



true-CA

Introduction

1. true-CA

Standalone, multi-tenant Certificate Authority

- [Introduction](#)

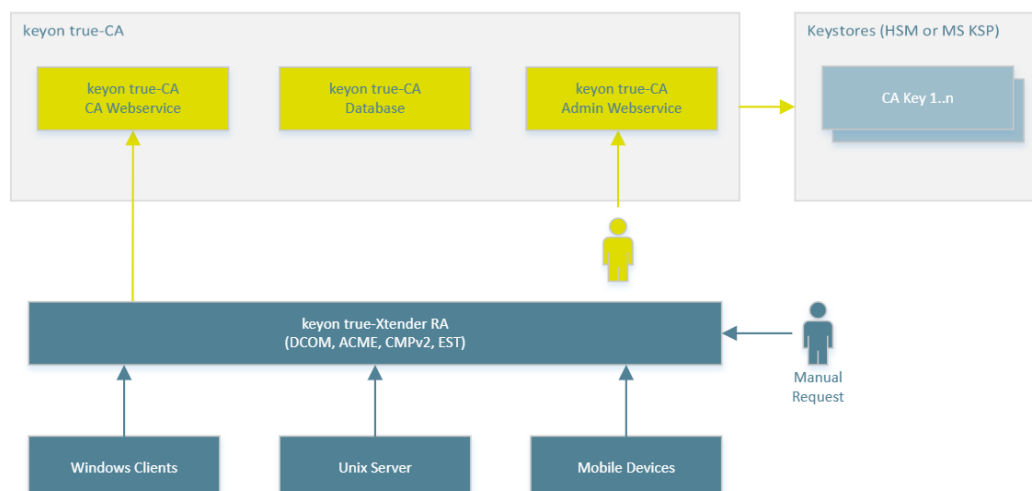
2. Introduction

3. true-CA Features

The keyon - true-CA is a standalone, multi-tenant certificate authority that allows you to use multiple CAs on a single server.

- Operating and managing multiple CA hierarchies on a single system (Microsoft IIS Webserver)
- Can easily be clustered for availability and performance
- Easily and quickly deploy and manage new Root CAs and Issuing CAs
- CA private keys may be stored on Hardware Security Modules (HSM) or as Softtoken (Microsoft Software KSP)
- Supports multiple certificate profiles (blueprints) per CA
- Supports multiple CRL profiles per CA
- Supported key algorithms are RSA, ECDSA_P256 and ECDSA_P384.
(*Post-Quantum algorithms: ML-DSA available for end-entity certificates, support for CA certificates on the roadmap)
- Fully integrated in keyon true-Xtender Registration Authority
- RA provided enrollment protocols: Microsoft DCOM, ACME, CMPv2 and REST API

4. Component Overview



Main components are:

- CA web service (used by CA agent)
- Admin Web Service (used by CA administrator)
- CA database

5. Technical Details

The true-CA service runs as an application in IIS and offers a CA web service and an administration web service. The true-CA CAConnector enables its use via the keyon true-Xtender Registration Authority, the keyon true-Xtender CAConnector Service, and the keyon true-Xtender Autoenroll PKI or in a standalone scenario.

There are plenty of options (by PowerShell scripts) to create new CAs (CA certificate generated as softtoken or in HSM) including certificate blueprints and CRL blueprints. The trueCAAdminUtil provides functionality for further administration.

true-CA Service uses CA certificates which are stored in Windows Certificate Store. This allows the Certificate private key to be stored on a HSM (e.g. for Thales SafeNet HSMs to be used with Safenet KSP, a CNG provider) as well as a Softtoken certificate with the protected key in the file system.

6. Component Details

