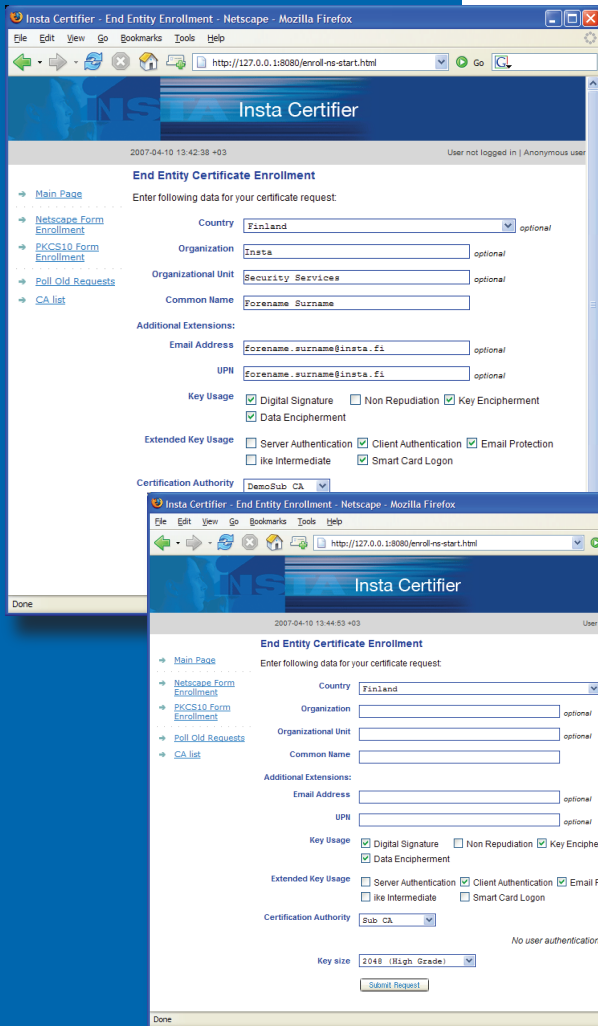


Insta Certifier

- For managing digital certificates



Granting employees, customers, partners, and suppliers access to mission-critical applications over unsecured networks is a cost-effective and common practice in today's business

environment. However, this convenience comes with important security concerns. Authentication is the first step in establishing trusted communications. Digital certificates provide the means to strongly authenticate users and devices in electronic communications.

process. By automating registration and revocation operations, HR personnel and administrators can manage user identities through a single management console while capitalizing on the benefits of PKI.

Multi-CA Hosting

New "virtual" certification authorities (CAs) with their own set of certificate policies and configurations are easily created by a system administrator with a graphical user interface (GUI), without the need to invest in additional costly hardware. This powerful feature makes Insta Certifier an ideal platform for hosting a managed multi-CA service environment. A new CA with its own policies and administrators can be created in a matter of minutes.

Scalable Architecture

Insta Certifier provides added availability and security by distributing the front-end PKI services and the Certifier engine on dedicated hosts in large-scale deployments. PKI enrollment, administration, and publishing can run independently on separate machines.

Flexible Certificate Policy Framework

Insta Certifier adapts to real-world business requirements of service providers and enterprises by providing a highly flexible framework for defining certificate policies and practices.

Support for Multiple Certificate Enrollment Protocols

VPN devices, remote access clients, and web browsers are supported for enrolling certificates with Insta Certifier. Service providers and enterprises can deploy the PKI effortlessly, as Insta Certifier does not require the

BENEFITS

- » Easy and quick to customize for customer needs
- » Effective policy configuration features
- » Servers and services can be easily multiplied for scalability and without extra cost still maintaining the security level
- » No separate client applications are needed
- » Adapts to existing environment
- » Install, configure – and just leave it running
- » Includes commercial database
- » Standards-based which enables interoperability between 3rd party sw/hw

Insta Certifier is a Public Key Infrastructure (PKI) platform product for issuing and managing digital certificates in an enterprise or service provider environment. It enables strong, two-factor user authentication based on smart cards and cryptographic tokens. The integrated identity management and authentication supported by Insta Certifier allows a highly cost-effective deployment and operation of PKI in environments of all sizes.

Integrated Identity Management

The concept of integrated identity management enables hiding the complexity of PKI by integrating the user certificate life-cycle management to the enterprise identity management

Features

Certificate Management Features

- » Online certificate lifecycle management
- » Web-based self-enrollment
- » Registration authority (RA) features with token personalization option
- » Flexible certificate issuing policies
- » Manual and online cross-certification
- » Online key backup and recovery
- » CA private key storage in a hardware security module (HSM)
- » CA/RA private key storage in a secure software environment
- » Microsoft Windows 2000/XP logon certificate issuance

Revocation Features

- » Periodic CRL publishing
- » Per-revocation CRL publishing
- » Self-revocation based on pre-shared key (PSK)
- » Built-in OCSP Responder Service

Scalable Architecture

- » Multi-platform support for all Certifier components
- » Support for duplicating Certifier servers and services for higher availability
- » Scalable architecture: a back-end Certifier Engine and front-end Certifier services
- » Multiple Virtual CAs/RAs within the same installation
- » Secure communication between Certifier components
- » Automated handling of internal system certificates

Directory Integration

- » Certificate and CRL publishing to standard LDAP directories
- » Flexible publishing schemas
- » Support for Microsoft Active Directory
- » Out-of-the-box TLS protection of LDAP publishing
- » XML-based framework for automated user provisioning

Administration

- » Web-based administration
- » Administrators can be restricted to specific CAs
- » Simplified administrator GUIs e.g. for help desks
- » Dual control and fine-grained separation of duties
- » Event logging and audit trail

Other Features

- » Customizable web enrollment pages for easier branding
- » Compliant with the EU Directive on Electronic Signatures (1999/93/EC)

Protocols

Certificate Enrollment and Management Protocols

- » Certificate Management Protocol (CMPv2)
- » Simple Certificate Enrollment Protocol (SCEP)
- » Web-form-based PKCS#10 certification requests
- » Microsoft Internet Explorer enrollment
- » Mozilla Firefox enrollment

Supported Formats

- » X.509 v3 certificate profile
- » PKIX-qualified certificate profile
- » X.509 v2 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)

Access Protocols

- » Lightweight Directory Access Protocol (LDAP)
- » Hypertext Transfer Protocol (HTTP)

Other Protocols

- » Transport Layer Security (TLS)
- » Online Certificate Status Protocol (OCSP)

Public-Key Algorithms

- » RSA, DSA

Hash Algorithms

- » MD5, SHA-1, SHA-256

Symmetric Algorithms Used with TLS

- » AES, DES, 3DES, RC2, RC4

Supported Platforms

- » Microsoft Windows 2000
- » Microsoft Windows 2003
- » Microsoft Windows XP
- » Most mainstream Linux distributions (eg. Red Hat Enterprise Linux 4 and SUSE Linux Enterprise Server 10)
- » Sun Solaris 9 (SPARC)
- » Sun Solaris 10 (SPARC)

Supported Databases

- » Sybase Adaptive Server Anywhere (embedded)
- » Oracle (Windows) via ODBC interface (requires a separate license)

Interfacing with Hardware Security Modules

- » PKCS#11 crypto API



Insta DefSec Oy

P.O. Box 174

Finlaysoninkuja 21 A

FI-33101 Tampere, FINLAND

email: security@insta.fi

www.certificate.fi