

Windows PKI

Secardeo GmbH, 2011

Windows PKI

What is PKI?

A Public Key Infrastructure (PKI) provides keys, certificates and other services, which make efficient and reliable security management possible. Nowadays, with digital identities (certificates) it is possible for a lot of applications to be secured on a very high level. The digital certificates of a PKI can be used for secure e-mail, web-security, windows smartcard-Logon, VPN, encryption of file systems or documents as well as digital signatures.

What is the benefit?

PKI makes the application of cryptographic security measures in large companies feasible. PKI enables the encryption of data, the strong authentication of users and IT components and digital signatures. Through this the security level can be increased significantly. Problems with forgotten or cracked passwords and expenses for helpdesks as well as for identity management can be minimized by using a PKI. Access to confidential information can be controlled, even if sensitive parts of a company are outsourced. Only a PKI allows the use of digital signatures and herewith the general automation of business processes. PKI offers

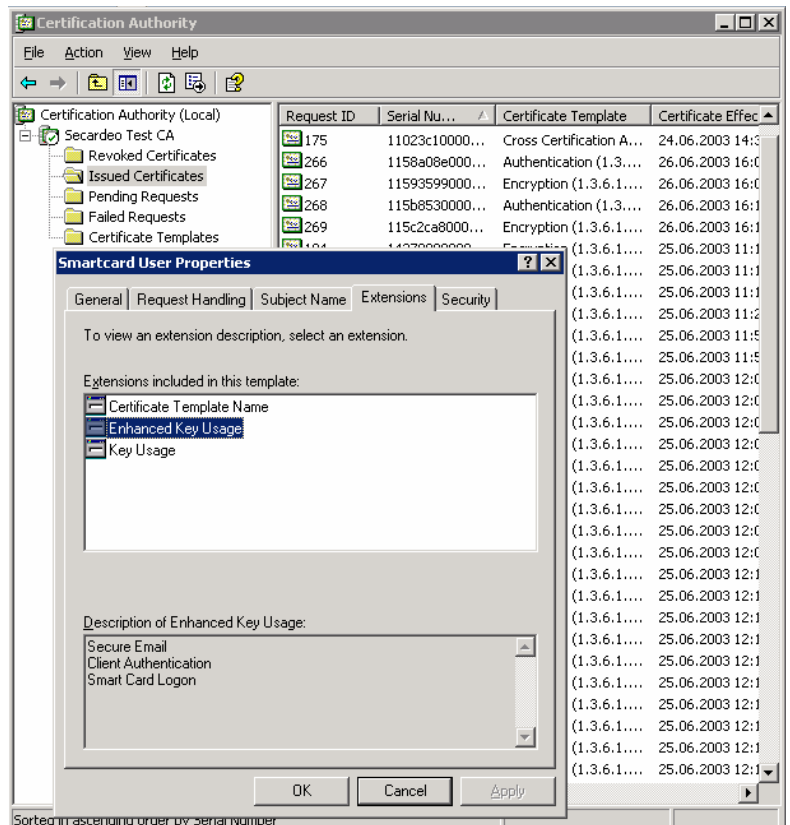
- High security
- common basis for security applications
- efficient identity management
- increased user comfort and
- cost reduction for administration and helpdesk.

Why Windows PKI?

The basis for a Windows PKI is already present in Windows Server and its Active Directory Certificate Services (AD CS). This service was introduced with Windows NT 4.0 and can be considered as a solid and reliable platform with the version contained in Windows Server 2008 R2. So, the Windows PKI has been well established in the market and besides a huge number of small and medium sized implementations also several global infrastructures with several thousands of users exist. In a native Windows infrastructure, all advantages of the Certificate Services can be used in combination with Active Directory as an Enterprise CA. But also in heterogeneous environments products from other vendors like Adobe, Cisco or Open Source Tools will be well supported by the supported standard formats and interfaces. With a Windows CA certificates can be issued in a cost effective and user transparent way by Autoenrollment or with manual registration methods and Enrollment Agents in a reliable manner. Software keys as well as SmartCards are supported. Microsoft provides a series of interfaces for enhancements or customer specific adaptations. By this, also third party SmartCard or Token Management Systems may be adapted.

What does a Windows PKI provide?

The Windows PKI supports major PKI-Standards like X.509, PKIX and PKCS. With a Windows PKI different trust models and certification structures may be mapped. In a multi level hierarchy a Windows CA may have the role of a Root, Intermediate or Issuing CA. A Windows CA may be operated in two modes:



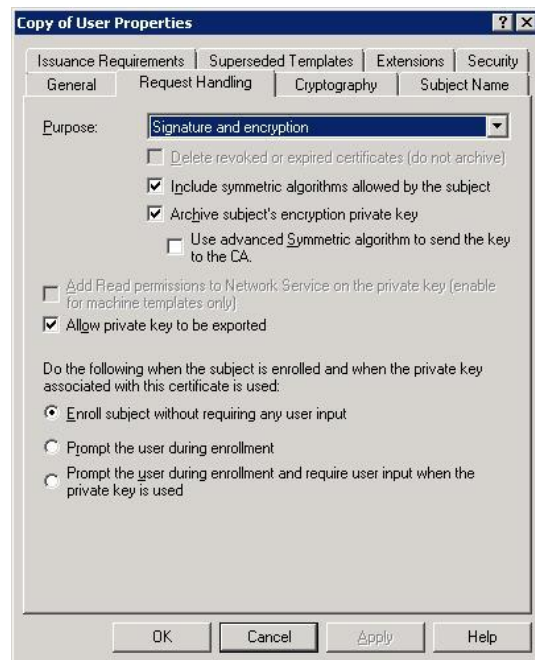
A Standalone CA enables the usage without Active Directory. A Standalone CA may also be logically integrated with the AD Domain, without being available at any time. An example is an Offline Root-CA for a domain. This variant offers a high level of security whereas the possibilities for user registration and certificate management are limited.

An Enterprise CA is fully integrated with an AD domain. Issued certificates and CRLs will be published to AD automatically. For the user friendly and flexible request of certificates so called certificate templates are used. With these templates different registration scenarios up to the automated registration and certification (Autoenrollment) without a user interaction may be implemented. With a certificate template also individual certificate profiles with customer specific extensions may be specified.

Windows supports a series of crypto algorithms and so called Crypto Service Provider (CSP). With such a CSPs key pairs will either be generated within the operating system or with an external hardware component like a SmartCard. In a Windows PKI software keys or SmartCards may be used for encryption, authentication or digital signatures.

The Windows CA may also be used for the backup and recovery of private decryption keys. These will be encrypted and stored in a database and they may be recovered by a key recovery agent (KRA) with specific certificates. This is important so that a user can read again his emails after having lost his private key.

The revocation lists (CRL) and delta-CRLs issued from the Windows CA enable the validation of a certificate. Starting with Server 2008 also the validation check using the Online Certificate Status Protocol (OCSP) is supported. This method is more efficient and avoids downloading large CRLs via the network.



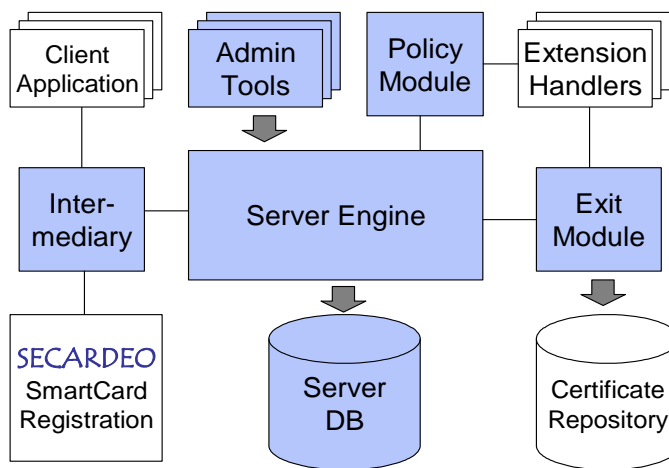
How does the Windows CA work?

The Windows CA has a modular concept and offers a number of interfaces. A client application like Internet Explorer generates a key pair and sends a certificate request to an Intermediary. It receives back an issued certificate. The Intermediary, e.g. Internet Information Services, provides an interface to the client, in this example a Web-ASP page and communicates with the central CA server via a COM interface.

The Server Engine passes the certificate request to the according Policy-Module and issues the requested certificate. Certificates and optionally private keys to be archived will be stored in the local certificate database and passed to an Exit-Module. The Policy Module checks the certificate requests and enhances or modifies them if required. It decides whether it has to be refused or to be issued immediately or to be delayed.

An Enterprise CA makes use of the pre-installed Enterprise Policy Module, a Standalone CA uses a different Default-Policy. An Exit-Module will be called in the case of certain events like the issuance of a new certificate. A major task is the publication of certificates and CRLs, e.g. in AD. Individual Policy- and Exit-Modules may be implemented and integrated.

Using the administrator interface certificate requests may be acknowledged or refused, Existing certificates may be validated or revoked. Furthermore, a CRL generation may be enforced.



What has to be considered for SmartCards?

Windows and AD CS support SmartCards and other components like USB Crypto Tokens and Hardware Security Modules (HSM). For this, the according CSP of the SmartCard must be installed and access using a smart card reader must be possible. Originally the usage of SmartCards was limited by Microsoft for authentication purposes like Windows SmartCard Logon. Keys for authentication and digital signatures may be generated on a smart card securely and they may be replaced by new keys or smartcards at any time. When using smartcards for en- and decryption further requirements exist. Especially the archival of the private key and the reconstruction of it must be possible at any time. Many SmartCards and their CSPs do not support this natively.

On the market there are products like card management systems or token management systems. Microsoft offers the product Identity Lifecycle Manager (ILM) which comprises the tool Certificate Lifecycle Manager (CLM). CLM requires the installation of specific Policy- and Exit-Modules on Enterprise CA and a client module on all attached Windows-Systems. CLM currently only supports a limited set of SmartCards and Tokens.

A thin and adaptable alternative is SECARDEO's certRA (Registration Authority). The certRA is a universal, SmartCard-independent registration tool that supports the Key Backup function and an extended PIN/PUK-Management. A card may be initialized flexibly and parameterized securely. Certificates may be issued or renewed for existing public keys and they may be published to any standard LDAP directory.

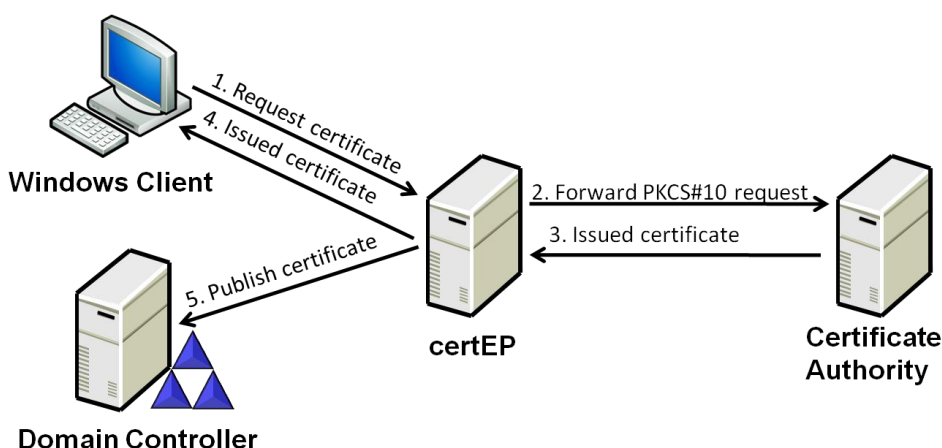
The certRA may be integrated with existing card management systems. By this, multifunctional employee badges, originally equipped with photos for access authorizations and payments may be enhanced for PKI.



Can certificates for a Windows domain be issued from a non-Windows CA?

In some environments the use of a certain CA product is desired, which can also issue certificates to windows user or systems. The Secardeo certEP Certificate Enrollment Proxy offers manual and automated enrollment of authentication and encryption certificates from a Non-Microsoft CA.

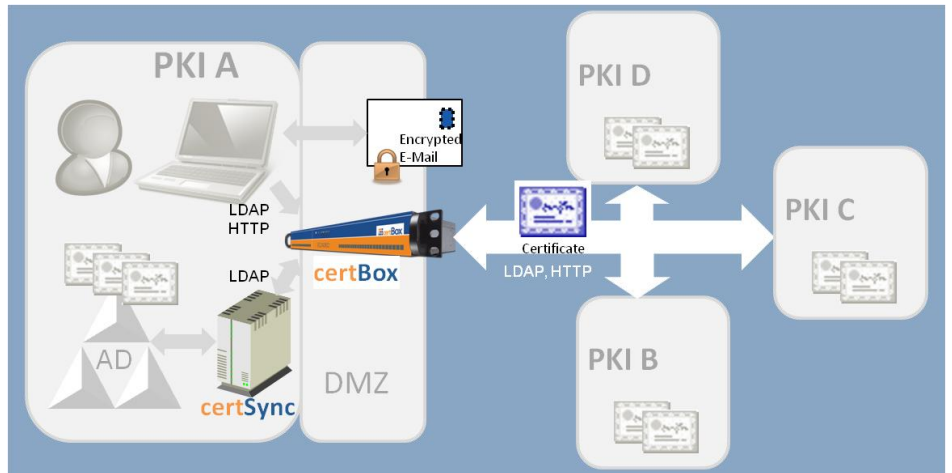
The certEP resides between the Windows Clients and the external Issuing CA. Towards the Windows Clients the certEP acts like a Windows Enterprise CA and serves their certificate requests. Towards the Issuing CA the certEP acts as a Client and it forwards the certificate requests to the CA.



How can I communicate securely with other PKIs?

For the encryption of data like e-mails the recipient's certificate is needed. This is normally feasible within a corporate network (Intranet). But what is the situation when communicating with external partners? Within a Windows AD Forest the certificate may be retrieved directly from AD by a client like Outlook. Normally the AD is not reachable from external by security reasons.

On the other hand searching for an external certificate from the Intranet in multiple LDAP servers is not, or even in a restricted way, possible today in most cases. These limitations are eliminated by SECARDEO's certBox Appliance which typically resides within a DMZ. In order to find the external certificate of a recipient for the searching client, the certBox localises the corresponding directory and forwards the search request to it. The certificate



returned will be passed to the client who can do the encryption then. If an external partner wants to encrypt data to an internal recipient he needs his certificate in AD. For this the certBox accepts LDAP search requests from external and forwards the tot he internals AD. Alternatively the AD's certificates may be published on the certBox using the certSync Service. The certBox provides access control and blocking of methodical trial requests and assures confidentiality of the returned data by a patented mechanism. Additionally, the certBox provides interoperability of different client applications with heterogeneous LDAP-Servers.

What can you expect from SECARDEO?

The Windows AD CS may be installed and taken into operation with the pre-defined authorizations by a few mouse clicks. A standard installation pre-defined by Microsoft may be performed with few efforts by an experienced system administrator. If such a standard installation fulfills the corporate security requirements and covers the company's systems and applications and if it may be operated and extended reliably and efficiently for a long term – these questions should a responsible IT manager ask beforehand. SECARDEO may help here, as SECARDEO has performed a huge number of PKI projects successfully and knows how to handle medium sized up to very large PKIs with several hundred thousands of users.

SECARDEO supports a PKI-Project in the preparation phase and the technical and organizational planning. Th implementation of a Windows PKI including project specific adaptations and the integration with individual IT environments is one of our core competences. Also during operation of a PKI we offer reliable, continuous support-, check- and troubleshooting services. SECARDEO helps you through

- Know-how transfer in Inhouse-Seminars and Workshops on Windows PKI,
- Design of a technical and organizational PKI concept,
- Installation, secure configuration and reliable take-into-operation of Windows AD CS,
- Generation of secure CA keys using hardware,
- Extensions for the management of SmartCards and Tokens with SECARDEO certRA,
- Integration mit der Kartenverwaltung für multifunktionale Mitarbeiterausweise,
- Connection with external certificate directories using SECARDEO certBox,
- Provisioning of a secure access to internal certificates using SECARDEO certBox,
- Adaptation of non-Microsoft CA products using SECARDEO certEP,
- Adaptation of existing applications and systems ,
- Piloting and support for a PKI-Rollout.

You need further information?

For further information please contact:

Secardeo GmbH
Hohenadlstr. 4
85737 Ismaning
Tel. 089/18935890