

Enterprise-wide strong authentication and VPN based on PKI

Insta CA - Use case scenario

Insta Certifier use case for enterprise-wide, strong, two-factor authentication

Insta Certifier can be used to issue digital certificates for secure and scalable user and server authentication. Because of its open and flexible architecture, the use of the certificates is not limited. Insta Certifier supports a wide variety of third-party security applications.

In this use scenario digital certificates are issued for smart-card-based authentication and IPsec VPN remote access for secure end-to-end application connections. Insta Token Master is an optional product component of Insta Certifier, which can be used as a tool to implement the user registration and electronic personalization of smart cards.

In this use case, Insta Token Master is being operated by the HR personnel as a part of their other user management duties. With the Integrated Identity Management concept, the work load for HR personnel can be kept in a minimum. There is no need for the personnel to enter duplicate user information for other system and Insta Certifier. The information entered once can be reused in certificate issuance.

Certifier Server provides the administration and CMPv2 services enabling the administration operations and user enrolment. Certifier Engine, on the other hand, is stored in a dedicated server with hardware security module (HSM) for additional security.

Figure 1 (Strong, two-factor authentication) shows an example use case how Insta Certifier can be used as an enterprise-wide authentication platform.

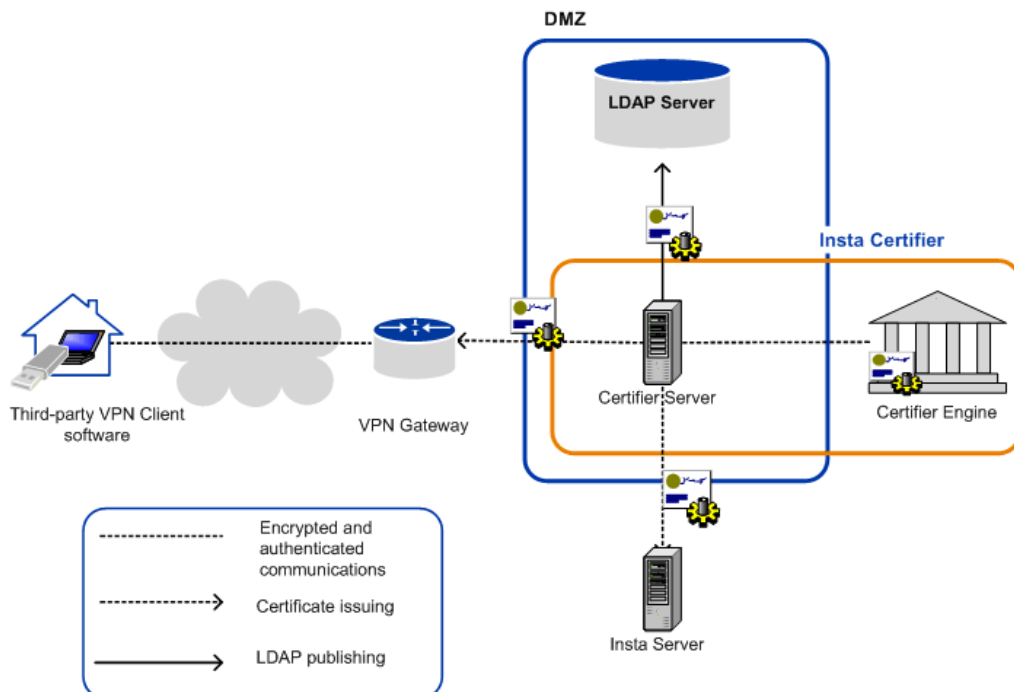


Figure 1: Strong, two-factor authentication with Insta Certifier

Sample Scenario

This section presents a sample scenario in which an imaginary Corporation X with several regional offices and a traveling sales force implements an IPsec-based VPN with a PKI. When on the road, the sales people need access to several IT resources, such as the company intranet and e-mail. There is confidential traffic between the geographically dispersed offices. Consequently, Corporation X has decided to securely connect the local networks of each office and to provide secure access to the same network for employees traveling with their laptops. To save costs, Corporation X has decided to build a VPN over the Internet instead of leasing secure lines between all offices. To avoid manual distribution of symmetric keys and to achieve strong authentication in the VPN, Corporation X has decided to use certificates and to deploy a PKI based on Insta Certifier. Software VPN clients are selected to be used for remote access in the sales personnel's computers.

PKI Deployment

After planning the deployment carefully, Corporation X decides to proceed with an installation described in Figure 2 (Insta Certifier for VPN management).

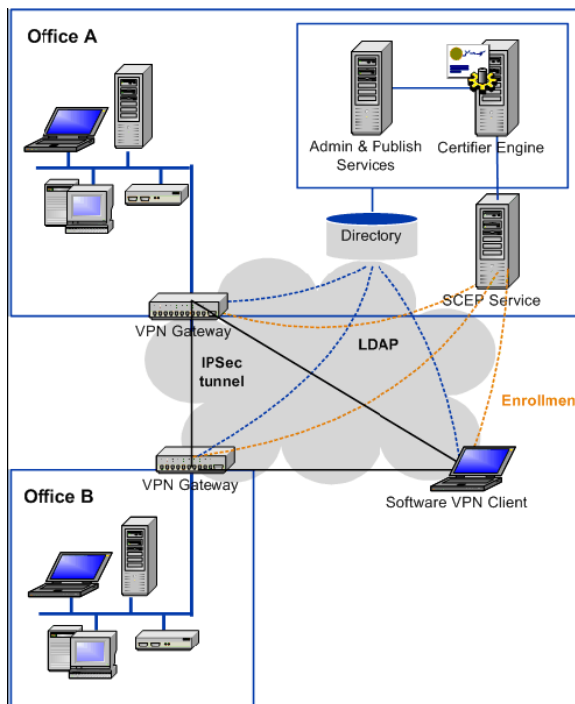


Figure 2: Insta Certifier for VPN management

The figure presents a scenario in which offices A and B are interconnected by an IPsec VPN. For the traveling personnel the company VPN is also accessible over the Internet with IPsec software clients. A VPN Gateway is the connecting point in each office. The Insta Certifier CA is installed in Office A, and provides the certification and the certificate and CRL publishing services required to operate the company VPN.

At the time of the PKI launch, Corporation X has no other plans for using certificates than to authenticate IPSec connections, so only one self-signed root CA is created. The CA's private key is stored on software (for the pilot project phase). A possible hardware-based solution will be considered later.

The Insta Certifier Engine is installed in its private network, physically on the premises with strict access control (a machine room maintained by qualified IT support personnel). A Certifier Server that runs the Administration and Publishing Services is installed on the same premises with the Engine.

Another Certifier Server is located in the semi-public (DMZ) network of the company, to enable certificate enrolment over the Internet. The only service running on this outside Certifier Server is the SCEP Service used for online certificate enrolment between the PKI, VPN gateways, and software VPN clients. The communication between the Certifier Engine and the two Certifier Servers is secured with Transport Layer Security (TLS). The support for TLS is a built-in feature of Insta Certifier and requires minimal configuration.

The directory software is installed on the same machine as the Certifier Server running the Enrolment Service. All the gateways and remote users are able to fetch the certificate revocation lists (CRLs) from that server.

Certification Practices

In the case of Corporation X the CA policy is configured to allow automatic issuance if the request includes a valid one-time password. IT support personnel who are working as CA operators will create these passwords and deliver them in person to remote users. The private key generation is done by the VPN client software and the VPN gateways, and the certificates are enrolled online. Users are instructed to use certificates only for authenticating IPSec connections. Users are also instructed to inform IT support immediately of any suspected unauthorized access to their personal laptops. As the pilot project progresses, Corporation X considers using smart-card-based authentication of remote connections.

CRLs are published by the CA every two hours, overlapping period of the CRLs is configured to be 10 minutes to avoid problems with slightly non-synchronous clocks.

Important Considerations

Not all PKI deployments are successful. To be successful in the PKI deployment presented in this example, Corporation X needs the following:

- A clear business need for the PKI must exist. Corporation X has a need for strong authentication and key management for securing mission-critical data within the organization.
- There have to be PKI-enabled applications that solve the business need. Corporation X employs PKI enabled VPN routers and VPN client software.
- Required resources for running the system must be available. Corporation X's competent IT support personnel will take on the PKI management responsibility.
- The deployment has to be planned carefully, with realistic goals and no over-ambitious plans in the first stage.

Used definitions

Public Key Infrastructure (PKI)

PKI is a scalable platform for secure user authentication, data confidentiality, integrity, and non-repudiation. PKI can be applied to allow users access to insecure networks in a secure and private way. PKI relies on the use of public key cryptography, digital certificates, and a public-private key pair to provide the following:

- **Confidentiality**
Confidentiality prevents unauthorised parties from reading or interpreting the contents of data. This is achieved by encrypting the communications and messages sent via the network. When a message is encrypted, only the person holding the correct decryption key can read the message.
- **Authentication**
Authentication can be achieved by digitally signing a message or by applying the challenge-response method to allow the recipient to ascertain the identity of the other party.
- **Integrity**
Data integrity can be guaranteed, for example, with digital signatures to ensure that files and data cannot be altered during delivery without anyone noticing.
- **Non-repudiation**
When a message is digitally signed, the signer cannot deny that he or she ever sent the message.

Virtual Private Network (VPN)

VPN allow organizations to establish end-to-end, encrypted VPN tunnels for secure connectivity for business networks, partners or remote employees. The secure tunnel is created with Internet Protocol Security (IPSec), which is a standard protocol for achieving confidentiality, authentication, and integrity in IP networks.

A typical VPN solution provides a security framework that guarantees the privacy and integrity of transferred data. Companies can establish secure tunnels between two distinct points over insecure networks. However, the tunnel cannot be considered secure if you do not know the identity of the communicating parties. More and more business critical information is stored on company servers and workstations. Companies need to ensure that only authorized users can access their resources and that the users are, in fact, those who they claim to be. In a computerized environment where face-to-face contact is not an option, companies must be able to trust that the party with whom they are in contact is indeed who the company thinks it is.

Two-factor Authentication

Authentication is a way to prove the identity of an individual or application. Two-factor authentication is any authentication protocol that requires two independent ways to establish identity and privileges. Typically one mean of identification is a physical token, such as a smart card or a USB token, and the other of which is typically something memorized, such as a security code. In this context, the two factors involved are sometimes spoken of as *something you have* and *something you know*. This contrasts with traditional password authentication, which requires only one factor (knowledge of

a password) in order to gain access to a system. Using more than one factor is also called strong authentication; using just one factor, for example just a password, is considered weak authentication.

In a VPN, PKI-based authentication methods are used to authenticate users securely. Data integrity and encryption are usually implemented in the IPSec/IKE protocol framework with symmetric algorithms.

In PKI-based authentication, security is as strong as the protection of the private key. If the private key becomes known, anybody can act as the holder of the private key. Therefore smart cards or hardware tokens (USB tokens) are used to protect the private key. These devices are next to impossible to copy and provide two-factor authentication in the same manner as OTP devices. They also offer a practical and secure method for distributing trusted CA certificates to users, as the delivery of smart cards and tokens to users is usually organized in a secure manner.

Solution Components:

The solution components of the use scenario include:

- Insta Certifier
- Standard smart cards and smart card readers or USB tokens (optional)
- Insta Token Master
- Insta Mover VPN

Insta Certifier

Insta Certifier is a CA (Certification Authority) product for issuing and managing digital certificates in a service provider and enterprise environment. Insta Certifier enables the use of strong two-factor user authentication with smart cards and USB tokens to support secure access to enterprise applications. In addition to providing authentication management, Insta Certifier can be used as a backbone for building secure services such as Virtual Private Networks (VPNs), secure e-mail, single sign-on (SSO), and network logon based on third-party products.

Smart Cards

Smart cards provide a tool for two-factor authentication together with the possibility of personalization also the physical interface of the smart card. Smart Cards are based on PKCS# 15 card profiles. The cards contain a chip where the users certificates are stored and a separate PIN-code is given for safely accessing the variety services in the organization. Insta also provides smart card readers and other software.

USB tokens

An ideal solution to two-factor authentication is the use of USB tokens. USB tokens are easy to use, portable and cost-effective identity devices. USB tokens provide identity proof with someone that the user has (USB token) and something that the user knows (PIN-code). No separate readers are needed for using the USB tokens.

Insta Token Master

Insta Token Master is a versatile Public Key Infrastructure (PKI) Registration Authority (RA) product for managing and personalizing various cryptographic tokens, such as smart cards and USB tokens with easy-to-use graphical user interface. Insta Token Master supports use of multiple CAs and RAs and multiple different token profiles.

Insta Mover VPN

Insta Mover offers remote users secure access to company local network and services. For remote sites and networks it enables easy and seamless connectivity to central office. Access control and authentication is based on Public Key Infrastructure (PKI) and communication is secured using IPsec VPN Technology. The mobility support is based on the Mobile IP standard.

Insta DefSec Security Systems

Insta DefSec's Security Systems is a global information security specialist developing and supplying networking and information security solutions. We focus on innovative solutions and applications for customers with high quality and security requirements.

Our product and service solutions enable our customers to benefit from improved business models and to develop their operations. Efficient, secure e-business and networking solutions improve our customers' business operations, administration and utilization of modern technology.

Our know-how, technology and processes represent the absolute top in their field, which is why we have reached an internationally recognized position in the information security market.