

Certificate Enrollment- and Signing Services for the Cloud

A behind-the-scenes presentation of a successful

cooperation between   

Introduction

- Based on our experience and the request from the market we would like to introduce a possible solution of a certificate enrollment and a digital signature service in the cloud which could make your life easier
- This presentation is a behind-the-scenes look of trustworthy cloud service providers and will focus on the end user experience and particular security measures applied to the respective services

PKI as a Service – Motivation

Today, more and more internal systems and applications rely on certificates for securing communication channels and for authentication purposes. Installing and operating a PKI infrastructure however is challenging, especially if a high level of security is requested:

- Dedicated secured PKI systems with expensive hardware security modules (HSM) for protecting the CA keys
- Availability of the critical components and contingency plan
- Administration of the PKI and separation of roles
- Keeping track of issued and expiring certificates, auditing

PKI as a Service – Solution

PKI as a service enables automated issuance and management of certificates on Windows domain and non-domain joined Systems, Mac OS, Linux/Unix, iOS, Android and Windows Mobile without the need to setup and operate a corporate PKI. Comprehensive cockpits and reports provide insight into the progress of certificate issuance processes or system states.

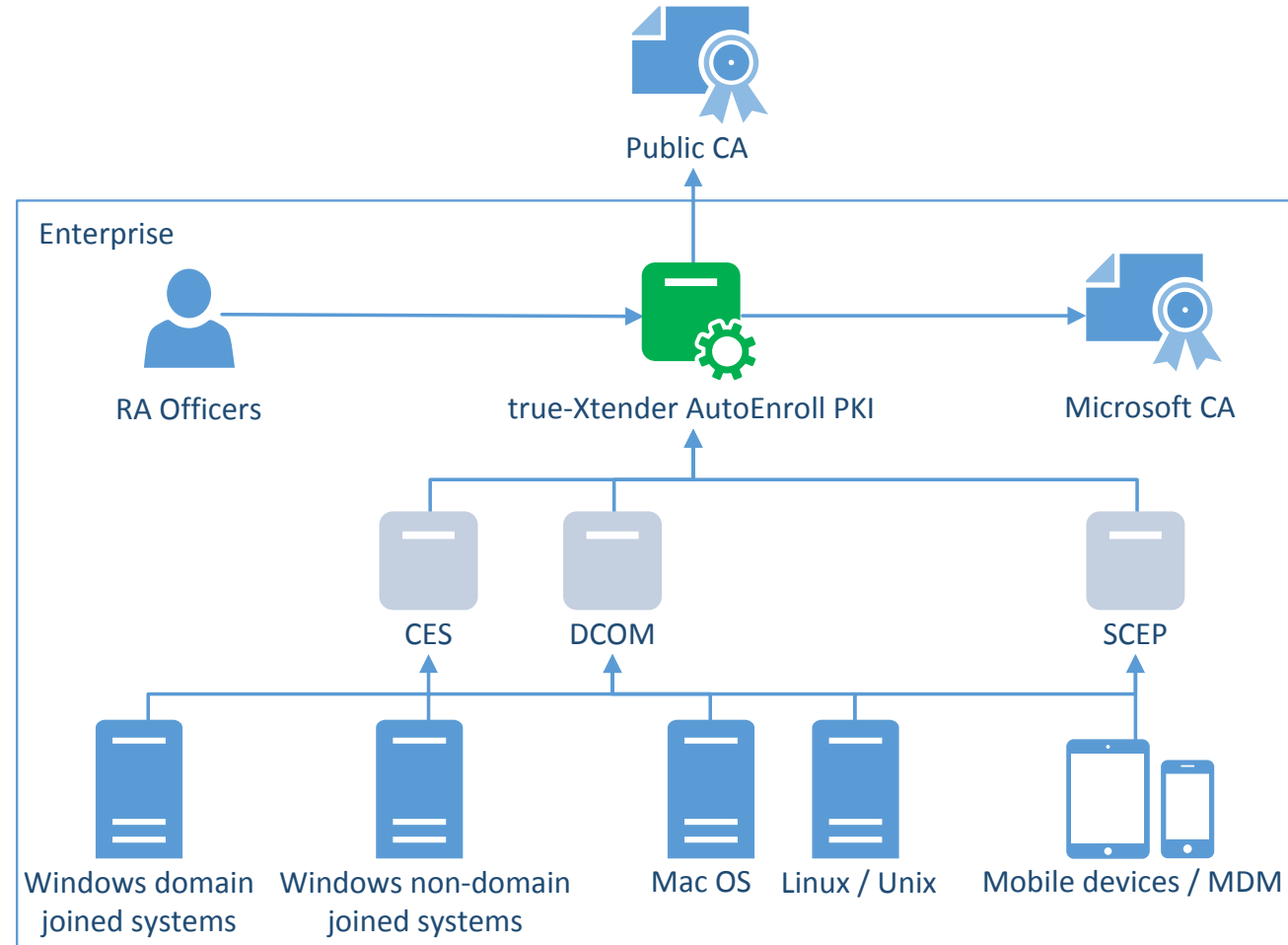
PKI as a Service – Architecture

Certificate Issuance:

- 1) Public CAs
(Quovadis, ...)
- 2) Internal CA
(Microsoft CA)
- 3) True-Xtender RA
(Cross-AD-Forest enrollment)

Enrollment Interfaces:

- 1) MS CEP/CES Web Services
- 2) DCOM – WCCE
(Windows Client Cert. Enrollment)
- 3) SCEP
(Simple Cert. Enrollment Protocol)



PKI as a Service – Principles

- Service provider hosts and operates the PKI with appropriate security measures such as using a HSM for CA key protection
- Enrollment Connector component is installed on-prem
- Certificates are issued automatically using readily available enrollment APIs.
- Authentication and authorization of clients is handled with information available in the enterprise (AD, DB, IAM)
- Authentication of clients can be based on Kerberos or using other credentials for e.g. on-domain joined systems
- Optional archival of client keys takes place on-prem

PKI as a Service – Cockpit and Reports

keyon true-Xtender Autoenroll PKI

Licensed for: Keyon Test
Logged in as: Administrator@kxap.test

Status: Pending Completed Failed show completed/failed from last 20 days.

0 Pending, 4 Completed, 0 Failed, 4 Total

ID	Account	Enroll Type	Certificate Profile	Status	Processed
4178	demotestuser1	Create	TXAPUser2	Completed	19.08.2016 14:15
4179	demotestuser1	Create	TXAPUser2	Completed	19.08.2016 14:35
4180	demotestuser1	Create	TXAPUser2	Completed	19.08.2016 14:42
4181	demotestuser1	Create	TXAPUser2	Completed	25.08.2016 11:12

keyon true-Xtender Autoenroll PKI

Licensed for: Keyon Test
Logged in as: Administrator@kxap.test

Certificate Issuance Information

Certificate Profile	License	Issued Total	Revoked Total	Pending*	Issued*	Revoked*
TXRA Test Device	Valid	14	11	0	0	0
SwissSign User	Valid	3	1	0	3	1
QuoVadis User	Valid	6	2	0	3	2
TXAP Test Computer	Valid	10	5	0	0	0
TXAP Test User	Valid	32	22	0	4	3
TXAPUser2	Valid	10	7	0	4	4
TXAPUser3	Valid	31	2	0	0	0

Tasks processed between: 06.08.2016 and 06.09.2016 Show Details Include disabled certificate types

Run connectivity check

Database Status: Autoenroll PKI database connection OK

LDAP Status: LDAP Connection Kerberos OK, LDAP Connection Password OK, LDAP Connection Certificate OK

Microsoft CA Status: Microsoft CA 'DC01TXAPCA01' connection OK

Microsoft CA 2 Status: Microsoft CA 2 'SVR01TXAPCA02' connection OK

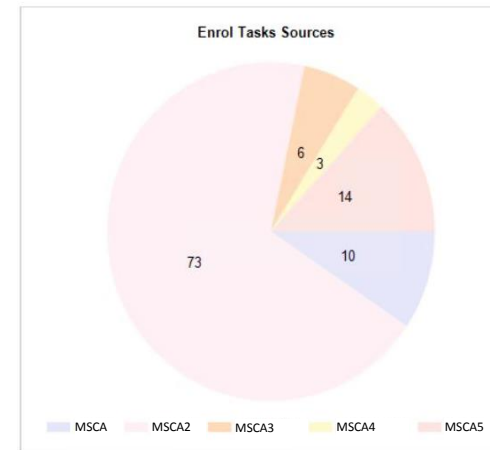
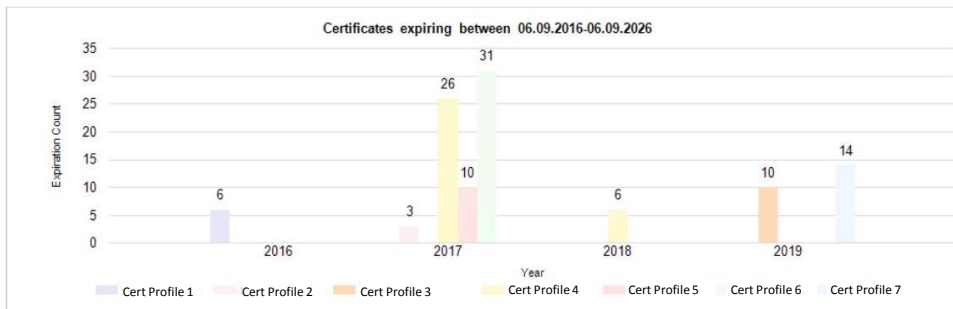
QuoVadis CA Status: TLEWS connection OK

SwissSign CA Status: SwissSign CA connection OK

True-Xtender RA Status: True-Xtender RA connection OK

Autoenroll PKI - Certificate Issuance and Expiration

true-Xtender Autoenroll PKI - licensed for Keyon Test



PKI as a service – Solution Challenges

- Only few components should be installed on-prem
- Different existing enrollment interfaces must be supported
- Multiple internal and external CAs must be supported
- Support for triggered updates without the need for user action (e.g. name change due to marriage)
- Key archival on-prem and secure key recovery processes
- Automatic lifecycle management, i.e. revocation of certificates issued to inactive users or computers
- Prevent enrollments “going wild” and inflicting costs

Signature as a service - Motivation

- Digital signatures are trending in B2B, B2C and C2B scenarios
- The legal requirements for qualified signatures are usually only met using Smart Cards
- Managing physical tokens in an enterprise environment can be challenging and also limits the usage scenarios

The image displays three screenshots of digital signature verification interfaces, each showing a signature validation status window.

Antragsteller: The interface shows a signature by Martin Christinat (Qualified Signature) dated 2016.04.12 14:10:34 +02'00'. The signature is valid, signed by Martin Christinat (Qualified Signature) with email <christinat@keyon.ch>. The document has not been modified since this signature was applied, and the signer's identity is valid.

Firmenvertretung¹: The interface shows a signature by Martin Christinat (Qualified Signature) dated 2016.04.12 14:11:29 +02'00'. The signature is valid, signed by Martin Christinat (Qualified Signature) with email <christinat@keyon.ch>. The document has not been modified since this signature was applied, and the signer's identity is valid.

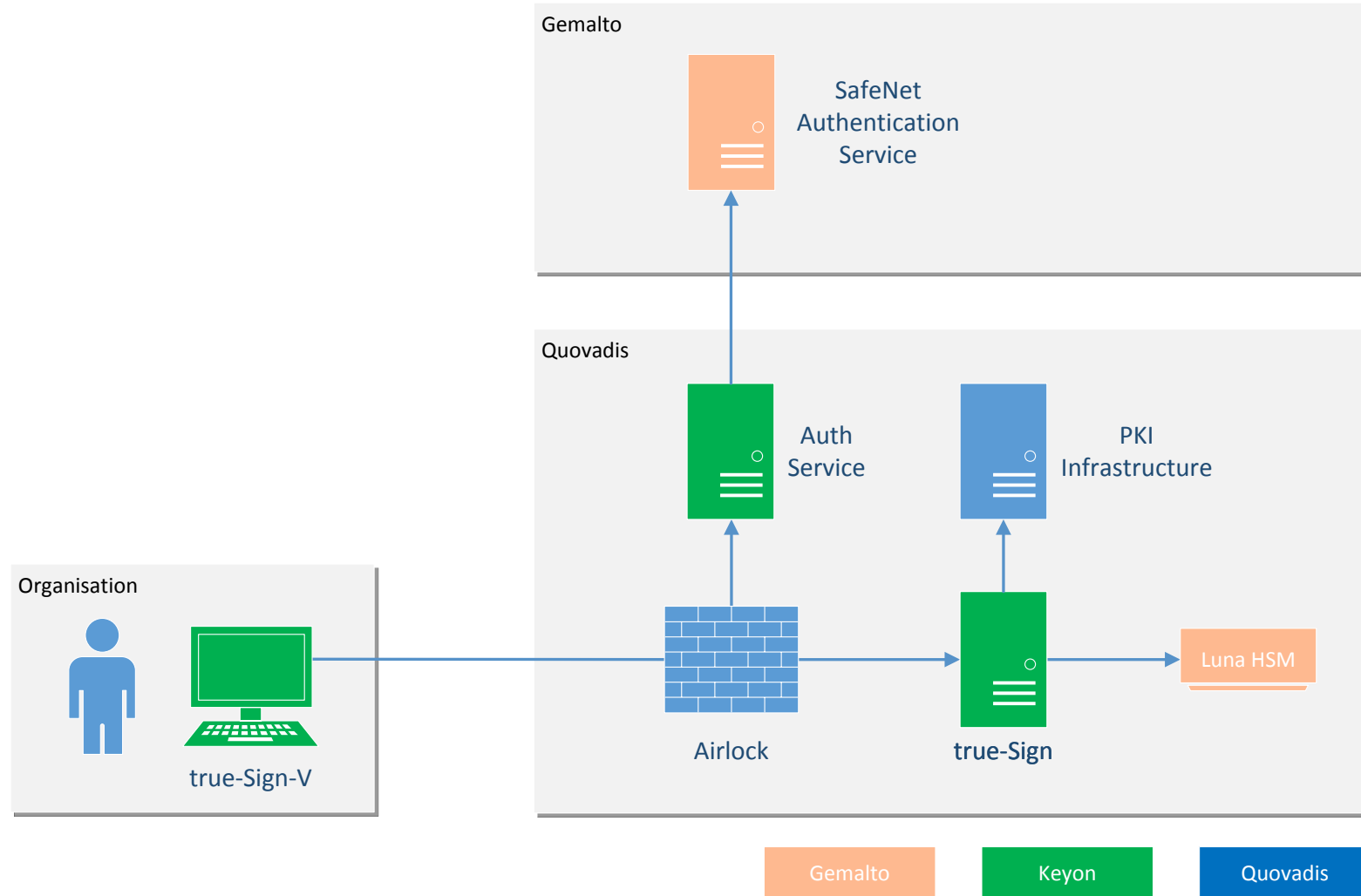
QuoVadis Trust: The interface shows a signature by Martin Christinat (Qualified Signature) dated 2016.04.12 14:11:29 +02'00'. The signature is valid, signed by Martin Christinat (Qualified Signature) with email <christinat@keyon.ch>. The document has not been modified since this signature was applied, and the signer's identity is valid.

Signature as a service - Solution

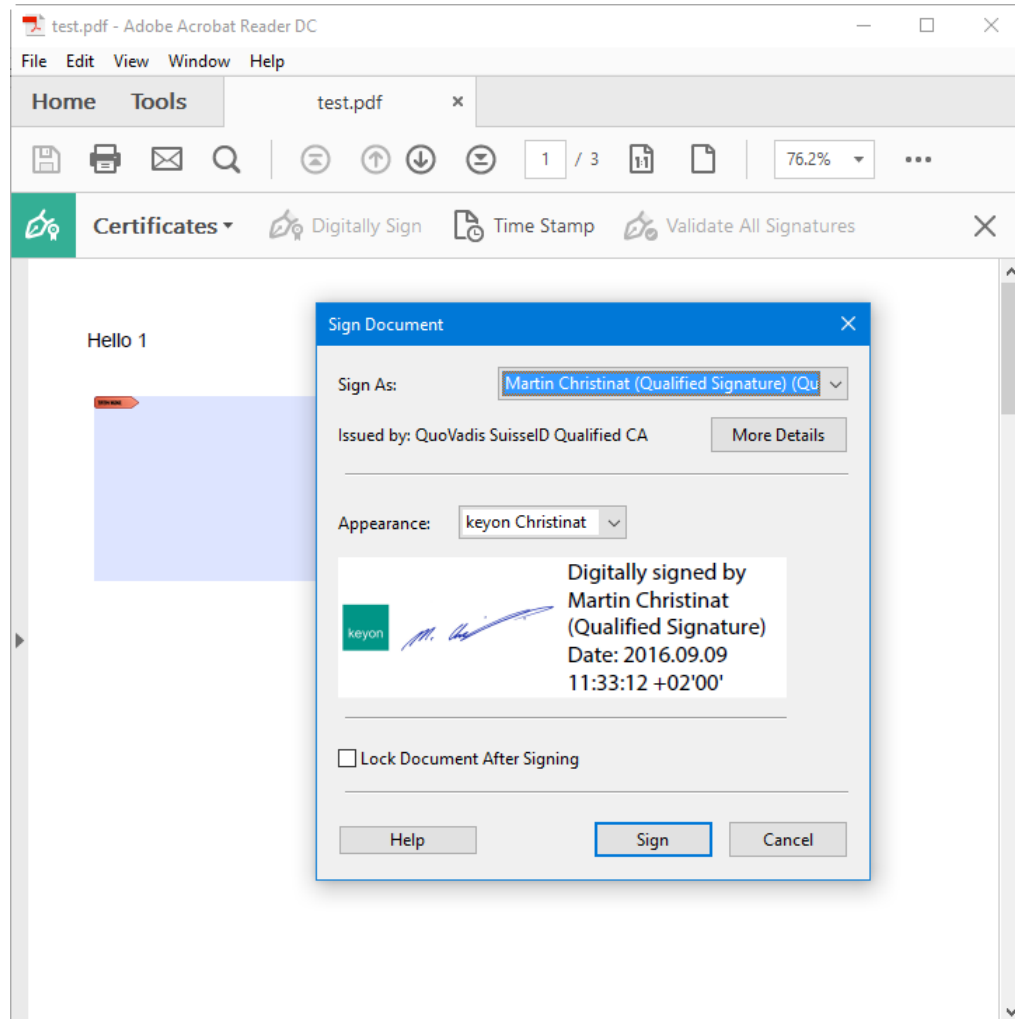
Signature as a service enables companies or individuals to easily apply advanced or qualified digital signatures without the need of installing or managing Smartcards or USB tokens.

- Apply digital signatures using any standard applications on Microsoft Windows (Office, Adobe Reader, etc.)
- Support strong authentication of users
- Private signature key is generated and used only in a certified Hardware Security Module located at the service provider
- Support digital signatures according to ZertES, EIDI-V, GeBüV, Adobe AATL, etc. and time stamping services.

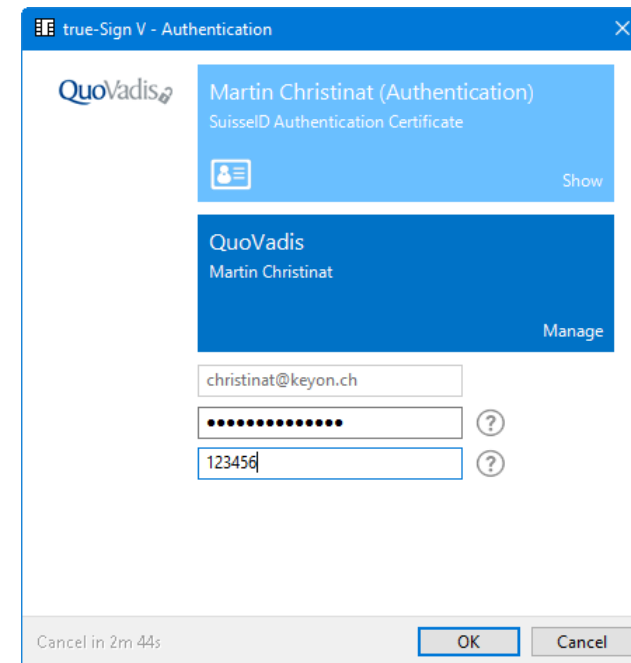
Signature as a service - Architecture



Signature as a service – Client View Step 1

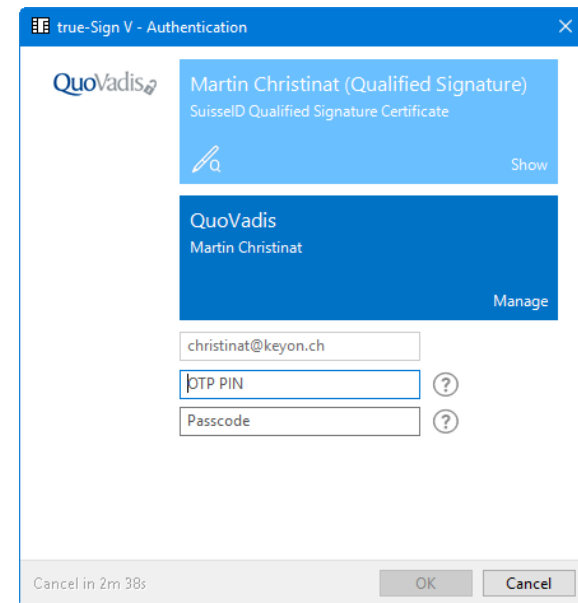
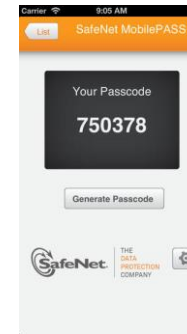


Authentication
(once per session / hour)



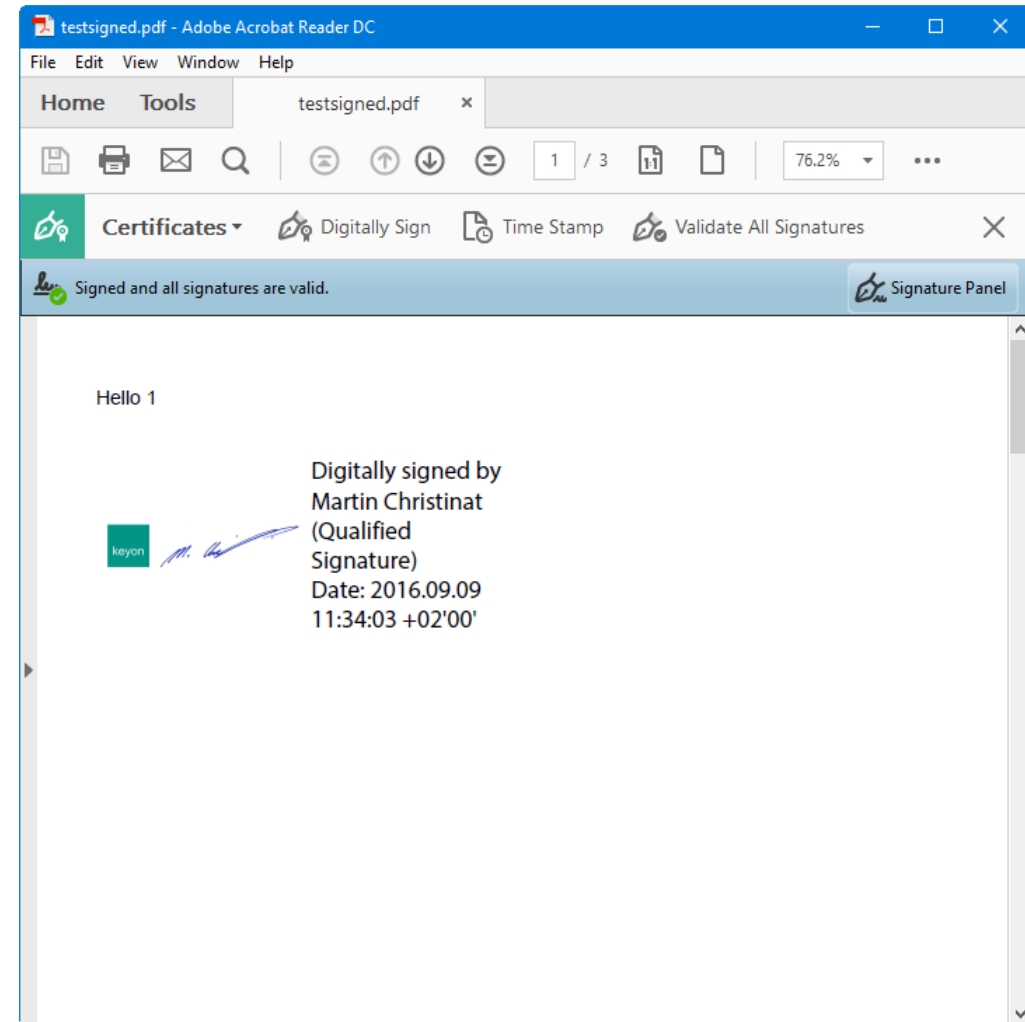
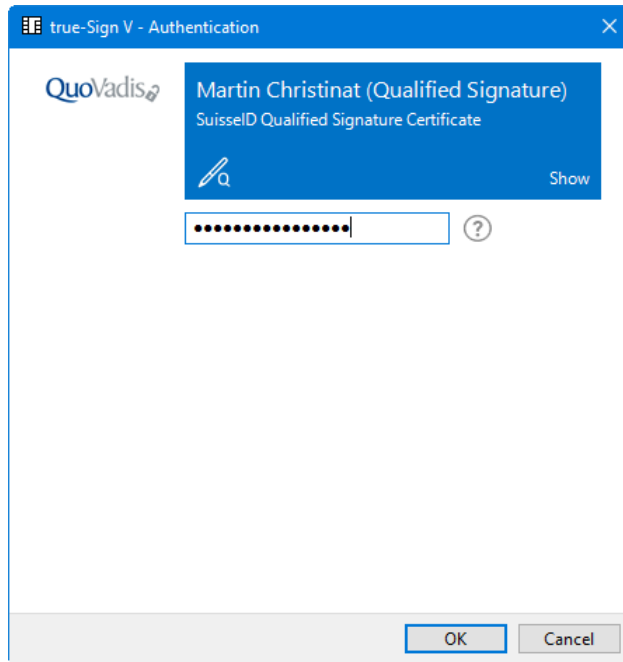
Signature as a service - Authentication

- Strong two-factor authentication with PIN and generated passcode to verify identity of the caller
- Smartphone app or physical OTP token available for generating passcode
- Authentication is validated using a cloud based service



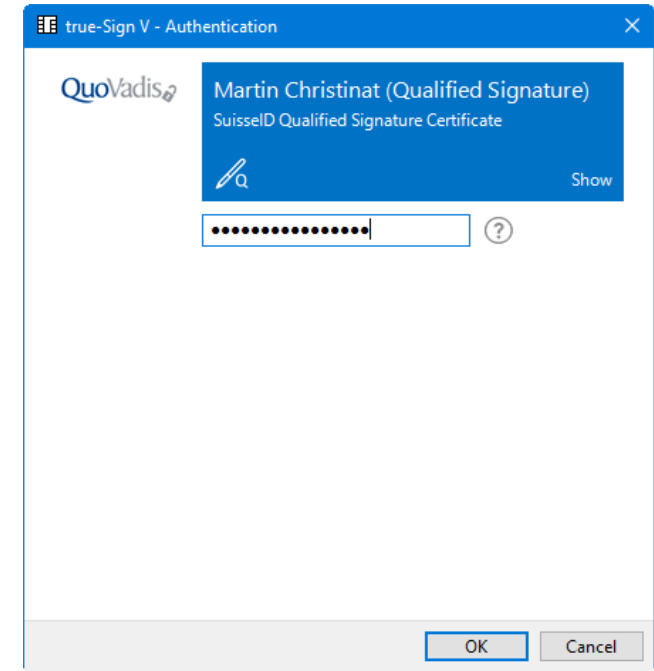
Signature as a service – Client View Step 2

Authorization (caching configurable)



Signature as a service - Authorization

- Password for using the private key is independent of authentication password and only transmitted in an end-to-end encrypted message from the client to the signature service
- Operations with private key take only place on a certified HSM and require the correct password to be presented
- Too many tries with wrong password will delete the private key permanently



Signature as a service – Solution Challenges

- Meet legal requirements for qualified signatures (e.g. authentication of the private key owner, ensuring that only the owner can authorize the use of the private key)
- Ensuring the security of the solution in corporate environments that break up TLS
- Limiting where the client can be used and which applications can create signatures
- Supporting all the different APIs on the client that applications use (CSP, KSP, PKCS#11)
- Supporting Terminal Services (RDP, Citrix) Scenarios

Signature as a service – Advanced Use Cases

Code Signing

- Security features in modern OS and applications allow restricting the execution of code, scripts and macros based on digital signatures
- Keeping the private key secure is very important and usually conflicts with the fact that more than one person and even automated build servers need to digitally sign the code
- The service shown can provide a secure solution for implementing this Use Case

Signature as a service – Advanced Use Cases

Clientless signing in workflows

- Since the signature is done on the HSM of the service provider, it is possible to integrate the signature solution into web based workflow systems (Depends on legal framework!)
- The workflow system prepares the data to be signed and redirects to a page hosted by the service provider which asks for the user credentials and creates the signature. The signature is then returned to the workflow provider using a redirection and can be embedded into the document.

Thank you for your attention

Q&A