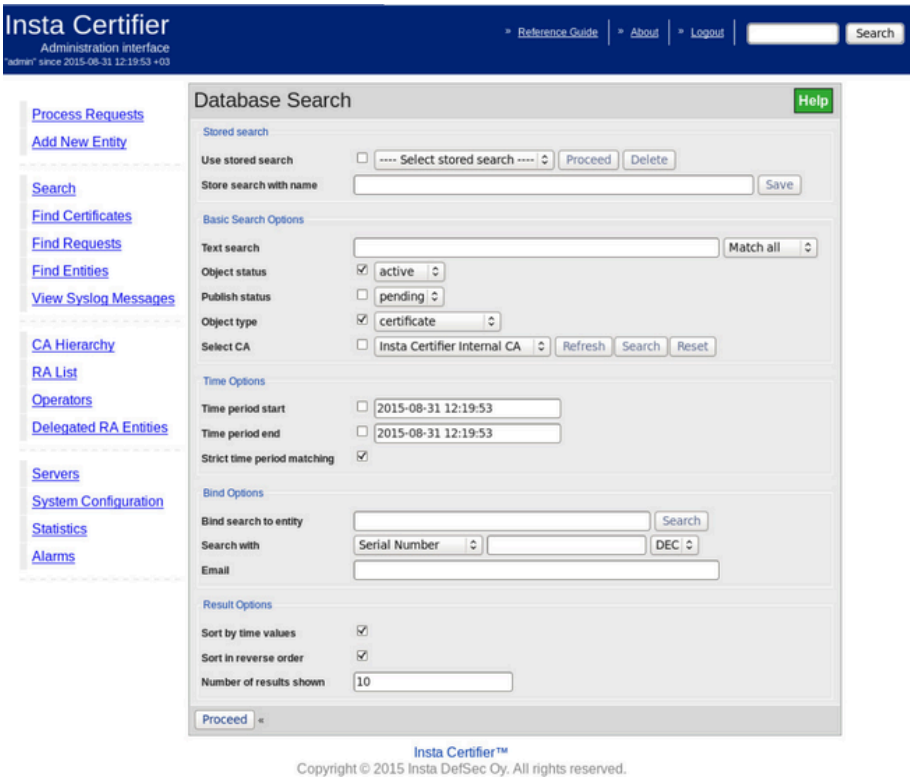
INSTA

Insta Certifier

The trust enabling CA product

insta.fi/cybersecurity

Insta Certifier is a full-featured CA (Certification Authority) product for issuing and managing digital certificates



Insta Certifier allows easy certificate enrolment for various use cases such as strong authentication of users, mobile devices, servers and web services. The product is fully standards-based, yet flexible ensuring easy adaptation to real life business processes and diverse corporate ICT environments.

Due to its security architecture and unique security features, such as support for latest algorithms, e.g. ECC (Elliptic Curve Cryptography), Insta Certifier is ideally suited to high security applications.

Being the trusted CA solution for large security-oriented organisations, a long life cycle is guaranteed, along with professional support, training and services.

KEY FEATURES

- Fully standards-based
- Scalable to large-scale PKI environments
- High availability through redundancy and clustering
- Flexible management of CA policy rules
- OCSP responder service
- Comprehensive algorithm support, e.g. ECC
- Evolving and supported

Product Highlights

Scalability and high availability through modular architecture
The modular product architecture ensures suitability for large-scale deployments with high availability requirements. The front-end PKI services and back-end certificate engine can run on dedicated servers. Furthermore, the services and certificate engine can be clustered on multiple servers to ensure high availability.

Standards-based certificate enrolment and publishing
Insta Certifier provides several standards-based interfaces for certificate enrolment, including CMPv2, SCEP and PKCS#10. Any standard HTTP server or LDAP directory, e.g. Microsoft AD or Linux directory server can be used for publishing certificates and CRLs.

Flexible management of CA policy rules
Insta Certifier provides a highly flexible framework for defining configurations for different applications. The framework enables easy creation of new CAs with their own set of certificate policy rules, making Insta Certifier the ideal platform for hosting managed multi-CA service environments.

OCSP responder included
Insta Certifier includes an OCSP (Online Certificate Status Protocol) responder service, enabling real-time retrieval of certificate status. By using OCSP, fetching and processing of potentially large amounts of CRL data can be avoided.

Product Features

Certificate management

- Online certificate life-cycle management
- Fully customizable automation of CA&RA policy rules
- Multiple CA hierarchies and RAs within an installation
- Web-based self-enrolment with customizable web enrolment pages
- Registration authority (RA) with smart card and USB token personalisation option
- Automatic CA renewal
- Manual and online cross-certification
- Online key backup and recovery
- CA private key storage in Hardware Security Module (HSM)

Revocation

- Periodic CRL publishing
- Per-revocation CRL publishing
- Self-revocation based on pre-shared key (PSK)
- OCSP responder service with whitelist checking and HSM support

Architecture

- Modular architecture: Front-end PKI services and backend certificate engine
- Clustering of multiple back-end certificate engines with geo-redundant deployment option
- Duplication of front-end PKI services
- Online and offline CA deployment options
- Secure communication between system components

Directory integration

- Certificate and CRL publishing to standard LDAP directory or HTTP server
- Flexible publishing schemas
- Support for Microsoft Active Directory
- TLS protection of LDAP publishing
- LDAP authentication

Administration

- Web administration UI with role-based access control
- Support for dual control and separation of duties
- Restriction of access to specific CAs and specific operations
- Integrity-protected event logging and audit trail
- SNMP support for monitoring and statistics

Compliance

- EU Directive on Electronic Signatures (1999/93/EC)
- EU/ETSI qualified certificates
- 3GPP CMP profile
- ICAO Doc 9303, Part 12 - Public Key Infrastructure for Machine Readable Travel Documents

Supported Protocols & Algorithms

Certificate enrolment, publishing and management protocols

- Certificate Management Protocol (CMPv2)
- Simple Certificate Enrolment Protocol (SCEP)
- Web-form-based PKCS#10 certification requests
- Web browser enrolment
- Online Certificate Status Protocol (OCSP)
- Lightweight Directory Access Protocol (LDAP)
- Hypertext Transfer Protocol (HTTP)

Supported formats

- X.509v3 certificate profile
- X.509v2 CRL format
- PKCS#1 RSA
- PKCS#6 extended certificate syntax (selectively)
- PKCS#7 envelopes
- PKCS#8 password-protected private keys
- PKCS#9 attribute types (selectively)
- PKCS#10 certification requests
- PKCS#12 Personal Information Exchange Syntax
- Certification Request Message Format (CRMF)

Interfacing with Hardware Security Modules (HSM)

- PKCS#11 crypto API
- Supports e.g. Thales and SafeNet HSMs

Security protocols

- Transport Layer Security (TLS)

Public-Key algorithms

- RSA (up to 8192 bits)
- ECC (secp256r1, secp384r1 and secp521r1)

Hash algorithms

- SHA-1
- SHA-2 (SHA-224, SHA-256, SHA-384 and SHA-512)

Symmetric algorithms

- AES 128/256-bit keys 3DES