# 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 live 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.

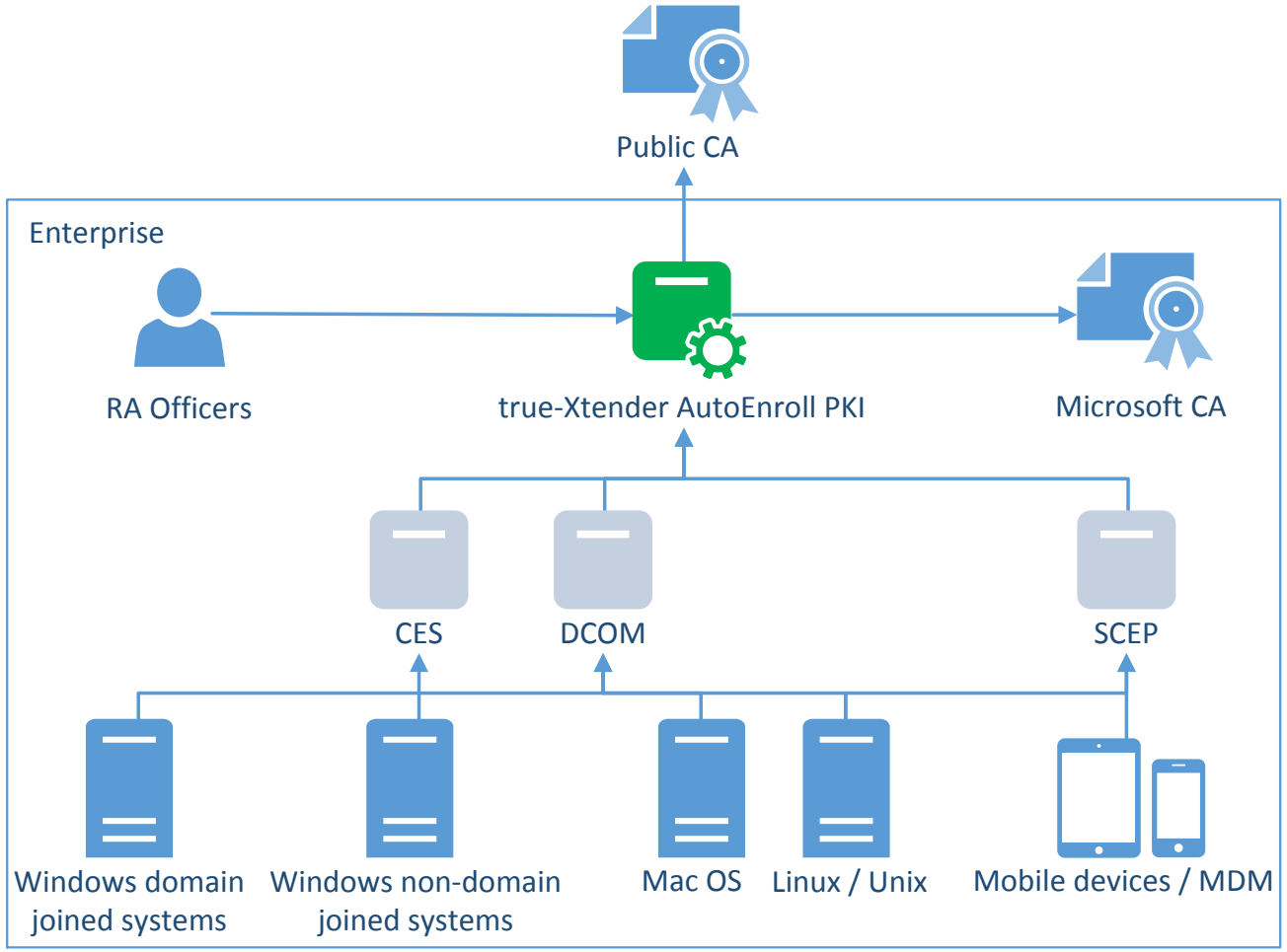
# PKI as a Service – Architecture

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)

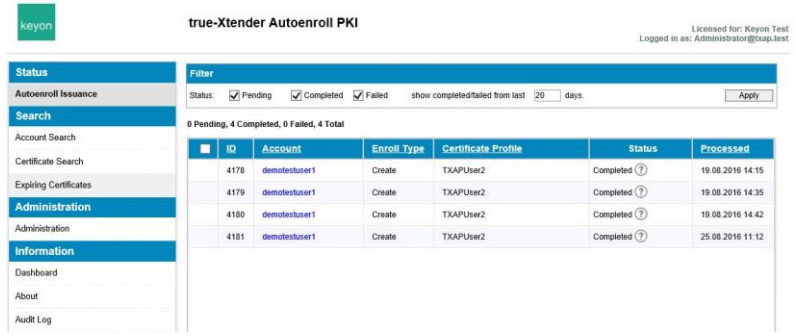


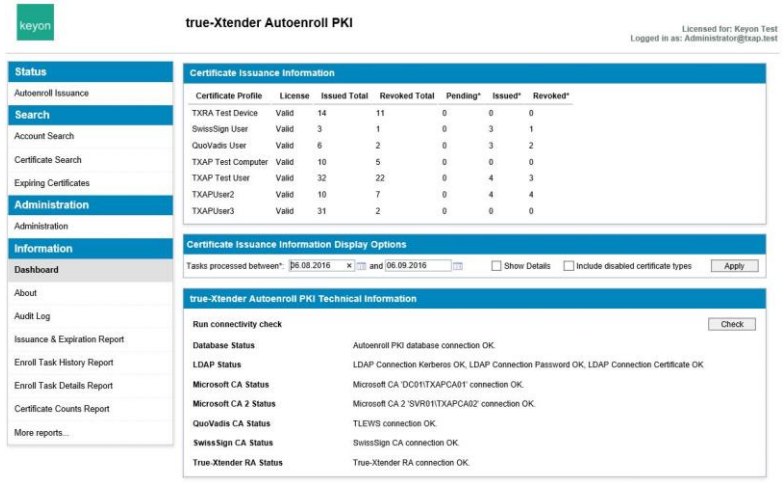

gemalto keyon QuoVadis

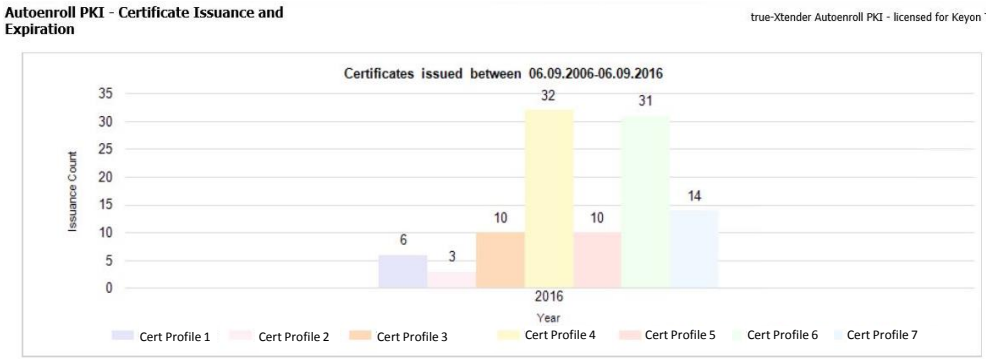
# PKI as a Service – Principles

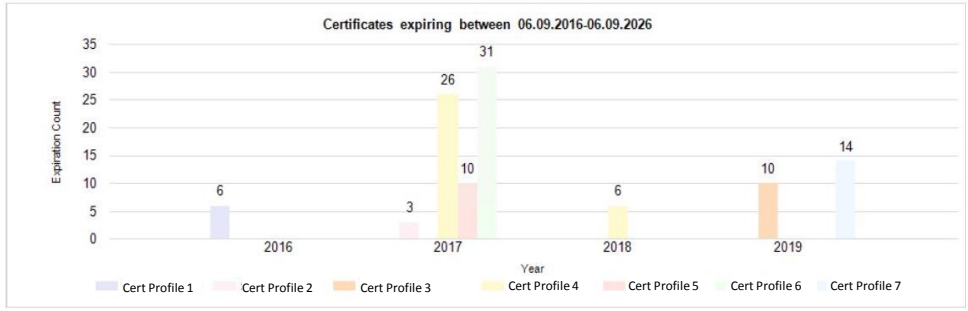
- Service provider hosts and operates the PKI with appropriate security measures such as using a HSM for CA key protection
- Enrollment Connector component is installed on-prem
- Certificates are issued automatically using readily available enrollment APIs.
- Authentication and authorization of clients 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

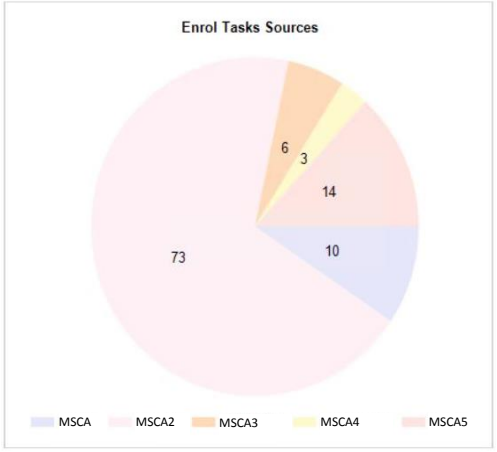
# PKI as a Service – Cockpit and Reports



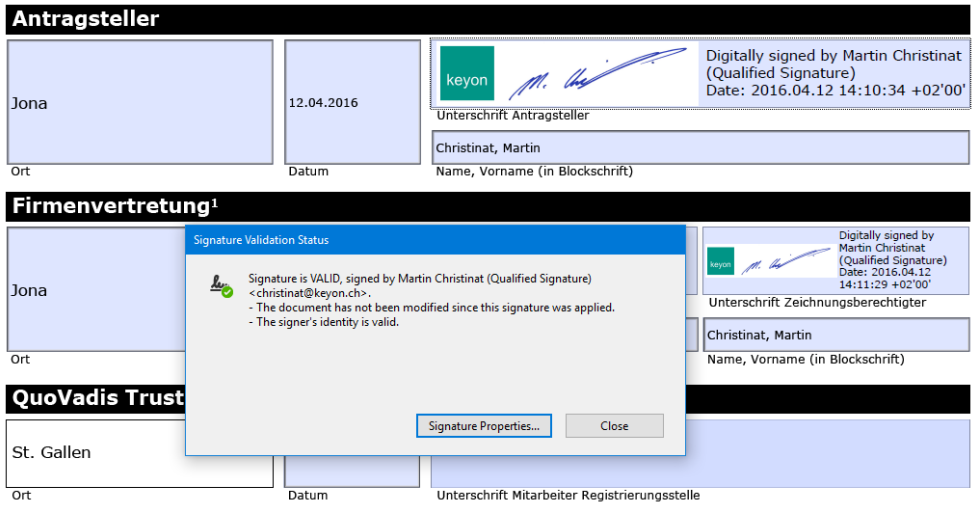



# PKI as a service – Solution Challenges

- 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

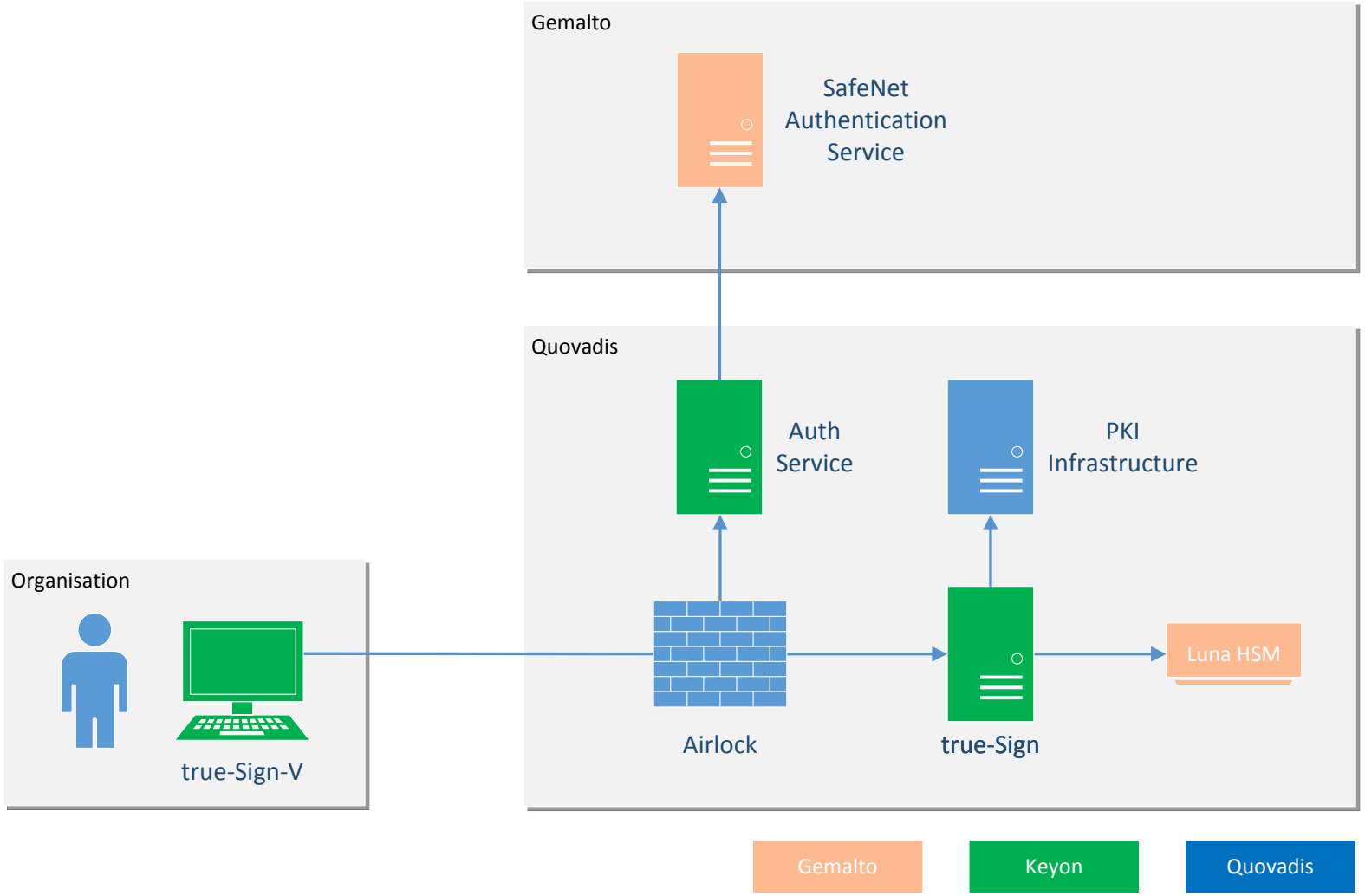


# Signature as a service - Solution

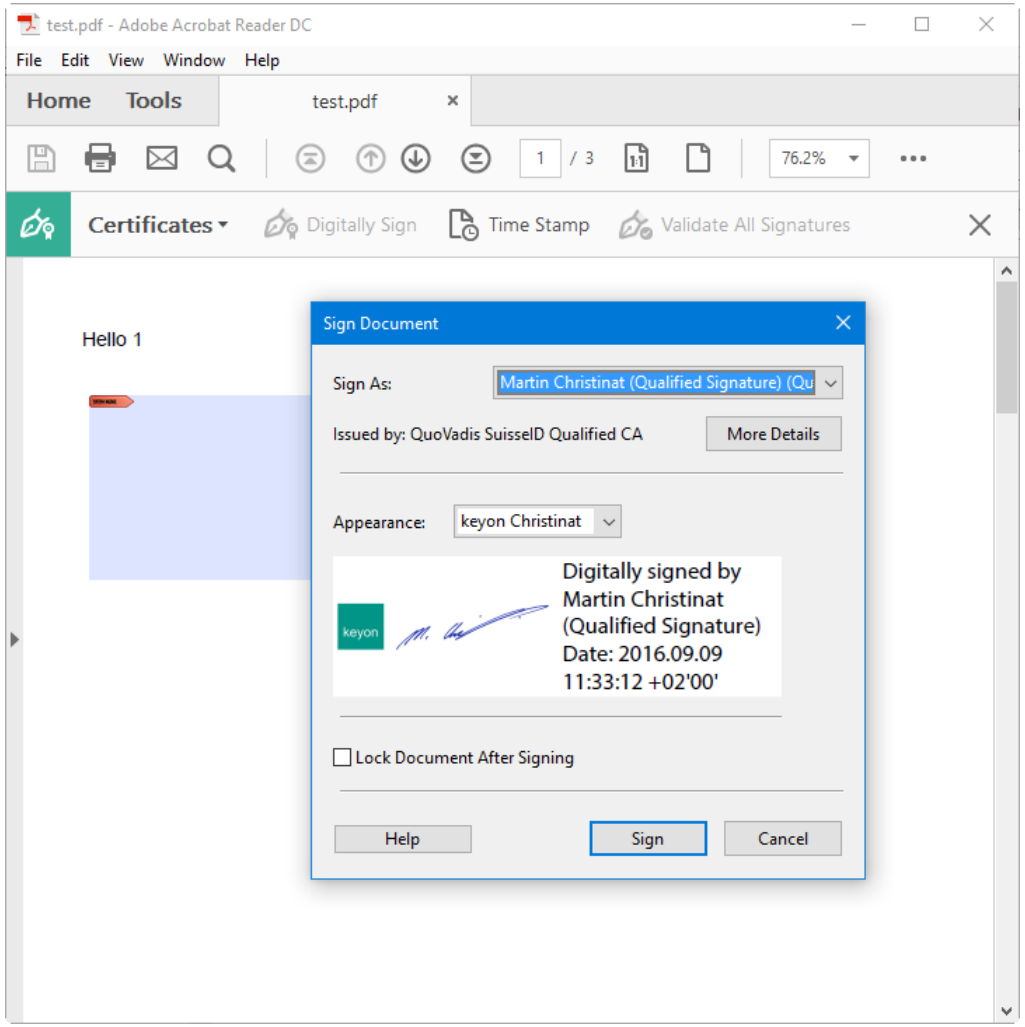
Signature as a service enables companies or individuals to easily apply advanced or qualified digital signatures without the need of installing or managing Smartcards or USB tokens.

- 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, ElDI-V, GeBüV, Adobe AATL, etc. and time stamping services.

# Signature as a service - Architecture

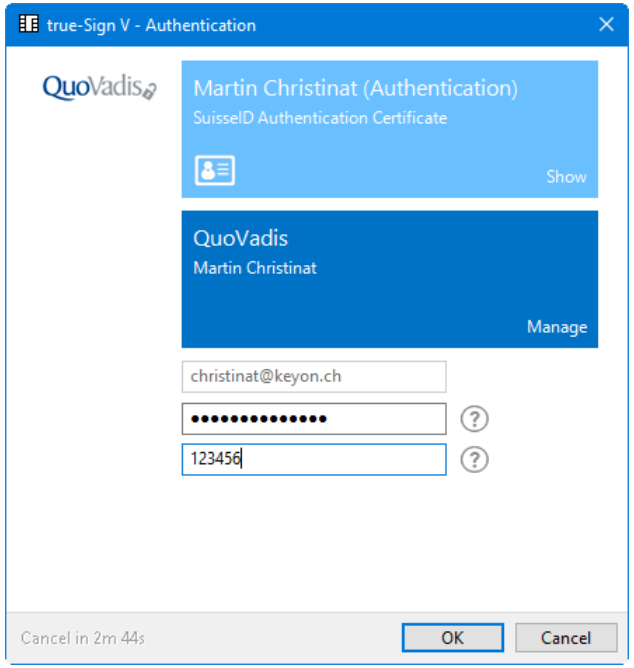


# Signature as a service – Client View Step 1



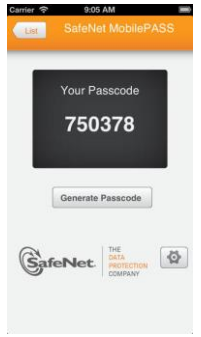

## Authentication

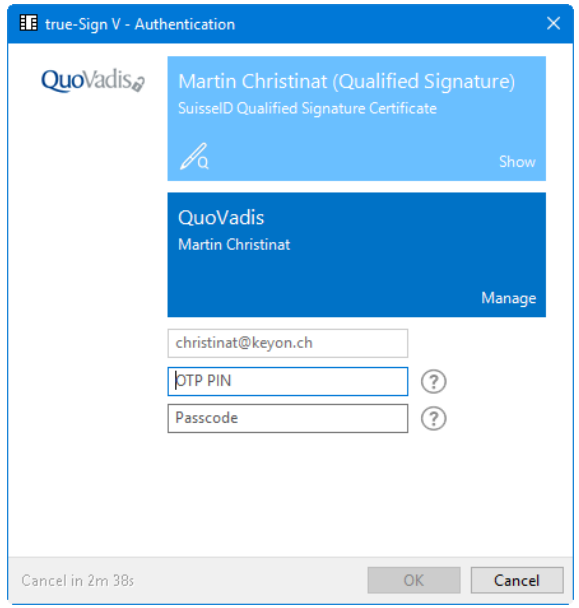
(once per session / hour)



# 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

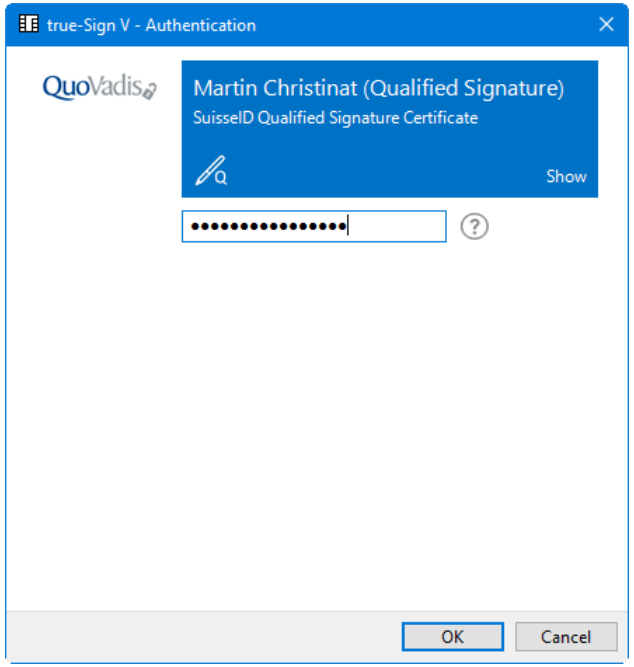


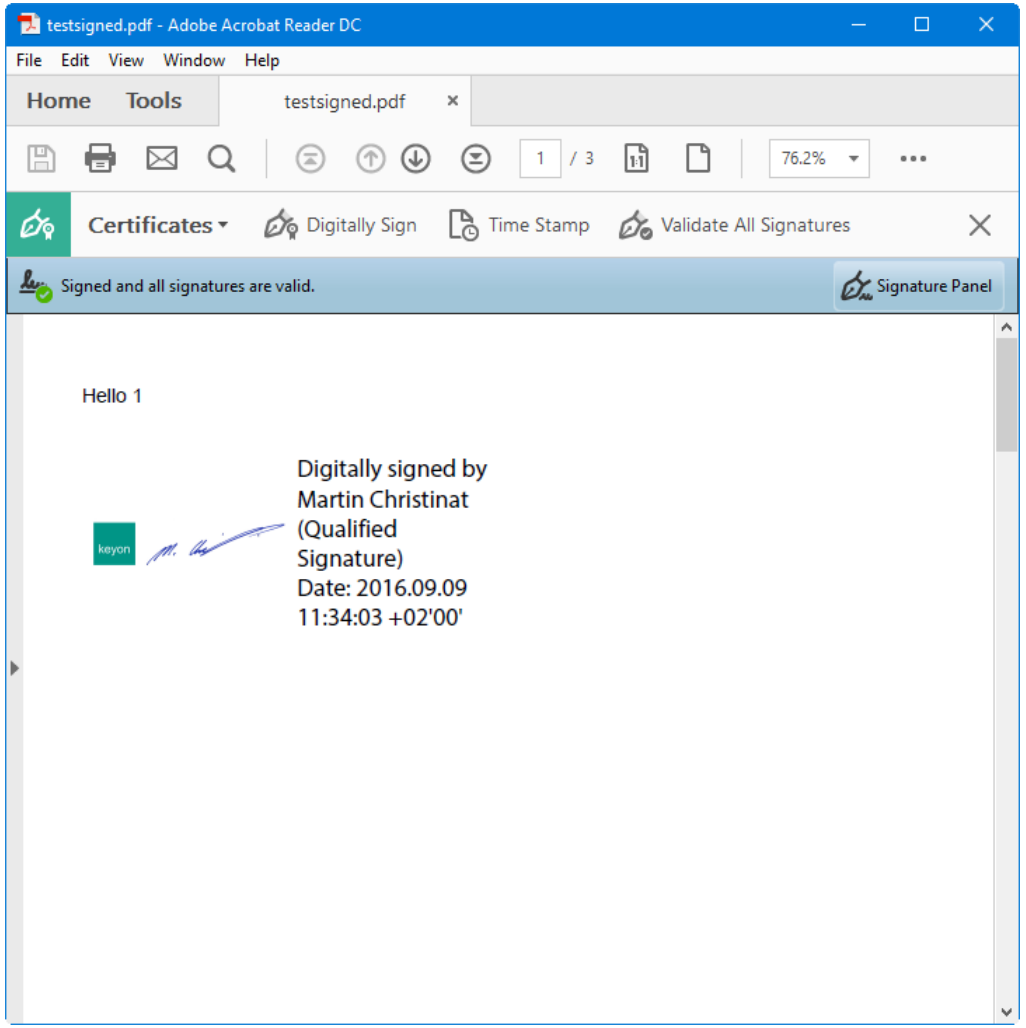



# Signature as a service – Client View Step 2

## Authorization

(caching configurable)

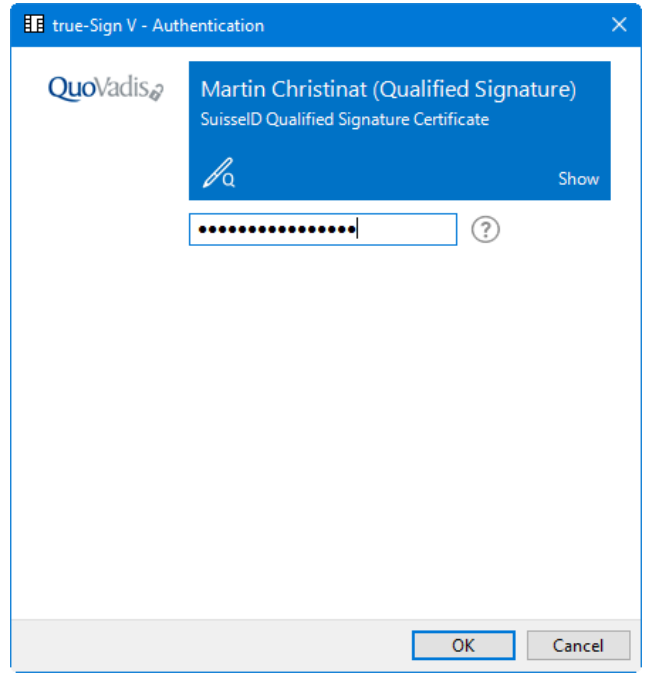



gemalto keyon QuoVadis

# 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

gemalto keyon QuoVadis