keyon

true-Sign V

Product flyer

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

With true-Sign V, companies can easily create electronic signatures for programs, macros, scripts (code) as well as for PDF, Office, and other Windows applications. The solution is easy to install and can be used with Windows single sign-on. The data to be signed never leaves the user's PC. Only the hash value is sent. Confidentiality is 100% guaranteed.

---

true-Sign V is an easy to use digital signature service for Windows clients. In other words, it's a virtual smart card on Windows PC. It supports any Windows application with digital signature capabilities (Applications, Office macros, PowerShell scrips (code signature), Office, PDF, e-mail, etc.).

keyon AG
Schlüsselstrasse 6
8645 Jona
Switzerland

Phone: +41 55 220 64 00
Fax: +41 55 220 64 01

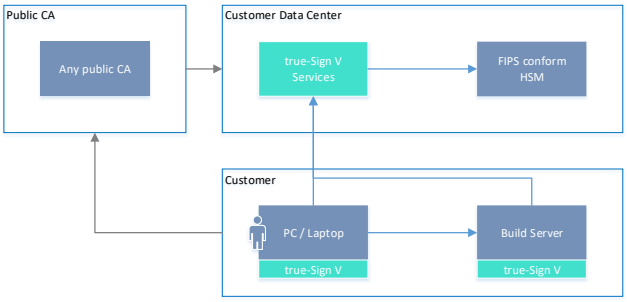
www.keyon.ch
info@keyon.ch

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. Any computer and browser in the world immediately trust every data that is signed with a public code-signing certificate. It must be prevented that malicious users can sign applications or macros with such a certificate.

Architecture

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



Microsoft Trusted Root Program Requirements

Companies using code signing must adopt to the new standard:

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

true-Sign V helps companies to protect the signature key from compromise and the quality of the signed data in accordance with the new standard for code signing certificates.

Authenticity and integrity

A code signature ensures the authenticity and integrity of the code. It applies to the following file-types:

- .exe, .msi, Microsoft Authenticode, PowerShell scripts, Java code, and other code signing aware file-types.
- Office macros (.pptm, .xlsm, .docm, etc.)

Get ready for true-Sign V

1. Acquire true-Sign V subscription from Keyon and install it on your PC
2. Obtain certificates from your preferred public CA. Create the certificate-signing request, 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.
3. Enjoy true-Sign V in your daily business!

Supported scenarios

Usually applications, macros or scripts are developed, built and packaged on a local PC or on a central build server. true-Sign V supports the application of code signatures on any Windows based developer environments supporting Crypto API (CAPI) or PKCS#11.

Get instant test access for free

Gain experienced with true-Sign V (test installation and test certificate). Contact us!

CA security council – best practices

The challenge with code signing is the protection of the private signing key associated with the code signing certificate. If a key is compromised, the certificate loses trust and value, jeopardizing the software that you have already signed. The following table shows seven best practices for code signing:

#	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 140-2 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 b) Test-signing private keys and certificates requires less security access controls than production code signing private keys and certificates c) Test-signing certificates can be self-signed or come from an internal test CA d) 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 e) 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.	☑
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 renews frequently in order to not impact good code that has been issued in the past.	☑

https://casecurity.org/