

Certificate service provision

Insta CA - Use case scenario

Insta Certifier use case for certificate service provision

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 Insta Certifier works as a base of CA hosting services.

Sample Scenario

In this sample scenario, Company Y is starting up a certification service provision business. The company is already on the security products and provision market with information security consultancy.

In Company Y's vision the provision of PKI services is an attractive business. Many small companies lack the resources to deploy their own internal PKIs, but still require PKI services to secure their internal and external IT services. Company Y attempts to seize the opportunity provided by the need of these companies, and has decided to start in the business of certification and CA hosting services.

The goal of the deployment is to build, host, and maintain a highly secure CA and certificate creation environment on behalf of the customers. However, the idea is that customers dedicate qualified administrators in their organization to handle the actual user identification and registration process. This allows the customers of Company Y to outsource most of the PKI deployment work and maintenance but yet retain full control of the user registration and certification practices.

Digital Certificates provide a means of proving your identity in electronic transactions. They can be used for strong authentication of user identities, digital signatures or data encryption. Strong authentication is required for secure remote access (IPSec), login onto Windows domains and web authentication (TLS/SSL). Digital signatures are used to ensure that data, documents or messages cannot be modified and to authenticate the identity of the signatory. For data encryption, digital certificates provide an easy and reliable way of sharing a public key.

In this case scenario the target applications that the customers are looking for are secure e-mail (S/MIME) and web server authentication (TLS). Support for most popular web browsers and an e-mail client is provided in the service.

PKI Deployment

Support for multiple CAs with hierarchies makes Insta Certifier suitable for a CA hosting environment. Company Y has located their Certifier Engine in high security premises. The CA private key will be stored in a hardware security module (HSM). When a new customer is being provisioned, a new CA private key and CA entity is generated for the customer and stored in the HSM. The policies, certificate publishing and revocation mechanisms are selected in co-operation with the customer.

The issuance policy of the hosted CAs is based on RA verification. Each company subscribing to Company Y's CA hosting services receives the Insta Certifier software with RA functionality. When the dedicated RA administrator of the customer has done the user verification, an RA-signed request is sent to the Insta Certifier CA maintained by Company Y. The Certifier Engine can then automatically issue the certificate with a corresponding customer CA private key. The CA policies allow automatic issuance of RA-verified user certificates so that manual certificate request processing is not needed in the CA environment.

Company Y's service offering includes also the certificate and CRL directory (or OCSP service) over the public Internet. Customers that do not want their certificates to be published on the Internet are provided a certificate-based or password-based access control to the certificate directory. The deployment is described in Figure 1 (Insta Certifier for a certification service provider).

Certification Practices in Distributed PKIs

All users that are registered into the PKI must be reliably and securely identified prior to the creation and enrollment of their certificates. The secure identification of users cannot be easily done by the certification service provider. Therefore, Company Y decides to delegate the responsibility for registration and operation to the customer organization. The customer companies that subscribe to Company Y's PKI services will set up internal registration authorities (RAs) for user identification duties. The CA/RA architecture of Insta Certifier provides convenient means for this. The end user employees perform browser-based enrollment including private key generation with their browsers using the RA server web pages that have been added to the intranets of the customer organizations. The RA administrators have generated a one-time password for each customer and distribute them. These passwords are used to access the enrollment web pages to enable automatic RA verification.

Once an RA-signed certification request is sent over the Internet to the CA operated by Company Y, a certificate matching the request is automatically generated, provided that the RA signature is found authentic.

It is important to notice that since the RA signature is a sufficient requirement for certification, the RA signature creation environment has to be secure. Company Y leases hardware-based key storage devices for customers who require a higher level of security than software keys can provide.

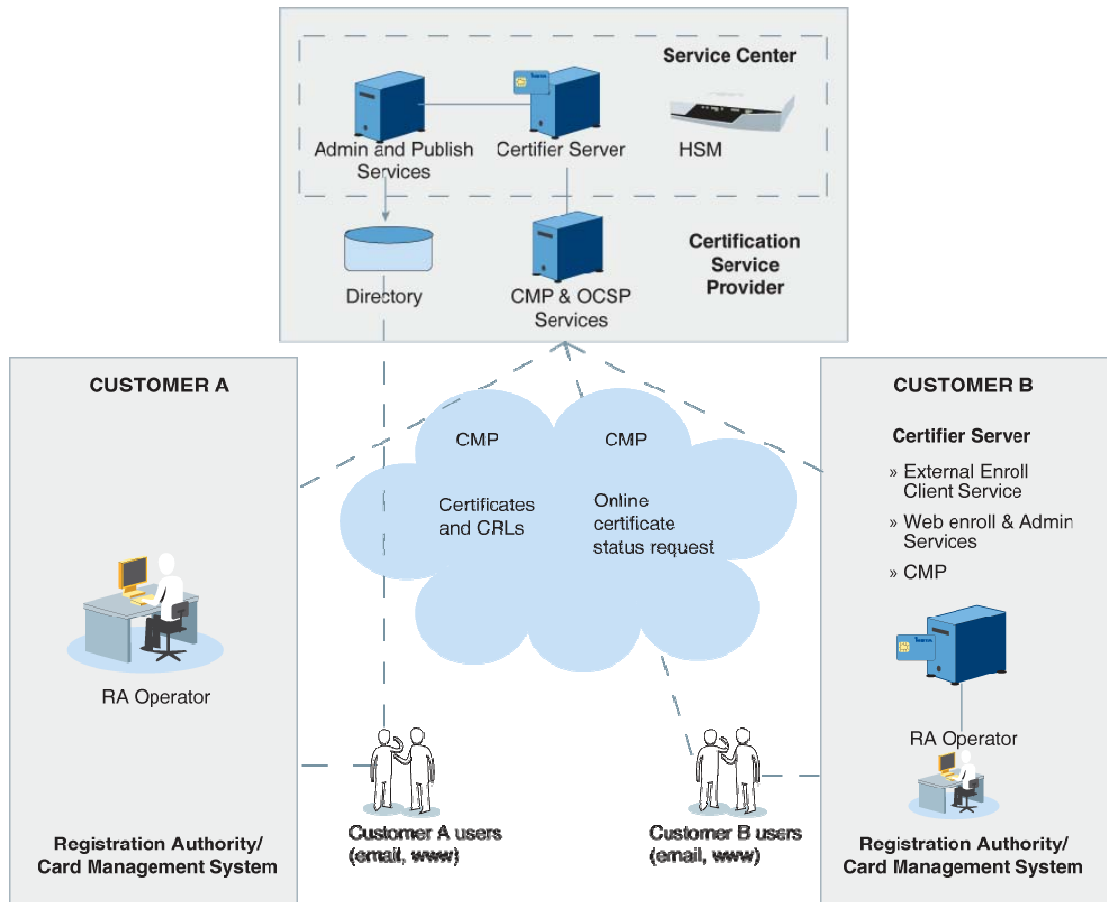


Figure 1: Insta Certifier for a certification service provider

In Figure 1 (Certification service provider), Company Y, acting as a certification service provider, serves two customer companies that both run the Insta Certifier RA installation on their premises. The CA of Company Y utilizes an LDAP directory for CRL and certificate publishing as well as an HSM for secure hardware storage of the CA private keys.

Important Considerations

The identification of users prior to the issuing of their initial certificates always requires manual effort. The tasks of password creation and delivery, face-to-face registration or other out-of-band verification cannot be omitted or entirely automated without risking the overall security of the PKI. These identification tasks can be either centralized to CA or distributed locally to RAs. The Insta Certifier supports both modes of operation.

An important decision in the PKI deployment planning is whether a distributed PKI architecture with RAs is used or not. While the CA administrators can have secure remote connections and operate locally, the use of RAs allows the building of a comprehensive local PKI registration system. In the example scenario presented above, Company Y with global operations lacks the resources to perform identification of every single end user, and therefore opts for the distributed RA model. In reality, it may also prove that customers subscribing to PKI services would not even want to delegate the user identification service to a third party. In the example case, providing on-site RA software for each customer brings Company Y significant savings in operational costs while offering the customer the possibility to manage the registration. Yet the overall system achieves the goal of outsourcing the certificate creation and CA operating services.

The less installation and configuration is required on the client side and the more the existing applications can be utilized, the better the chances for a successful PKI deployment are. In this example scenario, the registration and user certificate enrollment are provided with intranet web pages and the client applications are familiar web browsers and e-mail clients. Extensive user training is not required and most of the PKI specific technical details are hidden from the end users. One of the biggest obstacles to the adoption of the PKI technology has been the complexity of the technology from the users' point of view. Therefore, all steps that can be taken to hide this technological complexity and to make the system easier to use increase the chances of success.

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.

Secure E-mail (S/MIME)

MIME (Multi-Purpose Internet Mail Extensions) refers to an official Internet standard that specifies how messages must be formatted so that they can be exchanged between different email systems. MIME is a very flexible format, permitting one to include virtually any type of file or document in an email message. Specifically, MIME messages can contain text, images, audio, video, or other application-specific data. S/MIME is a secure version of MIME and it is based on digital certificates that allow people to send digitally signed and/or encrypted e-mail messages to others. S/MIME combines traditional symmetric ciphers, public key cryptography, hashing, and public key certificates to ensure secrecy and authentication of e-mail traffic.

Web Server Authentication (TLS)

Transport Layer Security (TLS) is a protocol that ensures privacy between communicating applications and their users on the Internet. When a server and client communicate, TLS ensures that no third party may eavesdrop or tamper with any message. TLS is the successor to the Secure Sockets Layer (SSL).

The protocol consists of two layers - a TLS Handshake Protocol and a TLS Record Protocol. The handshake protocol creates a "secret" used by the record protocol to encrypt messages. The record protocol also provides mechanisms for preventing a message from being altered.

Solution Components:

The solution components of the use scenario include:

- Insta Certifier
- Insta Token Master

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.

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 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.