SECARDEO

certEP

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

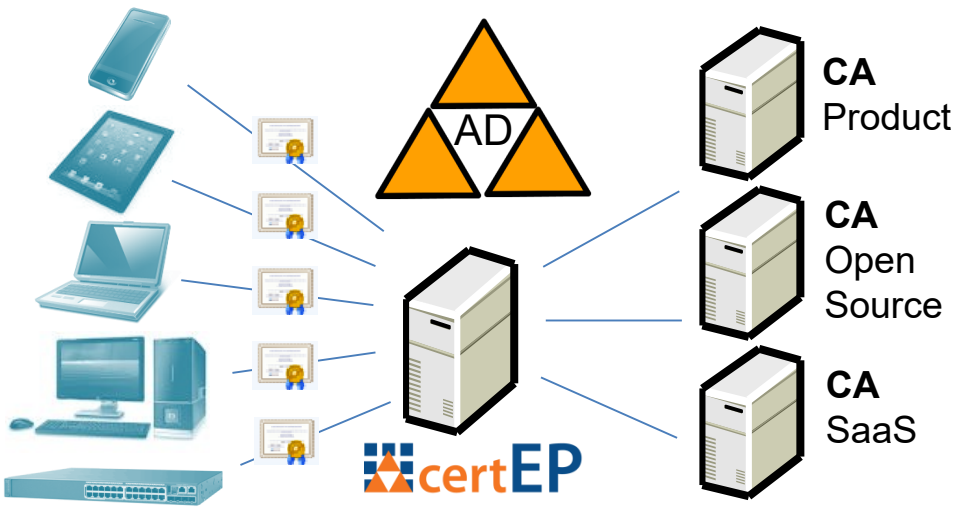
There are environments, where certificates have to be issued to Windows Domains by a non-Windows CA. Either by using an Open Source or vendor CA product or by an external MPKI SaaS provider. By this also globally accepted certificates for S/MIME may be enrolled from a public CA. Mechanisms are needed 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. If a certificate request contains an encrypted private key, key archival is done either locally using KRA certificates or remotely at the CA.
The certEP uses Microsoft certificate template information to process certificate requests. Automatic distribution of private encryption keys to mobile devices is possible using the optional certPush component.

Integrating the certEP

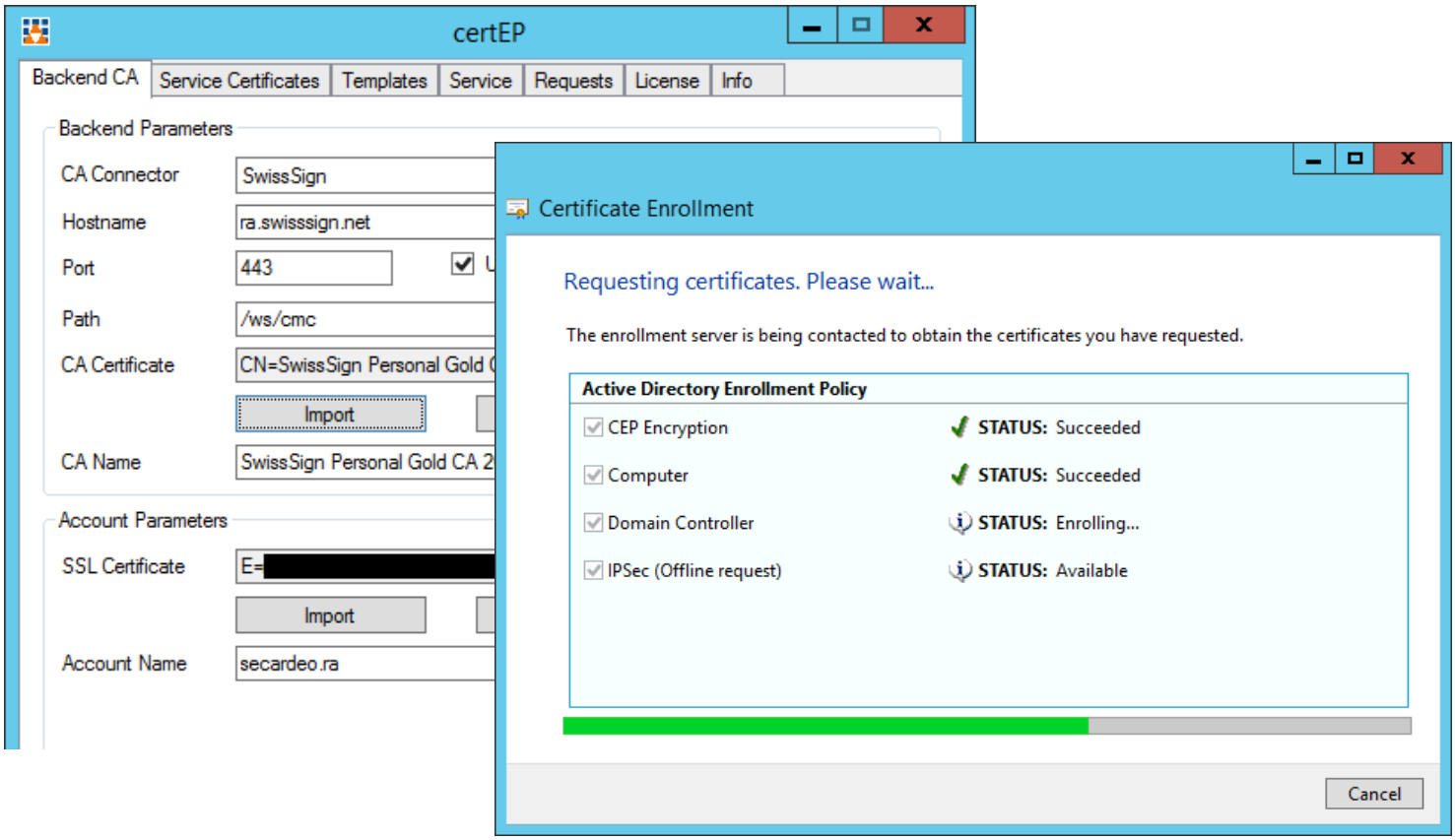
The Secardeo Certificate Enrollment Proxy provides HTTP, SOAP and CMP interfaces for transmitting requests to the issuing CA and it returns the issued certificate to the client. SSL Client Authentication using HTTPS is supported for this. A series of CA backends is already provided in the product. Integration with further CAs is possible.
The certEP is installed as a Windows service and is seamlessly integrated with Active Directory. By this, 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
- Enrollment of mobile device certificates for WLAN 802.1x or VPN Authentication via SCEP
- Local key archival using Key Recovery Agent certificates or remote key archival at the CA
- Supports v1-v5 certificate templates
- Certificate event audit and alerting
- Optional: Certificate request approval
- Optional: Synchronization of CRLs between CA and AD
- certRevoke extension: Auto-revocation and automatic re-enrollment after attribute changes (auto-modification)



Operating System:
- Windows Server 2008 R2
- Windows Server 2012, 2012R2
- Windows Server 2016

Requirements:
- .Net Framework v4
- Visual C++ 2010 Redistributable Package
- available disk space: 100 MB installation + 50 KB for each issued certificate

Supported Client OS:
- Windows 7,8,10
- Windows Server 2008 SP2, R2
- Windows Server 2012, 2012R2
- Windows Server 2016

Standards:
- X.509 certificates RFC 3289
- PKCS#10 RFC 2986
- CMS with PKCS#10 RFC 3852
- W3C SOAP v1.2
- CMC RFC 5272
- CMP RFC 4210

Supported Frontends:
- DCOM AD enrollment
- IIS Web enrollment
- NDES network enrollment
- MDM mobile enrollment

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
- Key Archival with KRA

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 us