



Certificate Enrollment

Certificate Enrollment Proxy

- Integrate Non-Microsoft CA with Active Directory
- Manual or autoenrollment
- Key archival (KRA)
- Flexible migration to other CA
- No client software installation required



Autoenrollment with a non-Microsoft 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.

Non-Microsoft CA

There are environments, where certificates have to be issued to Windows Domains by a non-Windows CA. Either by using an Open Source or vendor CA product or by an external MPKI SaaS provider. By this also globally accepted certificates for S/MIME may be enrolled from a public CA. Mechanisms are needed to seamlessly integrate such CA services with an existing Windows Domain.

Certificate Enrollment Proxy

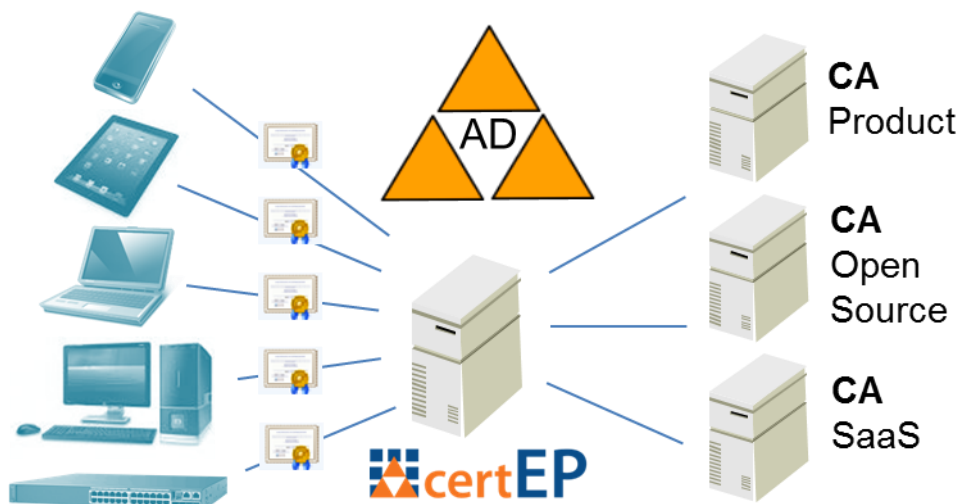
The Secardeo Certificate Enrollment Proxy (certEP) is a component that sits between the Windows Clients and the external issuing CA. The certEP acts as a Windows enterprise CA towards Windows clients.

It receives their certificate requests, enhances them with the required attributes and forwards them to the issuing CA. After receiving the issued certificate from the CA, it is passed to the requesting Windows client. Additionally, the certEP supports key archival, e.g. for S/MIME certificates. Private keys can be archived locally by encrypting them by KRA certificates or remotely at the CA. The certEP uses Microsoft certificate template information to process certificate requests.

Integrating the certEP

The Secardeo Certificate Enrollment Proxy provides HTTP, SOAP and CMP interfaces for transmitting requests to the issuing CA and it returns the issued certificate to the client. SSL Client Authentication using HTTPS is supported for this. A series of CA backends is already provided in the product. Integration with further CAs is possible. You can also connect to multiple CAs with one certEP instance. The certEP is installed as a Windows service and it is seamlessly integrated with Active Directory. It supports IIS, NDES and CEP/CES enrollment frontends.

By this, also many MDM systems may be connected with a non-Microsoft CA.



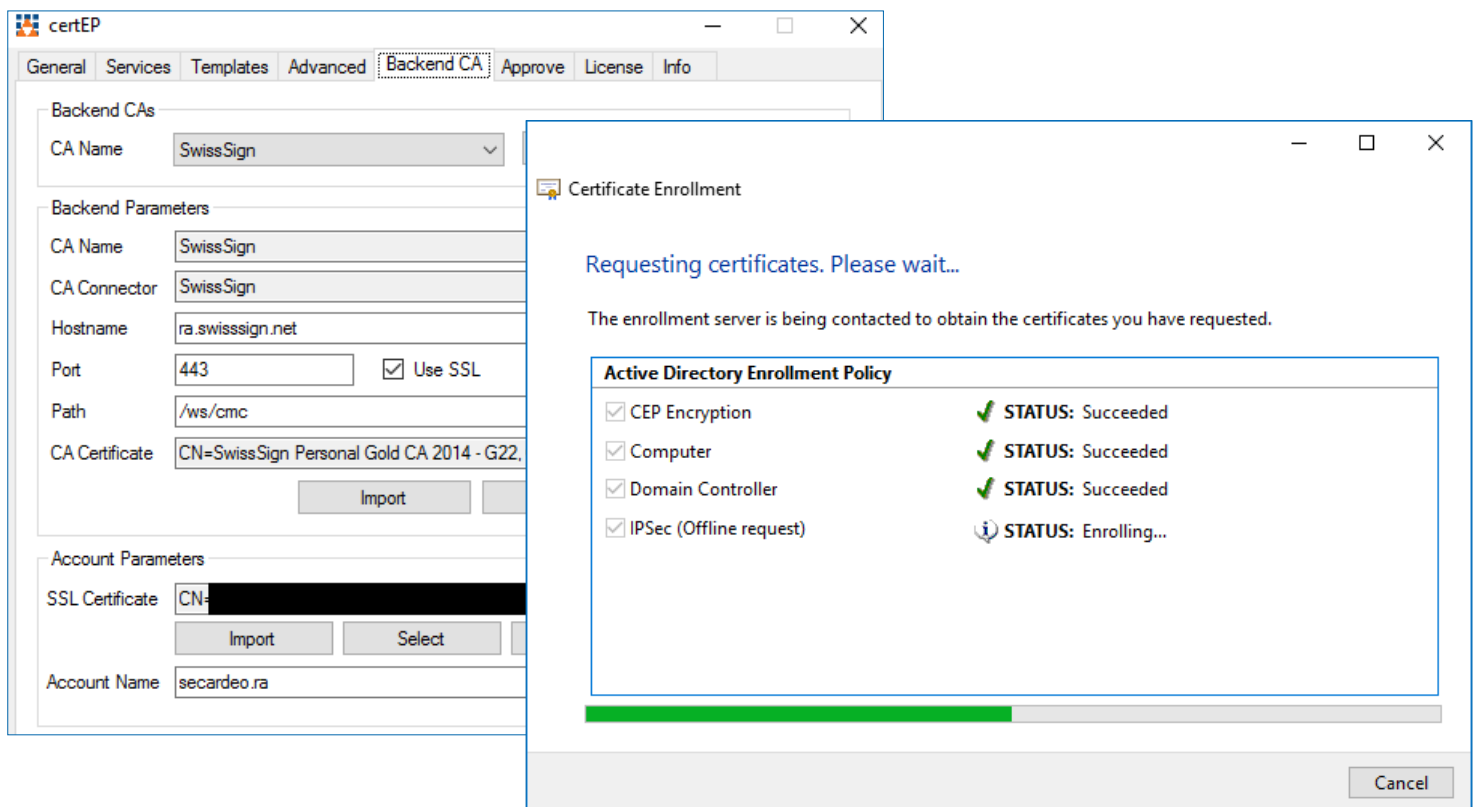
Secardeo GmbH
 Hohenadlstr. 4
 D-85737 Ismaning
 Tel. +49 89 18 93 58 90
 Fax +49 89 18 93 58 99
 info@secardeo.com
 www.secardeo.com

Secardeo certEP is a Certificate Enrollment Proxy for providing X.509 certificates from a non-Microsoft CA using Windows certificate enrollment. The certEP offers the following features:

- Manual and autoenrollment of certificates in Windows Domains via DCOM
- Autoenrollment for Network & Mobile Devices via NDES and SCEP
- Web enrollment via IIS and HTTP enrollment for non-domain clients using CEP/CES
- Local key archival using Key Recovery Agent certificates or remote key archival at the CA
- Certificate event audit and notifications
- Certificate request enhancements, approval, request blocking, publishing, revocation
- Hardware Security Module (HSM) Support

The certEP Enterprise Edition additionally provides

- Multiple Backend CAs
- AD Cross-Forest Enrollment



Operating System:

- Windows Server 2012-2016

HD Requirements:

- Disk Space: 100 MB installation + 50 KB per certificate

Supported Databases:

- MySQL Server v5.7 or higher
- Microsoft SQL Server 2016
- SQLite3

Supported Client OS:

- Windows 7-10
- Windows Server 2008-2016

Supported HSMs:

- Utimaco SecurityServer

Standards:

- X.509 certificates RFC 5280
- PKCS#10 RFC 2986
- CMS with PKCS#10 RFC 3852
- W3C SOAP v1.2
- CMC RFC 5272
- CMP RFC 4210 (subset)

Supported Frontends:

- DCOM AD enrollment
- IIS Web enrollment
- NDES network enrollment
- CEP/CES

Supported MDMs:

- Citrix XenMobile® 10.3 or higher
- VMware AirWatch® 8.4 or higher
- MobileIron Core® 8 or higher

Supported Templates:

- v1-v5 Certificate Templates
- Custom Templates

Supported CA Backends:

- OpenSSL CA
- OpenXPKI
- Dogtag CA
- EJBCA
- IBM z/OS CA
- Nexus CA
- Red Hat Certificate Server
- Windows AD CS
- SwissSign CA
- QuoVadis CA
- HydrantID CA

For further CAs, please ask.