



PKI Enrollment

Certificate Enrollment Proxy

- Enroll certificates to a Windows domain
- Non-Windows CA
- Manual enrollment
- Autoenrollment
- Key archival
- No software installation required on Windows clients



Issue Windows certificates by external CA
Automated, reliable, manageable

Windows Certificates

Windows Client and Server operating systems and many Windows applications support X.509 certificates. A Windows enterprise CA issues certificates to domain members either by manual requests or by autoenrollment. Enrollment is done by specific mechanisms which are supported by the Windows OS and by Active Directory.

Non-Windows CA

There are environments, where certificates have to be issued to Windows Domains by a non-Windows CA. Either by using a different CA software or an external PKI service provider. Mechanisms are needed to seamlessly integrate such CA services with an existing Windows Domain.

Certificate Enrollment Proxy

The Secardeo Certificate Enrollment Proxy (certEP) is a component that sits between the Windows Clients and the external issuing CA. The certEP acts as a Windows enterprise CA towards Windows clients and accepts their certificate requests. Towards the issuing CA, the certEP acts like a requesting client and it forwards the Windows requests to the CA. The certEP itself does not perform CA signing functions. After receiving the issued certificate from the CA, it is passed to the requesting Windows client. Additionally, the certEP supports key archival. If a certificate request contains an encrypted private key, the encrypted

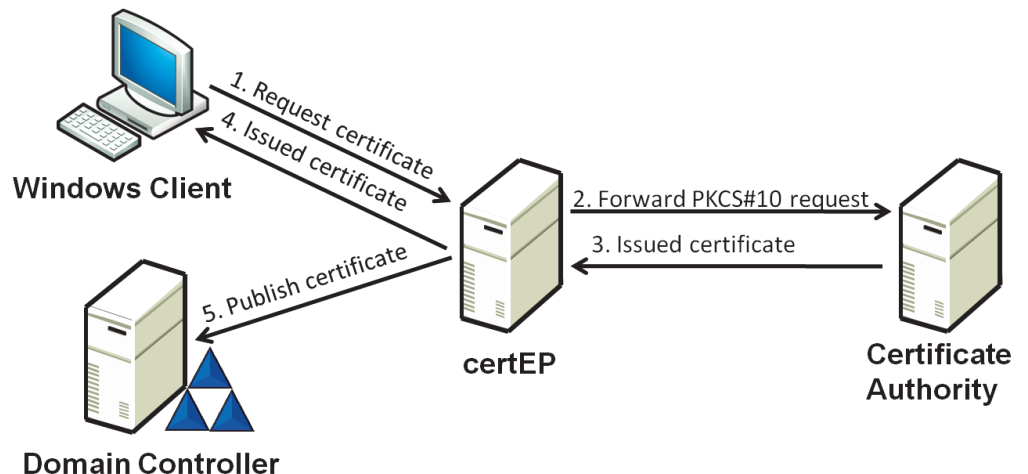
key is extracted and is sent together with the request to the external CA.

The certEP uses Microsoft certificate template information to process certificate requests.

Integrating the certEP

The Secardeo Certificate Enrollment Proxy uses a web interface for transmitting requests to the issuing CA. The response from the CA contains the issued certificate. SSL Client Authentication using HTTPS is supported for this. Depending on the CA product and interfaces, customization of this interface is possible.

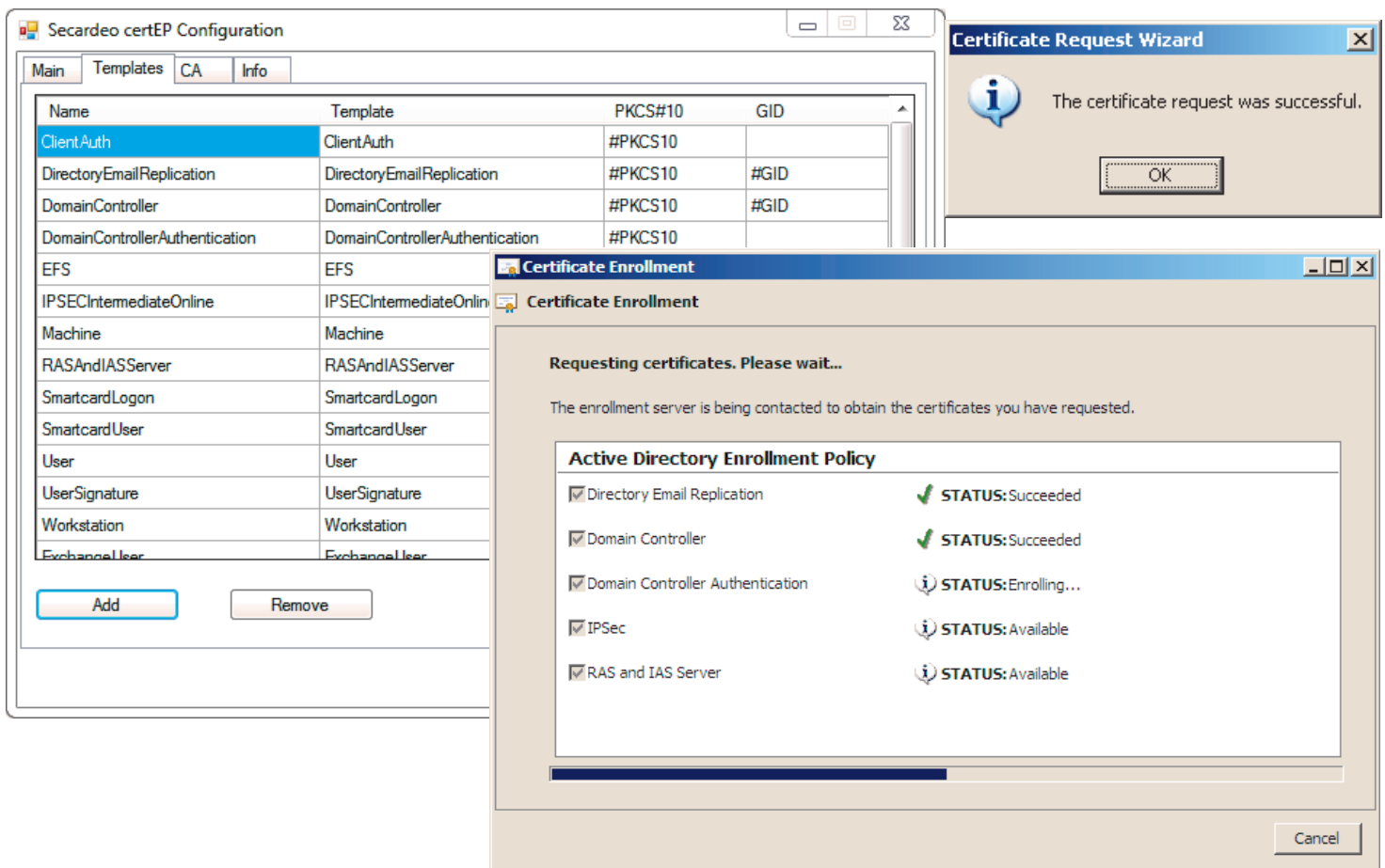
The certEP is installed as a Windows service and is integrated into the Active Directory.



Secardeo GmbH
Hohenadlstr. 4
D-85737 Ismaning
Tel. +49 89 18 93 58 90
Fax +49 89 18 93 58 99
info@secardeo.com
www.secardeo.com

Secardeo certEP is a Certificate Enrollment Proxy for X.509 Certificates. The certEP is deployed in a Windows domain and enables Windows clients to request certificates from a non-Windows CA product using Windows certificate enrollment. The certEP offers the following features:

- ICertRequestD interface implementation
- Manual and autoenrollment of certificates in Windows Domains
- Receives certificate requests from Windows computers and users via DCOM
- Extracts the PKCS#10 request from received certificate request and forwards it to a configured CA using a web interface
- Returns issued certificates to the requesting client and publishes the issued certificate to Active Directory
- Supports https with certificate-based client authentication to forward requests to the non-Windows CA
- Supports key archival
- Supports v1 and v2 certificate templates to process certificate requests from Windows clients
- Optional: Synchronization of CRLs between CA and AD



The screenshot shows the Secardeo certEP Configuration window with a table of templates and two dialog boxes. The Configuration window has tabs for Main, Templates, CA, and Info. The Templates tab is active, showing a table with columns Name, Template, PKCS#10, and GID. The Certificate Request Wizard dialog shows a successful message: "The certificate request was successful." with an OK button. The Certificate Enrollment dialog shows "Requesting certificates. Please wait..." and a list of Active Directory Enrollment Policies with their statuses.

| Name | Template | PKCS#10 | GID |
|--------------------------------|--------------------------------|---------|------|
| ClientAuth | ClientAuth | #PKCS10 | |
| DirectoryEmailReplication | DirectoryEmailReplication | #PKCS10 | #GID |
| DomainController | DomainController | #PKCS10 | #GID |
| DomainControllerAuthentication | DomainControllerAuthentication | #PKCS10 | |
| EFS | EFS | | |
| IPSECIntermediateOnline | IPSECIntermediateOnline | | |
| Machine | Machine | | |
| RASAndIASServer | RASAndIASServer | | |
| SmartcardLogon | SmartcardLogon | | |
| SmartcardUser | SmartcardUser | | |
| User | User | | |
| UserSignature | UserSignature | | |
| Workstation | Workstation | | |
| ExchangeUser | ExchangeUser | | |

Active Directory Enrollment Policy

| | |
|--|------------------------|
| <input checked="" type="checkbox"/> Directory Email Replication | ✓ STATUS: Succeeded |
| <input checked="" type="checkbox"/> Domain Controller | ✓ STATUS: Succeeded |
| <input checked="" type="checkbox"/> Domain Controller Authentication | ⓘ STATUS: Enrolling... |
| <input checked="" type="checkbox"/> IPsec | ⓘ STATUS: Available |
| <input checked="" type="checkbox"/> RAS and IAS Server | ⓘ STATUS: Available |

Operating System:

- Microsoft® Windows® Server 2003 (32 bit)
- Microsoft® Windows® Server 2008 (32 bit)

Requirements:

- Microsoft .NET Framework 2.0 SP1

Supported Client OS:

- Windows XP
- Windows Vista
- Windows 7
- Windows Server 2003
- Windows Server 2008

Supported Templates:

- V1 Certificate Templates
- V2 Certificate Templates

Supported Request Types:

- PKCS#10
- CMS with PKCS#10
- CMS with CMC
- Key archival requests

Key Features:

- Supports key archival
- Supports v1 and v2 certificate templates
- Publishes issued certificates into Active Directory

Standards:

- X.509-Certificates RFC 3289
- PKCS#10 RFC 2986
- CMS with PKCS#10 RFC 3852
- LDAPv3 RFC 2251
- Certificate Management over CMS RFC 5272

Supported Software Products:

- Aladdin Token Management System
- IBM z/OS CA
- OpenSSL CA
- Nexus CA
- Please ask for further CA products