certRevoke

Auto-Revocation

Revoke digital certificates

- By a Microsoft CA
- By any CA via certEP
- Users & Computers
- Active Directory monitoring of
  - deleted objects
  - changed attributes
- Consistency
- Improved security
- Save license costs

Revoke digital certificates for AD objects

Automated, consistent, efficient

Certificate revocation

Digital certificates can be revoked before the end of their lifetime. Then the contained public key will no longer be accepted for encryption or authentication. For this, the certificate is put on a certificate revocation list that is signed by the CA or the returned status of an online responder (OCSP) will be “revoked”. There are a couple of reasons to do that. In most cases, this is a manual process done by the certificate manager.

Automatic revocation

Many organizations are using Active Directory (AD) for managing users and computers. Autoenrollment is the efficient way to provide all users with a user or S/MIME certificate and computers with a computer authentication certificate.

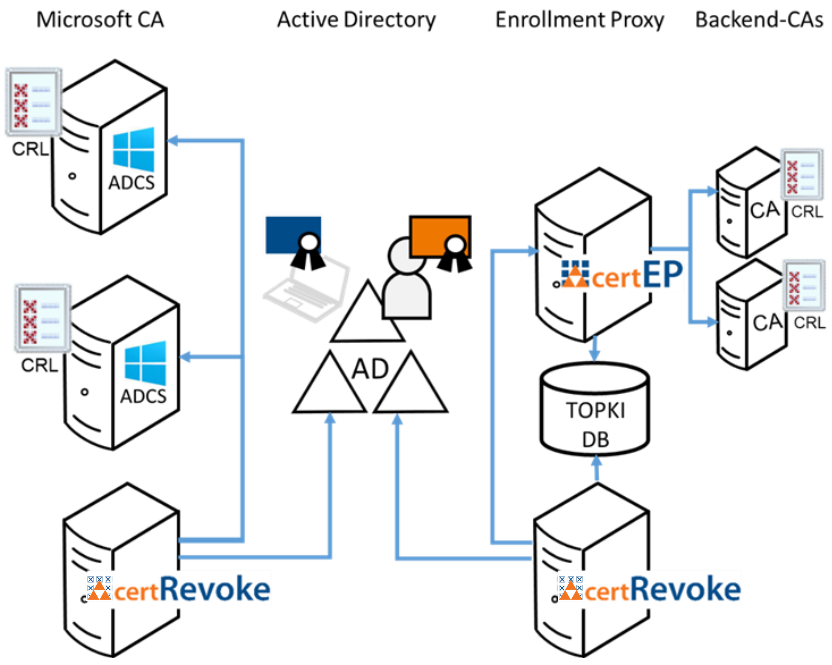
But common phenomenons like employee fluctuation or equipment replacement lead to situations where hundreds or thousands of valid certificates still exist but the contained subject or object has disappeared. This leads to an inconsistent state an it can have impact on the security, because the keys could still be used. Furthermore you will have to pay for the still valid certificates to your PKI service provider.

Automatic re-enrollment

Another typical scenario is that attributes of an AD object change. For example the surname and e-mail address after marriage or network addresses and names. In such a situation, the automatic revocation of the old certificate will initiate an automatic re-enrollment after startup or login of the user. The new certificate that contains the changed attributes can immediately be used.

Integration & monitoring

certRevoke is a Windows service that integrates with Active Directory and monitors the desired AD tree and object types for deletions or attribute changes. It integrates well with a Microsoft CA (ADCS) or Secardeo certEP.

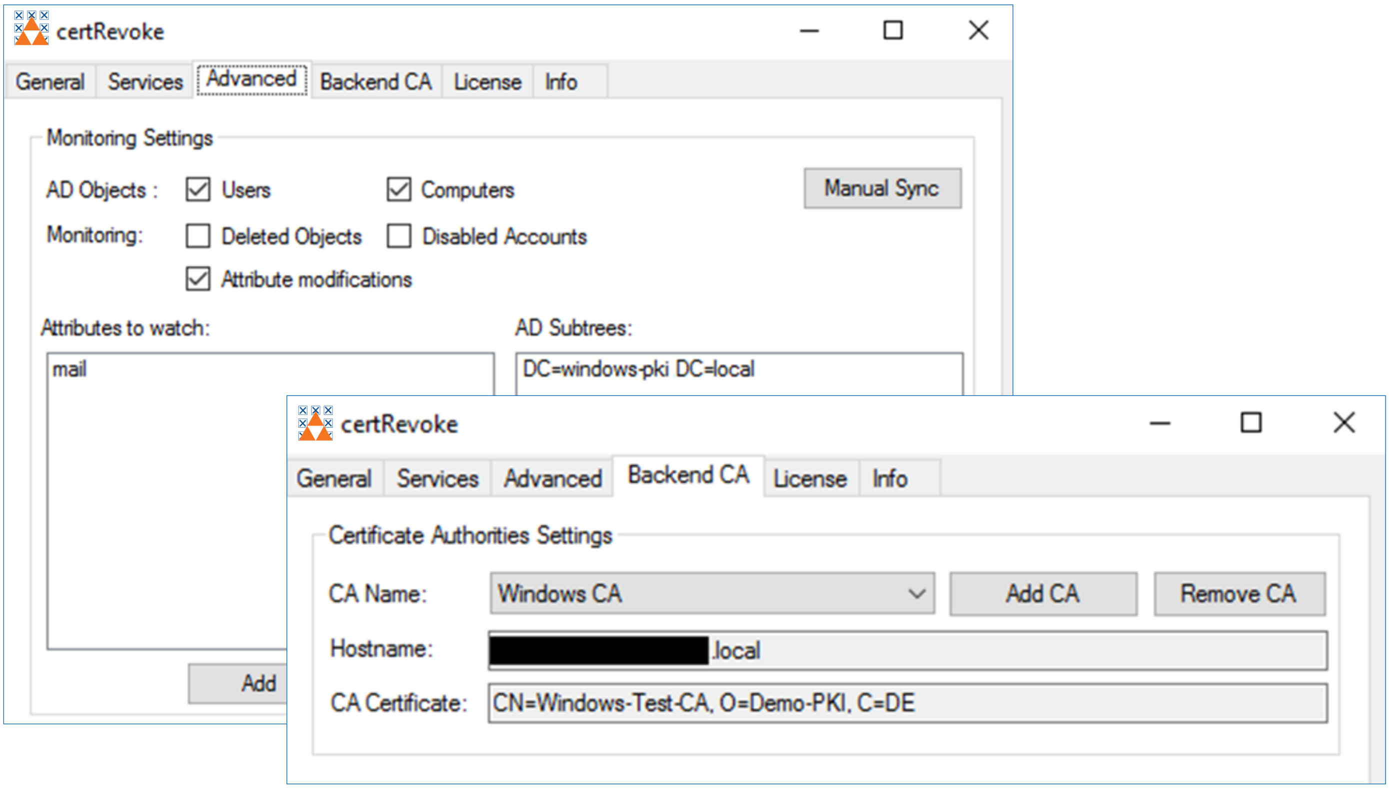


Secardeo GmbH
Hohenadlstr. 4
D-85737 Ismaning
Tel. +49 89 18 93 58 90
Fax +49 89 18 93 58 99
info@secardeo.com
www.secardeo.com

certRevoke

Secardeo certRevoke is an auto-revocation service for Active Directory that automatically submits revocation requests for a deleted or changed object to the CA. certRevoke offers the following features:

- Support of Microsoft CA (ADCS) and Secardeo certEP
- Multiple CA support
- Monitoring of user and machine objects in AD
- Flexible control of attributes to monitor
- Filter for specific OUs in the AD tree
- Configurable monitoring interval
- Notification service



Monitoring Settings

AD Objects : ☑ Users ☑ Computers

Monitoring: ☐ Deleted Objects ☐ Disabled Accounts

☑ Attribute modifications

Attributes to watch: mail

AD Subtrees: DC=windows-pki DC=local

Certificate Authorities Settings

CA Name: Windows CA

Hostname: [redacted].local

CA Certificate: CN=Windows-Test-CA, O=Demo-PKI, C=DE

Operating System:
- Windows Server 2016-2019
- Microsoft® .NET Framework 4.0

HD Requirements:
- Disk Space: 50 MB

Supported certEP Databases:
- MySQL Server v5.7 or higher
- Microsoft SQL Server 2016 or higher
- SQLite3

Standards:
- X.509-Certificates and CRLs RFC 5280
- PKCS#12: Personal Information Exchange, RFC 7292
- PKCS#7: Cryptographic Message Syntax (CMS),RFC 5652

Supported Backend CAs:
- Microsoft ADCS Enterprise CA
- Secardeo certEP with:
- Dogtag CA
- OpenXPKI
- SwissSign
- Windows CA

For further CAs, please ask.

SECARDEO