keyon

true-Sign V

Business Signatures (PDF, Office, etc.)
Code-Signatures (Applications, Office Macros, PowerShell scripts)
Secure Key Management in FIPS HSMs

September 2019, V1.0, eberhard@keyon.ch

www.keyon.ch, info@keyon.ch

About Keyon AG

IT-Security - successfully implemented

Corporate PKI
Software Engineering
Digital Signature Services
Identity & Access Management
Information Rights Management
On-Prem, Cloud- & Mobile Security

Covering the entire MS Security Suite

Microsoft Enterprise Mobility + Security

- Intune
- Cloud App Security
- Advanced Threat Analytics
- Azure Information Protection
- Azure Active Directory Premium

Microsoft Partner

Easy to use signature

true-Sign V

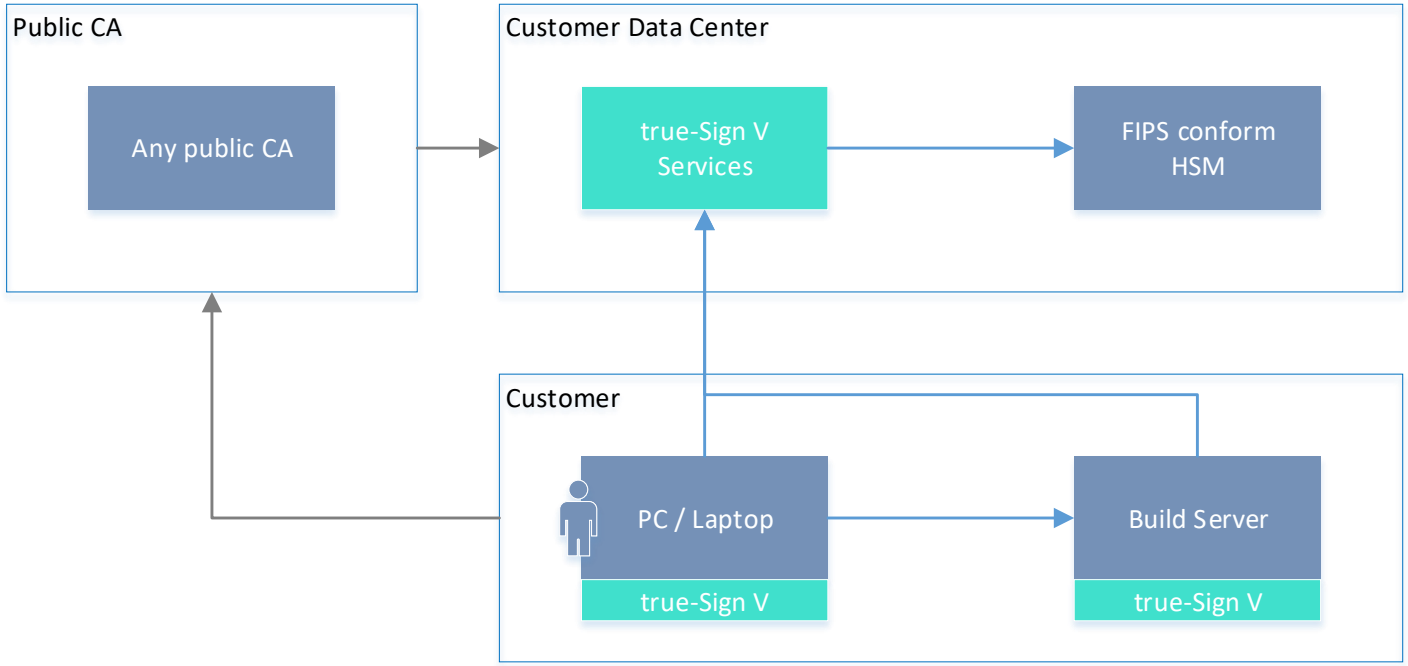
Signing applications and macros (code signature)
Signing business documents (PDF, Office, e-mail, etc.)
Supports certificates from all public CAs
Secure key management in FIPS HSM

About true-Sign V

- true-Sign V is an easy to use digital signature service for Windows clients
- The signature key is created, stored and used on a FIPS 140-2 Level 3 conform HSM. It never leaves the FIPS conform HSM
- Any Windows applications supporting Microsoft CAPI can benefit from true-Sign V (that's a lot)
  - Apply digital signatures for business documents (Office, PDF, e-mail, etc.)
  - Apply digital signatures for Applications and Macros (Code Signature)
- The data to be signed remains on the user's PC. Only the hash value is sent.

Architecture

- true-Sign V is hosted on-prem using a FIPS conform HSM.



Get ready for true-Sign V

1. Acquire true-Sign V subscription from Keyon
2. Install true-Sign V on your PC
3. Obtain certificate from your preferred public CA. Create the certificate signing request on your own, request the certificate from the public CA and install the certificate on-prem. All the necessary instructions and tools are part of the true-Sign V license.
4. Enjoy true-Sign V in your daily business

keyon

About code signatures

Digitally sign Applications, Installers, Macros and Scripts

https://casecurity.org/2016/12/08/leading-certificate-authorities-and-microsoft-introduce-new-standards-to-protect-consumers-online/

About code signatures

- Being able to sign an application or macro based on a public certificate is comparable to being a public CA issuing public certificates
- Every application or macro that is signed with a public code signing certificate is immediately trusted by any computer and browser in the world
- It must be prevented that public code signing certificates can be abused by malicious users or applications

About code signatures

- Microsoft Trusted Root Program Requirements
  - Effective February 1, 2017, any CA enrolled in the program that issues certificates capable of being used for code signing must adopt the Minimum Requirements for the Issuance and Management of Publicly Trusted Code Signing Certificates published by the CAB Forum Code Signing Working Group (available at http://aka.ms/csbr , refers to CA Security Council)

    https://social.technet.microsoft.com/wiki/contents/articles/31633.microsoft-trusted-root-program-requirements.aspx#D_Code_Signing_Root_Certificate_Requirements

- A code signature ensures the authenticity and integrity of the code. It applies to
  - Applications and installers (.exe, .msi, Java code, etc.)
  - Office Macros (.pptm, .xlsm, .docm, etc.)

CA Security Council - Best practices

#	Best practices	Security measures of true-Sign V and related processes	
1	**Minimize access to private keys** a) Allow minimal connections to computers with keys b) Minimize the number of users who have key access c) Use physical security controls to reduce access to keys	true-Sign V can manage dedicated code signing certificates per user, application or per build server. The authentication towards the true-Sign V server is done based on X.509 certificates. The signature keys are created, used and stored in a FIPS 140-2 Level 3 conform HSM.	☑
2	**Protect private keys with cryptographic hardware products** a) Cryptographic hardware does not allow export of the private key to software where it could be attacked b) Use a FIPS 140 Level 2-certified product (or better) c) Use an EV code signing certificate which requires the private key to be generated and stored in hardware	true-Sign V supports EV code signing certificates. The signature keys are create, used and stored in a FIPS 140-2 Level 3 conform HSM.	☑
3	**Time-stamp code** a) Time-stamping allows for the code to be verified after the certificate has expired or been revoked	true-Sign V supports code signature applications that include time-stamping.	☑
4	**Understand the difference between test-signing and release-signing** a) Test-signing private keys and certificates requires less security access controls than production code signing private keys and certificates b) Test-signing certificates can be self-signed or come from an internal test CA c) Test certificates must chain to a completely different root certificate than the root certificate that is used to sign publicly released products; this precaution helps to ensure that test certificates are trusted only within the intended test environment d) Establish a separate test code signing infrastructure to test-sign pre-release builds of software	true-Sign V supports specific policies for test- and production certificates. It can be ensured that only dedicated build servers / applications can use the production certificate.	☑

https://casecurity.org/

CA Security Council - Best practices

#	Best practices	Security measures of true-Sign V and related processes	
5	Authenticate code to be signed a) Any code that is submitted for signing should be strongly authenticated before it is signed and released b) Implement a code signing submission and approval process to prevent the signing of unapproved or malicious code c) Log all code signing activities for auditing and/or incident-response purposes	Keyon supports the customer in setting up appropriate code signature processes, which also includes the separation of test- and production environment and the malware scanning of the code before being signed. Any signature activities are logged by true-Sign V.	☑
6	Virus scan code before signing a) Code signing does not confirm the safety or quality of the code; it confirms the publisher and whether or not the code has been changed b) Take care when incorporating code from other sources c) Implement virus-scanning to help improve the quality of the released code	Keyon supports the customer in setting up appropriate code signature processes, which also includes the separation of test- and production environment and the malware scanning of the code before being signed.	☑
7	Do not over-use any one key (distribute risk with multiple certificates) a) If code is found with a security flaw, then publishers may want to prompt a User Account Control dialogue box to appear when the code is installed in the future; this can be done by revoking the code signing certificate so a revoked prompt will occur b) If the code with the security flaw was issued before more good code was issued, then revoking the certificate will impact the good code as well c) Changing keys and certificates often will help to avoid this conflict	Keyon supports the customer in setting up appropriate certificate lifecycle processes. true-Sign V can manage dedicated code signing certificates per application or per build server. In addition, code signing certificates may be renewed frequently in order not to impact a good code that has been issued in the past.	☑

https://casecurity.org/

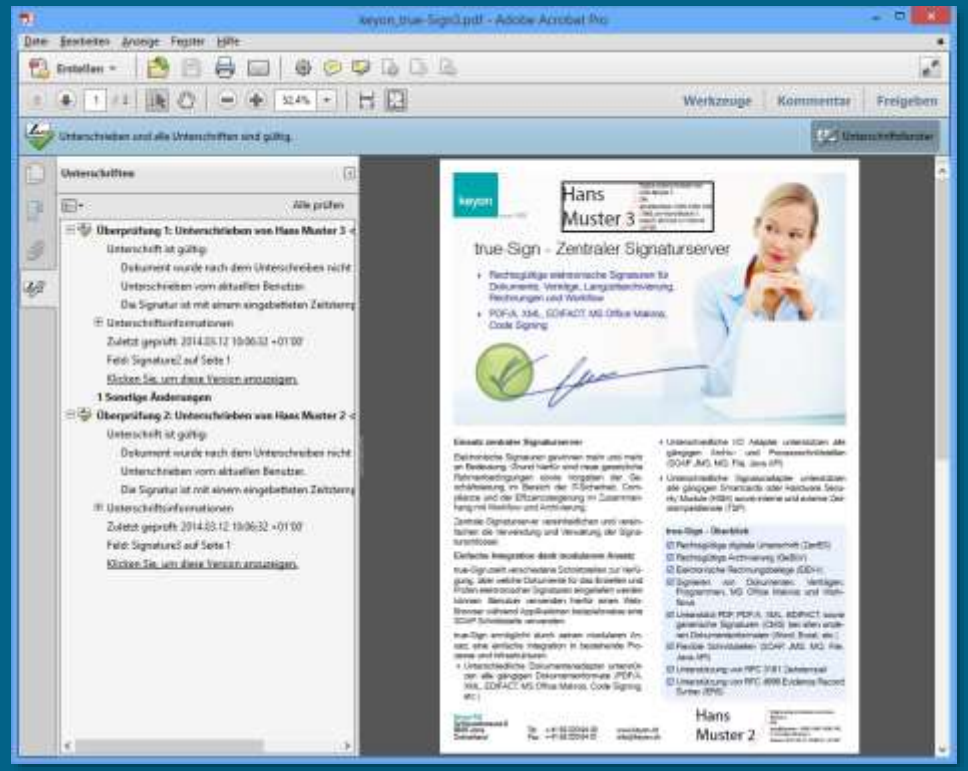
keyon

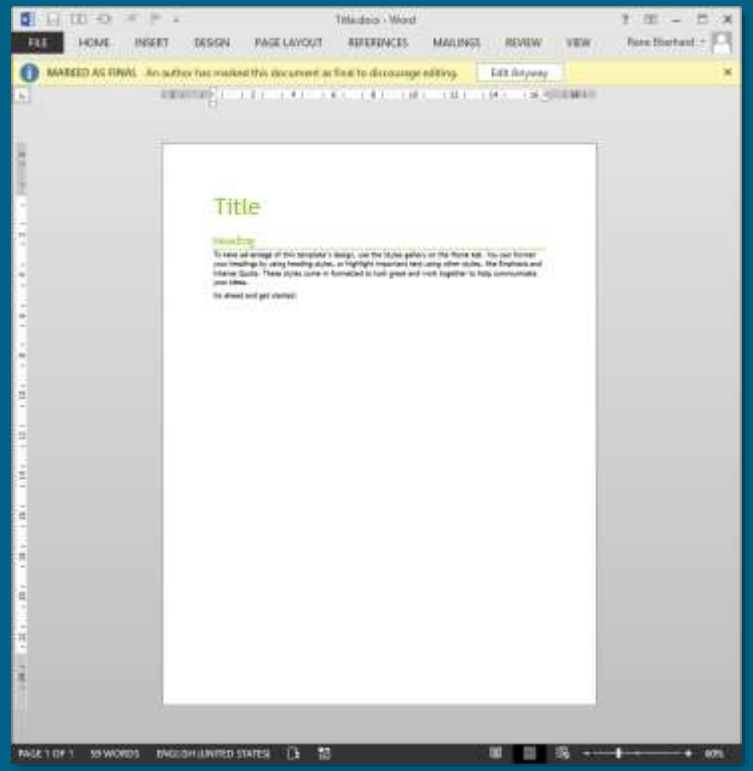
About business signatures

Digitally sign PDF-, Office Documents and e-mails

About business signatures

- true-Sign V support any Windows applications with digital signature capabilities.
  - Microsoft Office, Adobe PDF, etc.





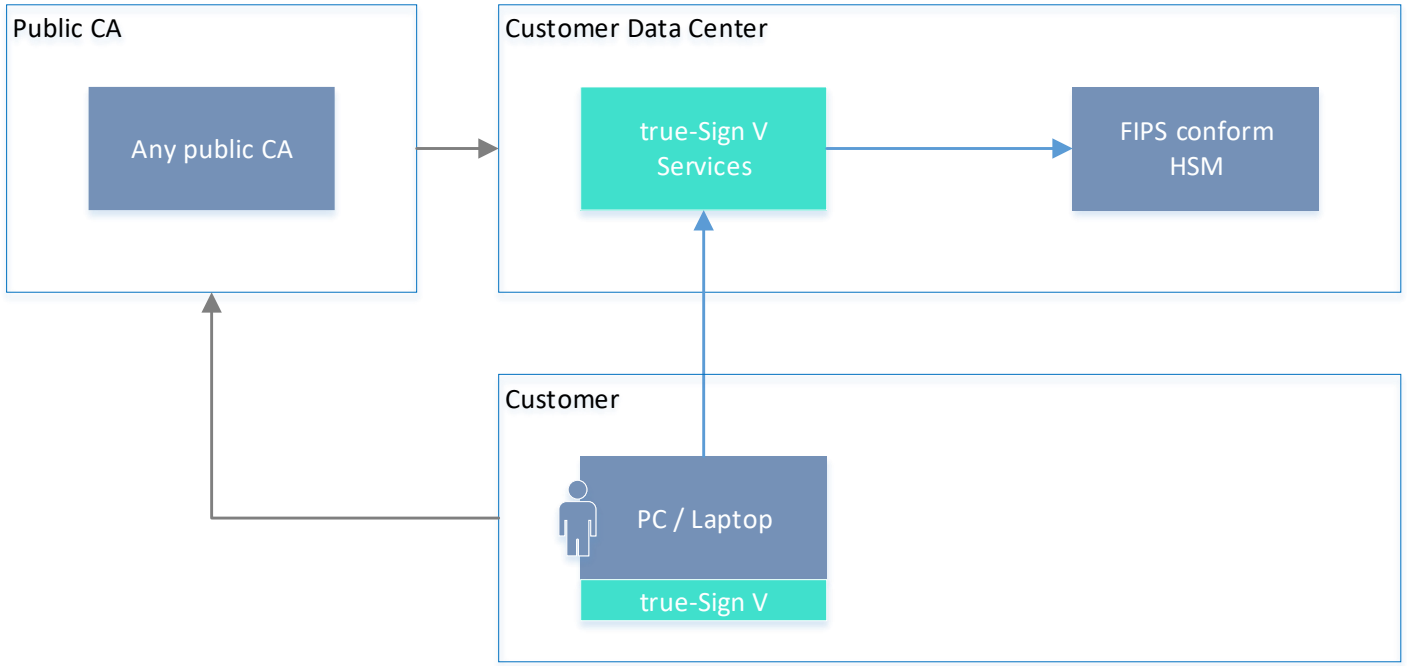
keyon

Live demo

Code-Signature
Business Signatures (Adobe Reader)

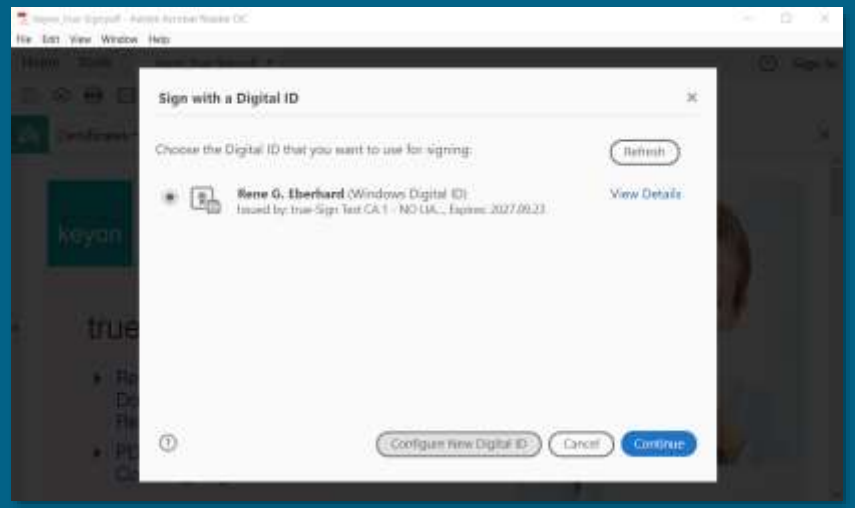
Live demo - overview

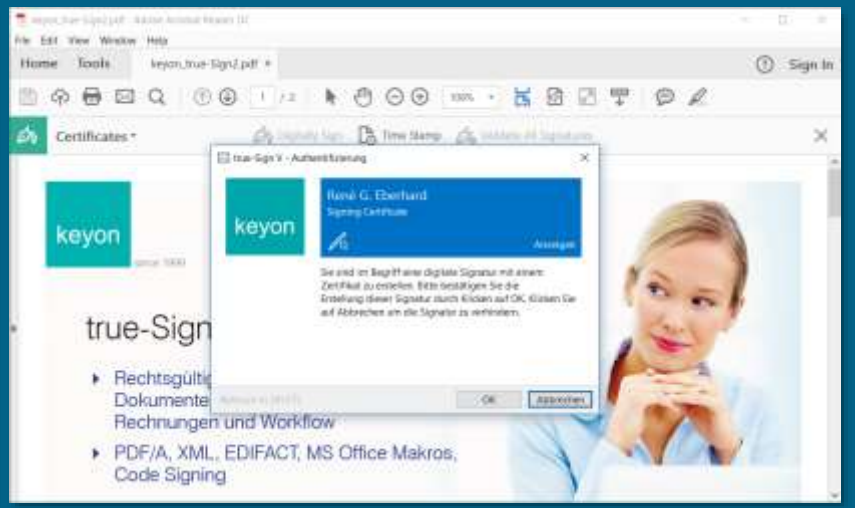
1. Digitally sign an application (.exe)
2. Digitally sign a PDF document

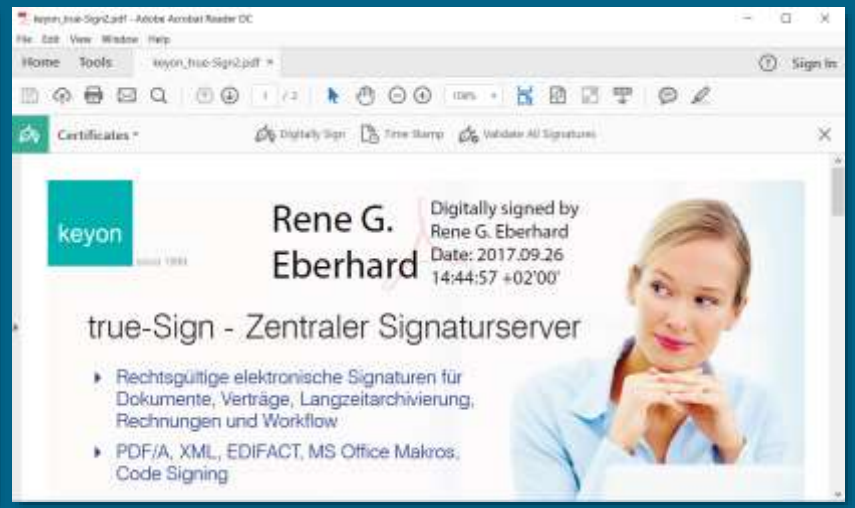


Live demo – Adobe Reader

- **Policy based certificate mapping:**
  Adobe Reader can only use the appropriate signing certificate that has been defined in the true-Sign V policy
- **Widows single sign-on capabilities – no login from the user required:**
  User gets notified whenever a signature is applied (true-Sign V policy, can be switched off)

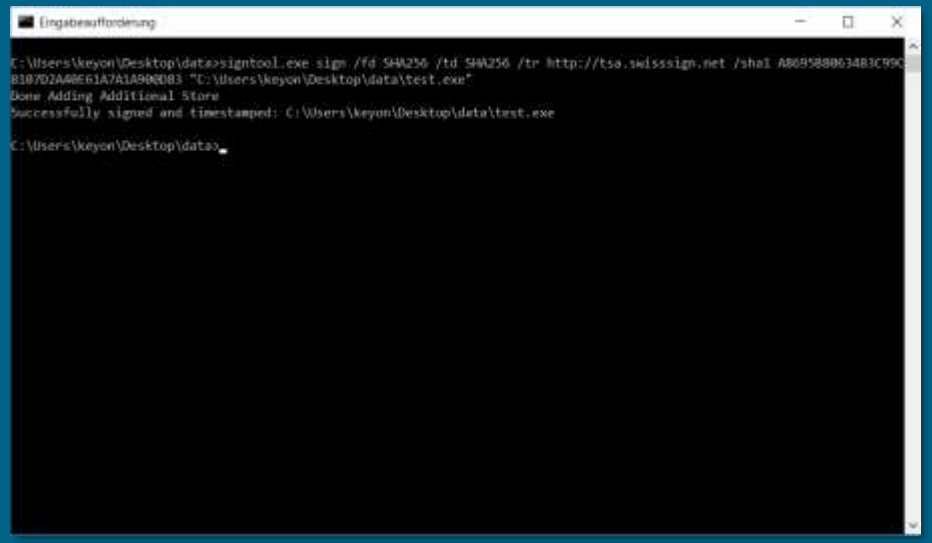


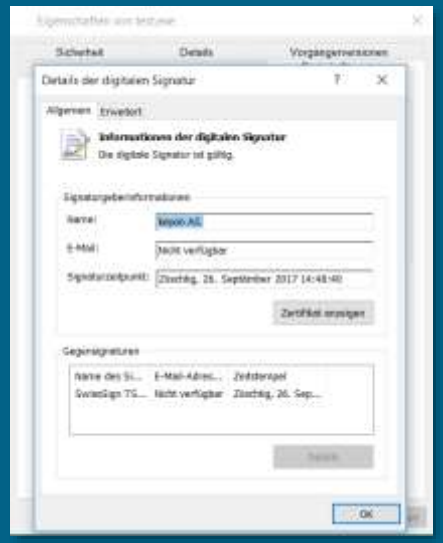




Live demo – Code Signature

- **Policy based certificate mapping:**
  Code signing applications can only use the appropriate signing certificate that has been defined in the true-Sign V policy
- **Windows single sign-on capabilities – unattended signing on a build server:**
  No signing notification when a signature is applied (true-Sign V policy for unattended signing)





keyon

Questions & Answers

Thank you for your attention