



iNSTA

Insta Certifier 10

The Next-Generation
Trust Platform



insta.fi/cybersecurity



Insta Certifier 10 is a high-performance, high-availability Certification Authority (CA) solution engineered for organizations that demand uncompromising trust and security

Purpose-built for high-assurance environments, Insta Certifier 10 delivers robust digital certificate management while embracing the latest advancements in cryptography and standards compliance. Certifier is used worldwide in mission-critical environments in various business segments, and trusted by governmental authorities.

Product Highlights

Performance & Scalability

Leveraging a modular, microservice architecture, Insta Certifier 10 ensures rapid certificate issuance and management at scale. Clustering and georedundant deployment options guarantee continuous service operation.

Designed for mission-critical operations, the platform has scalable installation options from offline root CA laptops to clustered high available multi-DC deployments.

Automated failover and load balancing ensure uninterrupted service delivery.

Trust for the Quantum Era

Insta Certifier 10 natively supports modern post-quantum cryptography (PQC) algorithms, providing future-proof protection against emerging threats.

Permission management

Insta Certifier 10 provides fine-grained management of permission groups, users and roles. This enables multi-level access control, customized and specific roles for different operations.

- Multi – approve functionalities for all admin operations.
- Support for external user management
- Multi-tenancy support for hosting multiple separate trust environments.

Built-in readiness to introduce new cryptographic algorithms and to respond to changes in standards, threats, and regulatory requirements.

Built by experts with decades of know-how in PKI field.



Product Features

Security-First Architecture

- A powerful policy engine enables granular control over certificate issuance, renewal, and revocation
- Multi-CA and multi-RA support allows for complex, segregated trust environments within a single deployment
- End-to-end encrypted (TLS1.3) communications between all system components
- Role-based access control, dual control, and separation of duties
- Tamper-evident Audit trails and integrity-protected event logging

Algorithm support

- RSA, ECDSA
- ML-DSA (FIPS 204) as specified for X.509 in RFC 9881
- Composite ML-DSA with ECDSA

Compliance & Standards

- X.509 certificates and CRLs according to RFC5280
- CA / Browser forum baseline compliant*
- Extended Validity (EV) Certificates*
- EU/ETSI Qualified Certificate Profiles*
- Certificate Transparency support (RFC6962)*
- EU Directive on Electronic Signatures (1999/93/EC)*
- 3GPP CMP profile*
- ICAO Doc 9303, Part 12 - Public Key Infrastructure for Machine Readable Travel Documents*

Seamless Integration

- CMPv2
- REST for integration and automation
- OCSP for real-time revocation checking
- EST
- SCEP
- ACME
- Native support for external user management (e.g., Microsoft Active Directory, LDAP)
- Support for Mobile Device Management (MDM) solutions for managing end entity certificates in an organization
- Active directory devices which enroll certificates can be served from Certifier instead of Microsoft Certificate Authority

Interfacing with Hardware Security Modules (HSM)

- Integration with PKCS#11 API
- Tested with Entrust and Thales HSMs

Other Product Features

- Mass operation utility for performing large-scale PKI operations
- SNMP support for monitoring and statistics
- Supported platforms:
 - Red Hat Enterprise Linux 9
 - Red Hat Enterprise Linux 10*
- *This feature will be included in upcoming releases

Insta Certifier 10

TheNext-GenerationTrust Platform



insta.fi/cybersecurity | cybersec.sales@insta.fi

iNSTA