



Enhancing Security: Timestamping

(การประทับรับรองเวลา)



High Scale Managed PKI Solutions for the Internet of Everything

โซลูชัน PKI ที่มีการจัดการระดับสูงสำหรับอินเทอร์เน็ตทุกสิ่งอย่าง

**Enabling Trust and Security with PKI.
GlobalSign Makes Certificate Management
Easy for Businesses and Scales Identity for
Service Providers and IoT**

การเปิดใช้งานความน่าเชื่อถือและความปลอดภัยด้วย PKI

GlobalSign ทำให้การจัดการใบรับรองเป็นเรื่องง่ายสำหรับธุรกิจ และระบุตัวตนของผู้ให้บริการและ IoT

We've been a leader in the Public Key Infrastructure (PKI) space since 1996, taking a consultative approach in helping enterprises speed up their digital transformations with identity and security solutions that scale.

เราเป็นผู้นำในพื้นที่โครงสร้างพื้นฐานคีย์สาธารณะ (PKI) มาตั้งแต่ปี ค.ศ. 1996 โดยใช้แนวทางทำให้คำปรึกษาเพื่อช่วยให้องค์กรต่างๆ ในการเปลี่ยนแปลงทางดิจิทัลด้วยโซลูชันการระบุตัวตนและการรักษาความปลอดภัยที่ปรับขนาดได้

Headquartered in
Japan, globally
reputed **Certificate
Authority**

Leading provider
of **Identity &
Security
Management
Solutions**

One of the longest
**WebTrust accredited
Certificate Authority
(CA) worldwide**

**A GMO Internet
Company. GMO
Internet, Inc.
(TSE: 9449)**

 **ENTERPRISE**
Automate and Manage
PKI in the Enterprise

 **IOT**
IoT Security
Starts with PKI

 **SERVICE PROVIDERS**
Build PKI
into Your Service


GlobalSign's Certifications

? ISMS Cloud Security – ISO/IEC 27017:2015

Holds Certificate No: **CLOUD 771047**
and operates an ISO/IEC 27001:2013 certified ISMS that complies with the commonly accepted controls of, and takes the implementation guidance of ISO/IEC 27017 into account for the following scope:


The Information Security Management System applies to the Certification Authority & Trustlogon segment of GMO GlobalSign which includes CA Software Development, CA Infrastructure Management & CA DC Operations. This is in accordance with Statement of Applicability ver 15 dated 09-Aug-2022.

This relates to ISO 27001:2013 Certificate No. IS 710738.

For and on behalf of BSI: 
Theuns Kotze, Managing Director Assurance - IMETA

Original Registration Date: 2022-11-01 Effective Date: 2022-11-01
Latest Revision Date: 2023-02-07 Expiry Date: 2025-10-20

Page: 1 of 2




...making excellence a habit.™

? Privacy Information Management System – ISO/IEC 27701:2019

Holds Certificate No: **PM 744600**
and operates a Privacy Information Management System which complies with the requirements of ISO/IEC 27701:2019 for the following scope:



The Privacy Information Management System applies to the Certification Authority segment of GMO GlobalSign which includes CA Software Development, CA Infrastructure Management, CA DC Operations and Verification Activity as well as support functions that includes Corporate IT Operations, General Office Security, Corporate IT Infrastructure and Human resources, both as PII controller and PII processor.

This is based on the Information security certificate number IS 710738, and in accordance with Statement of Applicability ver 15 dated 09-Aug-2022.

For and on behalf of BSI: 
Theuns Kotze, Managing Director Assurance - IMETA

Original Registration Date: 2022-11-14 Effective Date: 2022-11-14
Latest Revision Date: 2023-01-30 Expiry Date: 2025-11-13

Page: 1 of 3




...making excellence a habit.™

? Business Continuity Management System – ISO 22301:2019



Holds Certificate No: **BCMS 714780**
and operates a Business Continuity Management System which complies with the requirements of ISO 22301:2019 for the following scope:

The Business Continuity Management System applies to the Certification Authority segment of GMO GlobalSign which includes key activities CA Infrastructure Management, Verification Activity, Customer Support, Key Management & CA DC Operations as well as support functions that includes Human resources.

For and on behalf of BSI: 
Theuns Kotze, Managing Director Assurance - IMETA

Original Registration Date: 2019-10-21 Effective Date: 2022-08-24
Latest Revision Date: 2022-10-21 Expiry Date: 2025-10-20

Page: 1 of 3



...making excellence a habit.™

? Information Security Management System – ISO/IEC 27001:2013

Holds Certificate No: **IS 710738**
and operates an Information Security Management System which complies with the requirements of ISO/IEC 27001:2013 for the following scope:

The Information Security Management System applies to the Certification Authority & Trustlogon segment of GMO GlobalSign which includes CA Software Development, CA Infrastructure Management, CA DC Operations, Qualified Trust Service Provider, TimeStamping Authority DC Operations, and Verification Activity as well as support functions that includes Corporate IT Operations, General Office Security, Corporate IT Infrastructure and Human resources.

This is in accordance with Statement of Applicability ver 15 dated 09-Aug-2022.

For and on behalf of BSI: 
Theuns Kotze, Managing Director Assurance - IMETA

Original Registration Date: 2019-10-21 Effective Date: 2022-10-21
Latest Revision Date: 2023-01-30 Expiry Date: 2025-10-20

Page: 1 of 3



...making excellence a habit.™

Global Presence

GLOBAL SCALE DEVELOPER

- > 5,000 global partners
- 4 Global Data Centers

PROVEN EXPERTISE

- > 500 employees
- > 60m identities issued
- > 4m SSL Certificates
- > 2b OCSP Responses/monthly

**TRUSTED
CERTIFICATE
AUTHORITY**



46%
Creators &
Engineers

19
Countries

60
Locations

Publicly
Traded Firms
10
Firms

6,180
Group
Partners

Group Companies
100
Companies

Trusted Around the World

เรา “GlobalSign” ได้รับความไว้วางใจทั่วโลก



CUSTOMERS

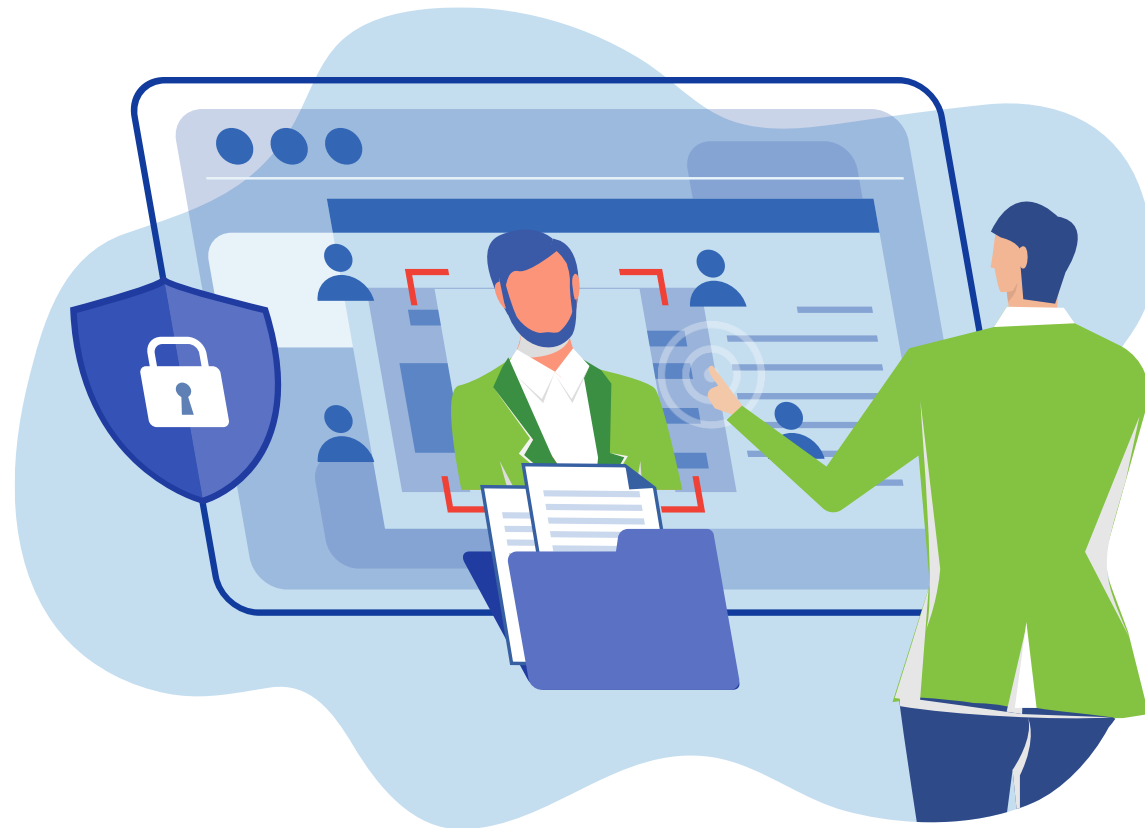


PARTNERS



Contents/สารบัญ

1. Timestamping (การประทับรับรองเวลา)
2. Signing Solutions (โซลูชันการลงนาม)
3. Adobe Approved Trust Lis (ใบรับรองที่เชื่อถือได้
Adobe AATL)
4. Digital Signing Services (บริการลงนามดิจิทัล DSS)
5. Code Signing (การลงนามรหัส)
6. Questions? (คำถาม)



Product Overview

Timestamping

การประทับรับรองเวลา

Timestamping Overview

Specialized Products and Services

ผลิตภัณฑ์และบริการเฉพาะทาง

- ✓ Quick and easy ง่ายและรวดเร็ว
- ✓ Recognized and compatible เป็นที่ยอมรับและเข้ากันได้
- ✓ RFC 3161 compliant ตรงตามมาตรฐาน RFC 3161
- ✓ Verifies time of signing ตรวจสอบเวลาของการลงนาม
- ✓ Prevents tampering ป้องกันการแก้ไขข้อมูล
- ✓ Secures non-repudiation for signatures รับรองการไม่ปฏิเสธลายเซ็น



Why Timestamping is needed

What is it really?

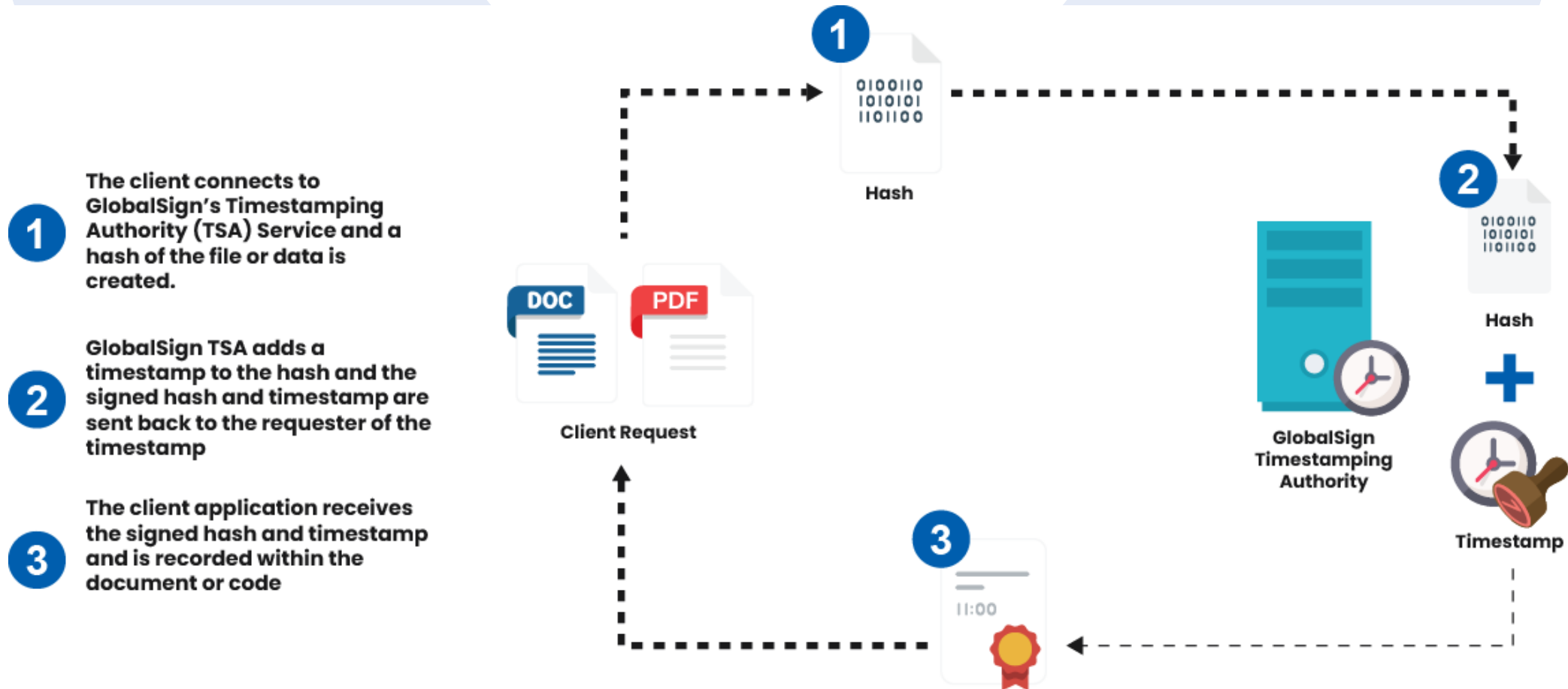
- ✓ An attestation that your digital signature was placed at a logged, verifiable time
เอกสารรับรองว่าลายเซ็นดิจิทัลของคุณถูกวางไว้ตามเวลาที่บันทึกไว้และสามารถตรวจสอบได้
- ✓ Allows signed code and documents to remain valid long past the end-entity certificates expiration date
อนุญาตให้รหัสและเอกสารที่ลงนามยังคงใช้งานได้นานหลังจากวันหมดอายุของใบรับรองเอ็นทีดีปลายทาง

What about our individual, standalone service?

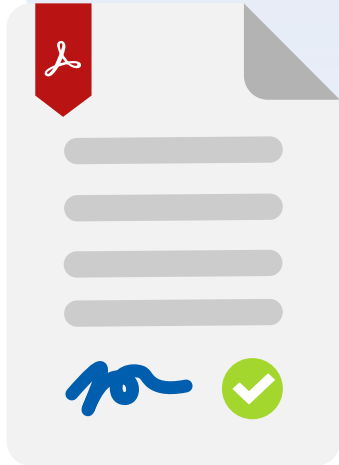
- ✓ Globalsign offers a unique service separate from certificates, for organizations needing a reliable timestamp server for their processes.
นำเสนอบริการพิเศษที่แยกจากใบรับรอง สำหรับองค์กรที่ต้องการเซิร์ฟเวอร์การประทับเวลาที่เชื่อถือได้สำหรับกระบวนการของตน



Trusted Timestamping Services



Our Products & Service that use Timestamping



AATL Certificates



DSS



**CodeSigning
Certificates**

Sample Signed & Timestamped Document

Signed by GMO Sign

Ensure document integrity

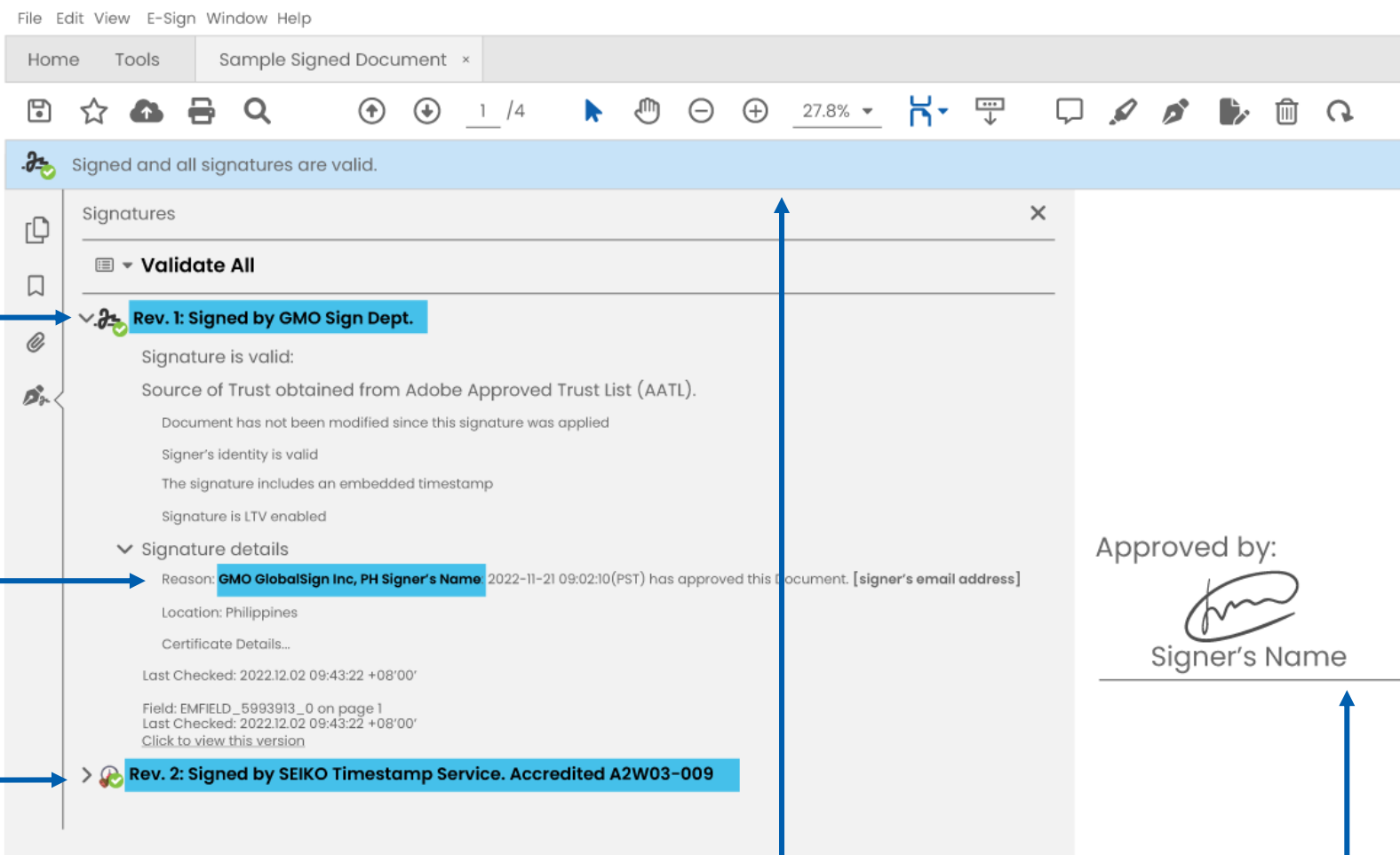
ตรวจสอบความสมบูรณ์ของเอกสาร

E-signed by user

Signer details indicated at "Reason" section. รายละเอียดผู้ลงนามระบุไว้ในส่วน "เหตุผล"

- Company
- Name
- Email

Trusted Timestamping



Signature Properties

click signature to view signature properties คลิกลายเซ็นเพื่อดูคุณสมบัติลายเซ็น

Visible Signature

Long Term Validity (LTV)

Long Term Validity

ความถูกต้องในระยะยาว



× Signatures

✓ Rev. 1: Signed by GMO Sign Dept.

Signature is valid:

Source of Trust obtained from Adobe Approved Trust List (AATL).

Document has not been modified since this signature was applied

Signer's identity is valid

The signature includes an embedded timestamp.

Signature is LTV enabled

✓ Signature Details

Reason: Han: 2023-10-04 13:48:26(SGT) has approved this Document. [zhonghan_chua@yahoo.com]

Location: Singapore

[Certificate Details...](#)

Last Checked: 2024.07.15 16:09:38 +08'00'

Field: EMFIELD_10415678_0 on page 1

[Click to view this version](#)

> Rev. 2: Signed by Seiko Timestamp Service. Accredited A2W01-102

Different

Timestamping

ความแตกต่างของการประทับตราเวลา

Our Offering

Standard RFC 3161 Timestamp



Standard timestamp,
usually used for
CodeSigning as no
further accreditation is
needed

การประทับเวลามาตรฐาน มักใช้
สำหรับการลงนาม CodeSigning
เนื่องจากไม่จำเป็นต้องมีการ
รับรองเพิ่มเติม

AATL Timestamp



Timestamp under
the AATL Root
Program

การประทับเวลาภายใต้
โปรแกรม AATL Root

Qualified Timestamp



Timestamp under
the EU TL Root
program

การประทับเวลาภายใต้
โปรแกรม EU TL Root

Seiko Timestamp



Timestamp
certified by Japan
Data
Communications
Association, using
Japanese Time

การประทับเวลาที่ได้รับ
การรับรองโดย Japan
Data Communications
Association โดยใช้เวลา
ของญี่ปุ่น

gning

Signing

Solutions

โซลูชันการลงนาม

Solution

Signing Solutions



AATL Certificates

On-Premise



DSS

API-Based



CodeSigning Certificates

Cloud-Based

Approved
Adobe Approved

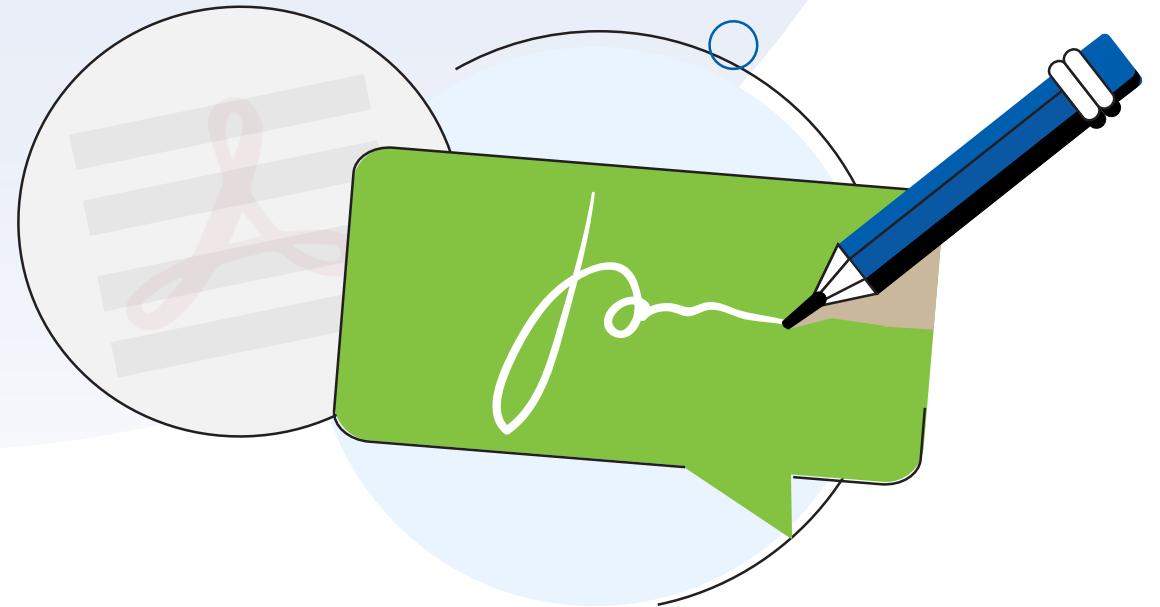
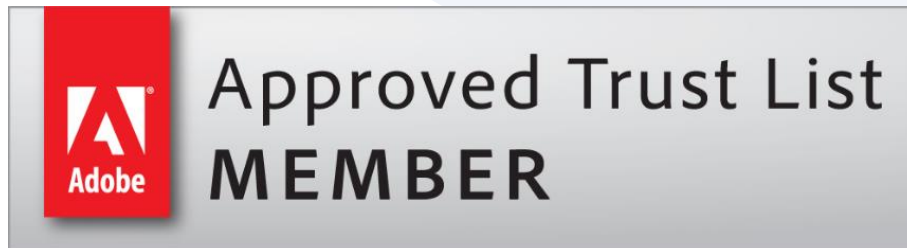
Trust List

ใบรับรองอิเล็กทรอนิกส์ภายใต้สมาชิก Adobe

Overview

Adobe's Approved Trust List (AATL)

ใบรับรองอิเล็กทรอนิกส์ภายใต้สมาชิก Adobe



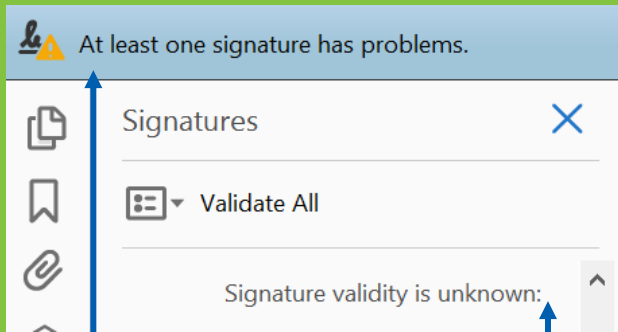
The Importance of Public Trust

GlobalSign digital signatures are trusted across the leading desktop and cloud-based signing platforms:

ลายเซ็นดิจิทัลของ GlobalSign ได้รับความไว้วางใจในแพลตฟอร์มการลงนามบนเดสก์ท็อปและคลาวด์ชั้นนำ



Untrusted Signature



Untrusted signature
warnings

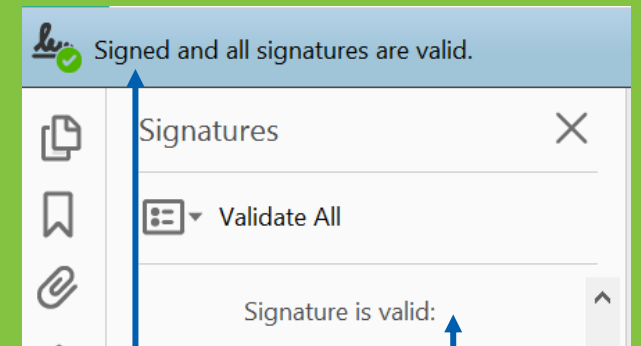
คำเตือนลายเซ็นที่น่าเชื่อถือ

Untrusted

VS

Publicly Trusted

Publicly Trusted Signature



Automatic signature
validation

การตรวจสอบลายเซ็น
อัตโนมัติ

Deployment Options for AATL

The Adobe AATL Certificate Policy requires certificates to be stored on FIPS*-compliant hardware, such as a SafeNet E-Token or Hardware Security Module (HSM).

นโยบายใบรับรอง Adobe AATL กำหนดให้จัดเก็บใบรับรองไว้ในฮาร์ดแวร์ที่รองรับ FIPS* เช่น SafeNet E-Token หรือ Hardware Security Module (HSM)

GlobalSign offers a variety of deployment options to support the needs of all organization, small to large.

GlobalSign นำเสนอตัวเลือกการใช้งานที่หลากหลายเพื่อรองรับความต้องการของทุกองค์กร ตั้งแต่ขนาดเล็กไปจนถึงขนาดใหญ่

- The Federal Information Processing Standard (**FIPS**) Publication 140-2, (**FIPS PUB 140-2**), is a U.S. government computer security standard used to approve cryptographic modules
- * Federal Information Processing Standard (FIPS) Publication 140-2 (FIPS PUB 140-2) เป็นมาตรฐานความปลอดภัยคอมพิวเตอร์ของรัฐบาลสหรัฐอเมริกาที่ใช้ในการอนุมัติโมดูลการเข้ารหัส



USB Tokens

Ideal for lower volume signature needs



HSM

Ideal for organizations looking to integrate with an internally developed, or of-the-shelf automated document application



Cloud-based Digital Signing Service

Ideal for higher volume signature needs

General Product Overview

	Individual AATL	Department AATL
Hardware required for certificate Storage ฮาร์ดแวร์ที่จำเป็นสำหรับการจัดเก็บใบรับรอง	SafeNet Token or HSM for the HSM version of the product.	SafeNet Token or HSM for the HSM version of the product.
Example Identity on the Certificate ตัวอย่างข้อมูลประจำตัวใบรับรอง	CN = John Smith O = GMO GlobalSign Ltd OU = Support L = Maidstone S = Kent C = GB E = john.sargent@globalsign.com	CN = Accounting O = GMO GlobalSign Ltd OU = Support L = Maidstone S = Kent C = GB E = accounting@globalsign.com
Required Software ซอฟต์แวร์ที่จำเป็น	Adobe Acrobat, Microsoft Office, Libre Office or BlueBeam	Adobe Acrobat, Microsoft Office, Libre Office or BlueBeam
Timestamping Services บริการประทับเวลา	Included	Included

Digital Signing

Services

บริการลงนามดิจิทัล

Cloud-Based Digital Signing Service

GlobalSign's Digital Signing Service provides everything you need to apply legally admissible and digital signatures in one-cloud based service

บริการลายเซ็นดิจิทัลของ GlobalSign มอบทุกสิ่งที่คุณต้องการเพื่อใช้ลายเซ็นดิจิทัลและลายเซ็นดิจิทัลที่ยอมรับได้ตามกฎหมาย
ในบริการบนคลาวด์เดียว



Digital signing for
the hash of any
document or other
transaction



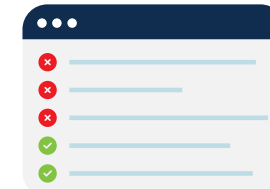
Signing certificate
issuance



Private key storage
on GlobalSign's
cloud-based HSM

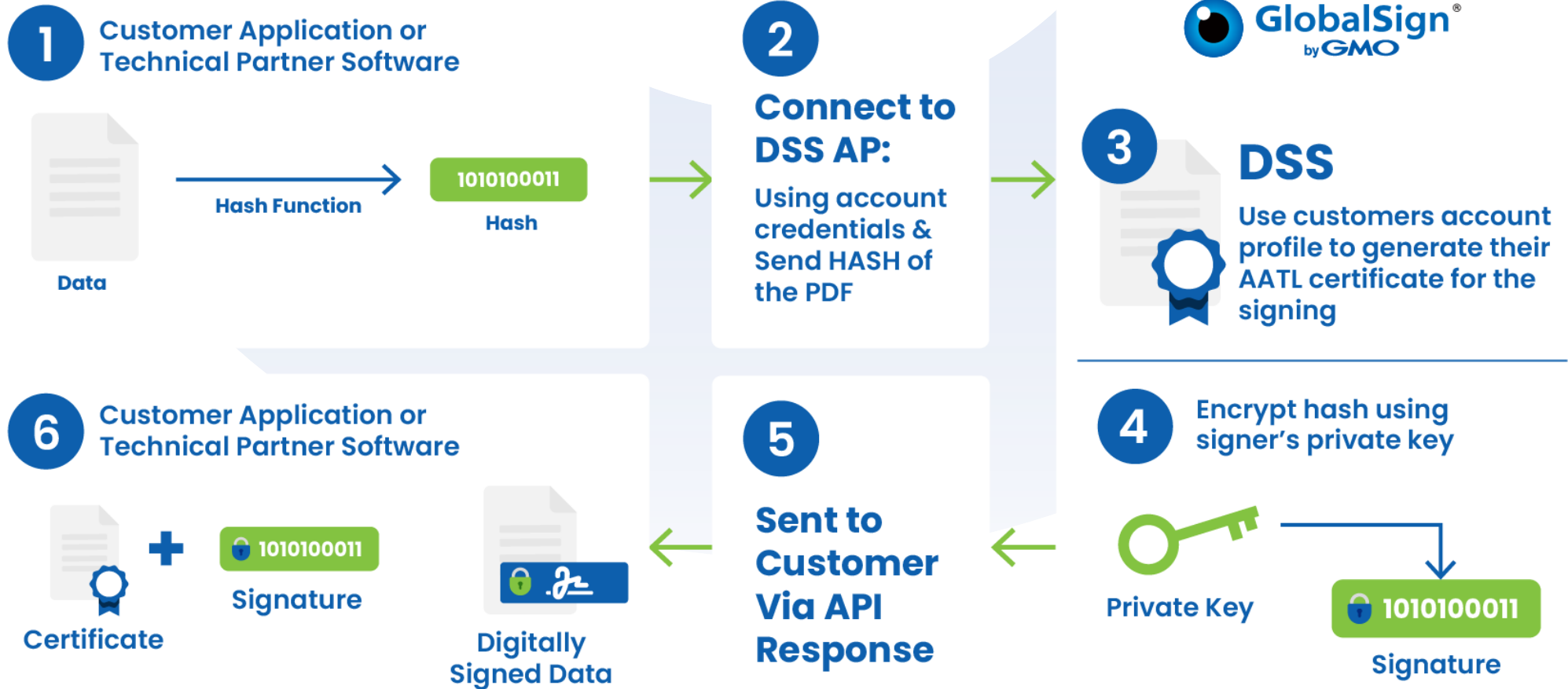


Trusted
timestamping
service

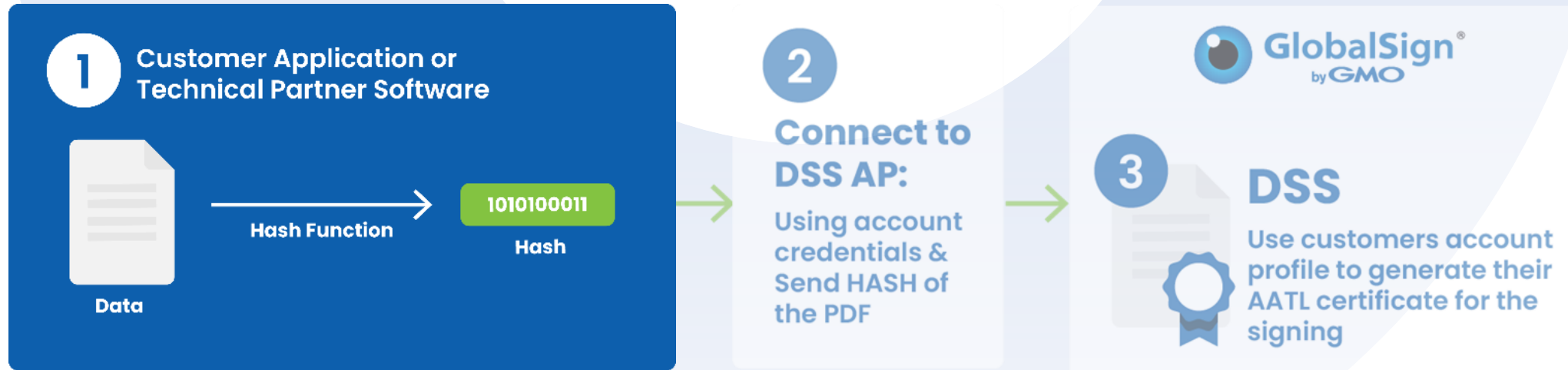


Revocation check
included in response
(required for long
term validation)

How DSS Works?



How DSS Works?



Customers application or Technical partners software is used to take a Hash of their PDF document

แอปพลิเคชันของลูกค้าหรือซอฟต์แวร์ของพันธมิตรทางเทคนิคใช้ในการแฮชเอกสาร PDF ของพวกเขา

How DSS Works?

1 Customer Application or Technical Partner Software



Data

Hash Function

1010100011

Hash

2

Connect to DSS AP:

Using account credentials & Send HASH of the PDF



3

DSS

Use customers account profile to generate their AATL certificate for the signing

- Connects to our DSS API using the provided account credentials and client certificate for authentication.

เชื่อมต่อกับ DSS API ของเราโดยใช้ข้อมูลรับรองบัญชีที่ให้มาและใบรับรองไคลเอ็นต์สำหรับการตรวจสอบสิทธิ์

- The Hash of their PDF document is then to our DSS SAAS platform via the API.

จากนั้นแฮชของเอกสาร PDF จะถูกส่งไปยังแพลตฟอร์ม DSS SAAS ของเราผ่านทาง API

How DSS Works?

1 Customer Application or Technical Partner Software



Data

Hash Function

1010100011

Hash

2

Connect to DSS AP:

Using account credentials & Send HASH of the PDF



3

DSS

Use customers account profile to generate their AATL certificate for the signing

- **DSS uses the account credentials supplied to confirm the customer profiles**

DSS ใช้ข้อมูลรับรองบัญชีที่ให้มาเพื่อยืนยันโปรไฟล์ลูกค้า

- **The Profile is then used to generate a short lifespan AATL**

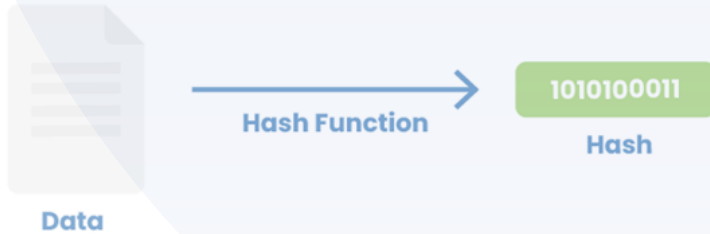
จากนั้นโปรไฟล์จะถูกใช้เพื่อสร้าง AATL ที่มีอายุขัยสั้น

- **Certificate that will last for that 10 minutes signing session only.**

ใบรับรองที่จะคงอยู่สำหรับการลงนามในช่วง 10 นาทีนั้นเท่านั้น

How DSS Works?

1 Customer Application or Technical Partner Software



2

Connect to DSS AP:

Using account credentials & Send HASH of the PDF

3

DSS

Use customers account profile to generate their AATL certificate for the signing



The private key of the AATL certificate is then used to sign the provided HASH of the customers PDF document.

จากนั้นคือส่วนตัวของใบรับรอง AATL จะใช้ในการลงนาม HASH ที่ให้มาของเอกสาร PDF ของลูกค้า

4

Encrypt hash using signer's private key



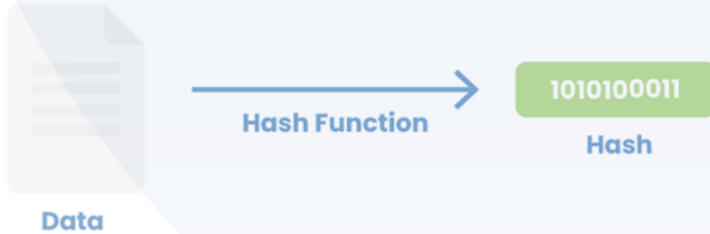
Private Key

1010100011

Signature

How DSS Works?

1 Customer Application or Technical Partner Software



2

Connect to DSS AP:

Using account credentials & Send HASH of the PDF



3

DSS

Use customers account profile to generate their AATL certificate for the signing

4

Encrypt hash using signer's private key



5

Sent to Customer Via API Response

The Signed HASH and the Certificate containing only the public key is then sent back to the customer via an API Response.

HASH ที่ลงนามและใบรับรองที่มีเฉพาะรหัสสาธารณะ จะถูกส่งกลับไปยังลูกค้าผ่านการตอบกลับของ API

How DSS Works?

1 Customer Application or Technical Partner Software



2 Connect to DSS AP:

Using account credentials & Send HASH of the PDF

3 DSS



Use customers account profile to generate their AATL certificate for the signing

6 Customer Application or Technical Partner Software



Connects to our DSS API using the provided account credentials and client certificate for authentication.

เชื่อมต่อกับ DSS API ของเราโดยใช้ข้อมูลรับรองบัญชีที่ให้มาและใบรับรองไคลเอ็นต์สำหรับการตรวจสอบสิทธิ์

The Hash of their PDF document is then to our DSS SAAS platform via the API.

จากนั้นแฮชของเอกสาร PDF จะถูกส่งไปยังแพลตฟอร์ม DSS SAAS ของเราผ่านทาง API

Digital Signing Service

✓ Everything you need for Digital Seal including:

ทุกสิ่งที่คุณต้องการสำหรับ Digital Seal รวมถึง:

- Certificate
- Timestamping
- Key Management & Hash Signing

✓ Minimum Effort & Overhead

ความพยายามขั้นต่ำและค่าใช้จ่าย

✓ One simple API integration

การรวม API ง่ายๆ เพียงครั้งเดียว

✓ High Availability & Disaster Recovery

ความพร้อมใช้งานสูงและการกู้คืนความเสียหาย

✓ Best cost to value offering

การเสนอราคาที่ถูกที่สุด

✓ AATL and Microsoft Root Trust

 **It Just works!**

A Better Way to Digitally Sign

Separate Component Solutions

✗ You need to separately source & integrate

คุณต้องแยกแหล่งที่มาและบูรณาการ

- Certificate.
- Timestamping.
- Key Management & Hash Signing.

✗ More effort and overhead Complex integration requiring advanced crypto expertise.

การรวมที่ซับซ้อนและค่าใช้จ่ายที่มากขึ้นซึ่งต้องอาศัยความเชี่ยวชาญด้าน crypto ขั้นสูง

✗ No high availability & disaster recovery (without additional on-premise hardware investment)

ไม่มีความพร้อมใช้งานสูงและการกู้คืนความเสียหาย (โดยไม่ต้องลงทุนฮาร์ดแวร์ภายในองค์กรเพิ่มเติม)

✗ Pay More, Get Less. จ่ายมากขึ้นรับน้อยลง

It's just a headache! 

DSS Options

DSS Solution available Service Option (ตัวเลือกบริการที่มีโซลูชัน DSS)

CSR Fields	Individual Identity Signing	Organisation Identity Signing
CSR Fields		GlobalSign
CSR Fields	GlobalSign Ltd	GlobalSign Ltd
CSR Fields	Sales (optional)	Sales (optional)
CSR Fields	UK	UK

Customer Built Applications



pdftools

ITEXT

PDFBox[®]



Product Overview

Code Signing

การลงนามรหัส

What is Code Signing?

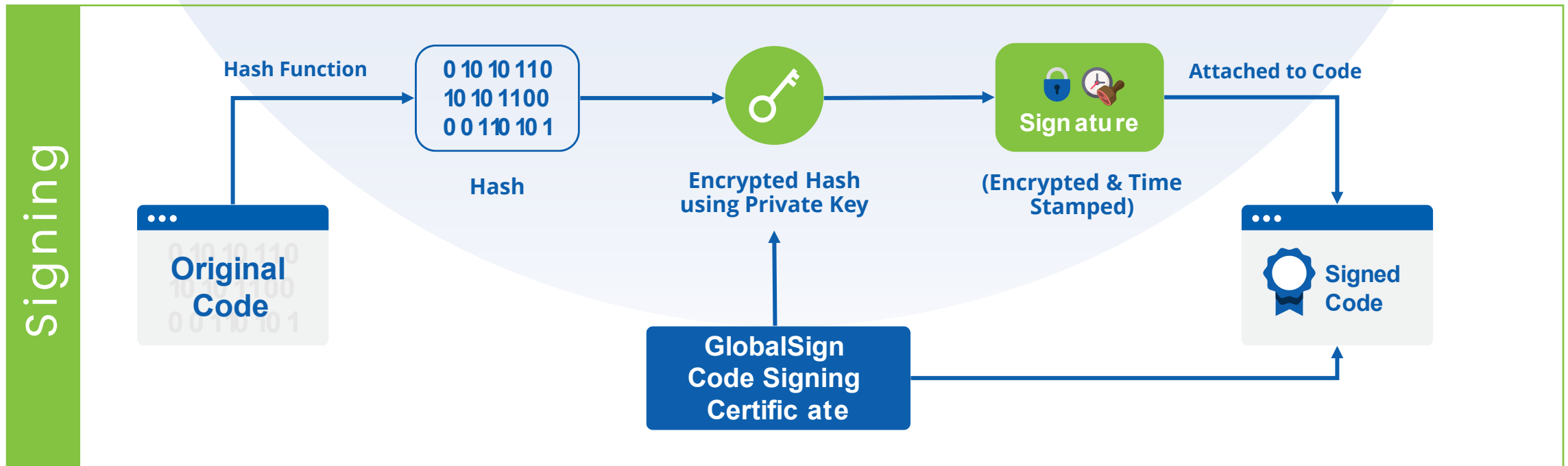
Code Signing is the process of applying a digital signature to software/applications and is the virtual equivalent to shrink-wrapping CD based software for distribution.

การลงนามโค้ดเป็นกระบวนการในการปรับใช้ลายเซ็นดิจิทัลกับซอฟต์แวร์/แอปพลิเคชัน และเป็นเสมือนที่เทียบเท่ากับซอฟต์แวร์ที่ใช้การย่อขนาดซีดีเพื่อการจำหน่าย

What is Code Signing?

Code Signing is the process of applying a digital signature to software/applications and is the virtual equivalent to shrink-wrapping CD based software for distribution.

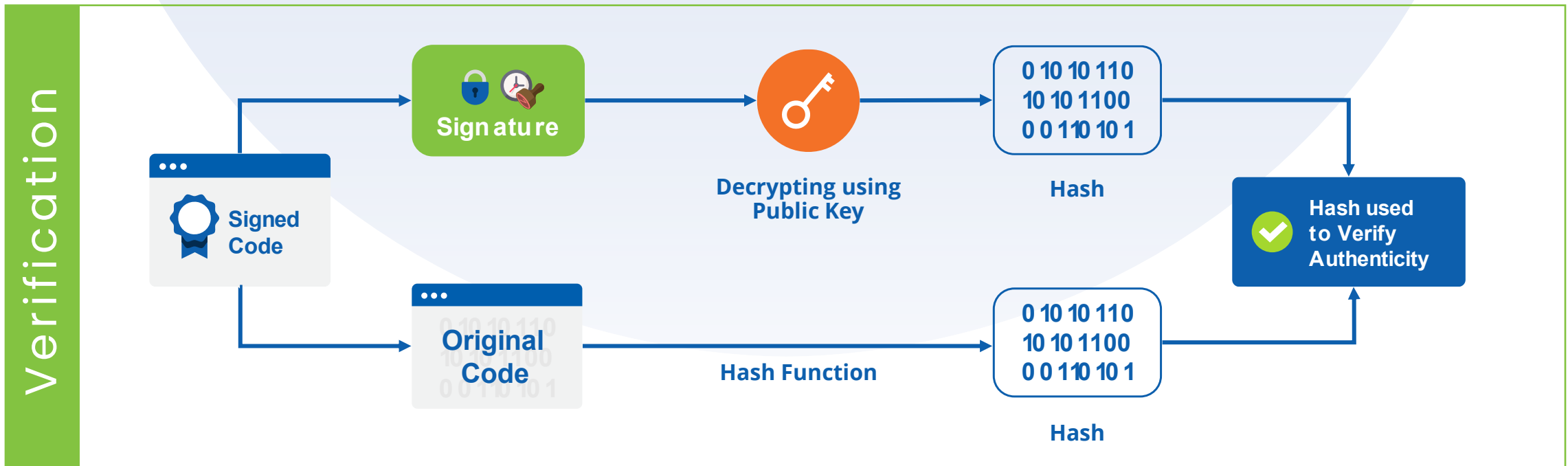
การลงนามโค้ดเป็นกระบวนการในการปรับใช้ลายเซ็นดิจิทัลกับซอฟต์แวร์/แอปพลิเคชัน และเป็นเสมือนที่เทียบเท่ากับซอฟต์แวร์ที่ใช้การย่อขนาดซีดีเพื่อการจำหน่าย



What is Code Signing?

Code Signing is the process of applying a digital signature to software/applications and is the virtual equivalent to shrink-wrapping CD based software for distribution.

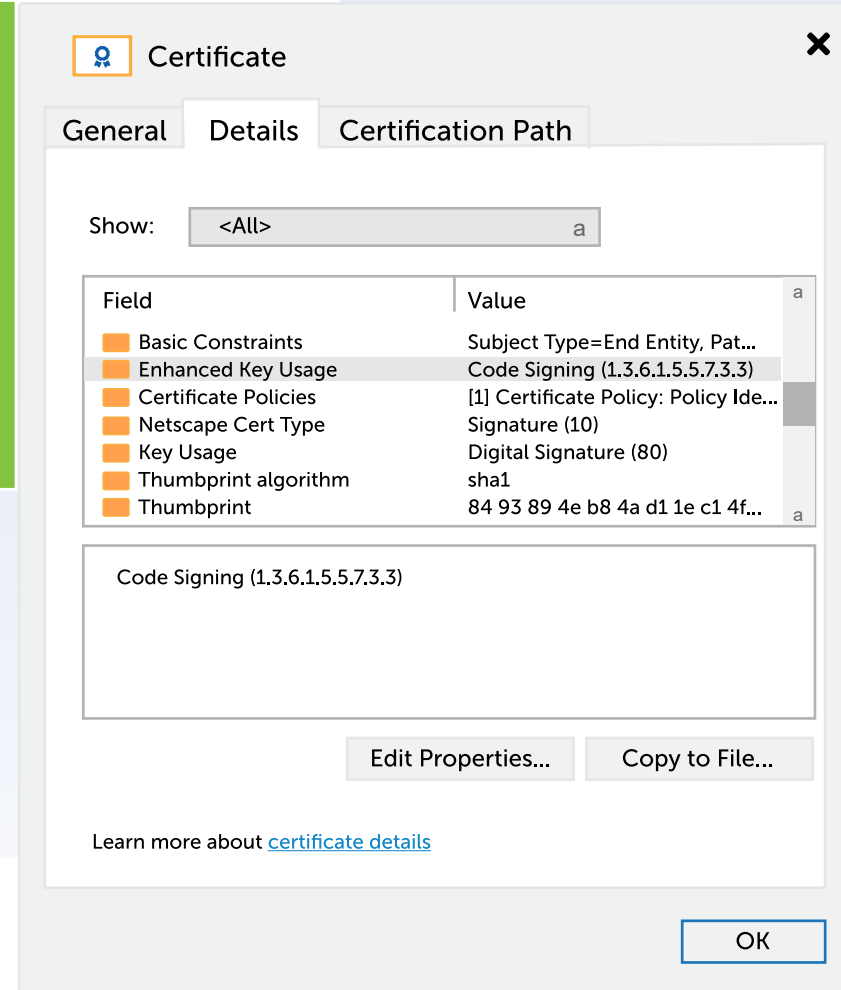
การลงนามโค้ดเป็นกระบวนการในการปรับใช้ลายเซ็นดิจิทัลกับซอฟต์แวร์/แอปพลิเคชัน และเป็นเสมือนที่เทียบเท่ากับซอฟต์แวร์ที่ใช้การย่อขนาดซีดีเพื่อการจำหน่าย



Code Signing Certificate

- ✓ Contains information that fully identifies an entity
มีข้อมูลที่ระบุถึงเอนทิตีได้อย่างครบถ้วน
- ✓ Binds the identity of an individual or entity to a public key that is mathematically related to a private key pair
ผูกข้อมูลประจำตัวของบุคคลหรือเอนทิตีเข้ากับคีย์สาธารณะที่เกี่ยวข้องทางคณิตศาสตร์กับคีย์ส่วนตัว
- ✓ Developer signs code with its private key and the end user uses the developer's public key to verify the developer's identity
นักพัฒนาลงนามรหัสด้วยรหัสส่วนตัว และผู้ใช้ปลายทางใช้รหัสสาธารณะของนักพัฒนาเพื่อตรวจสอบตัวตนของนักพัฒนา
- ✓ Dual signing is available for customers, who wish to sign using a standard Code Signing certificate; whilst also signing the same file with EV Code Sign
การลงนามแบบคู่มีให้บริการสำหรับลูกค้าที่ต้องการลงนามโดยใช้ใบรับรองการลงนามโค้ดมาตรฐาน ในขณะที่เดียวกันก็เซ็นไฟล์เดียวกันด้วย EV Code Sign

Client Certificate



Digital Certificate marked for Code Signing (Code Signing Certificate)

Trusted Timestamping Services

- ✓ Add value to digitally signed or electronically signed documents

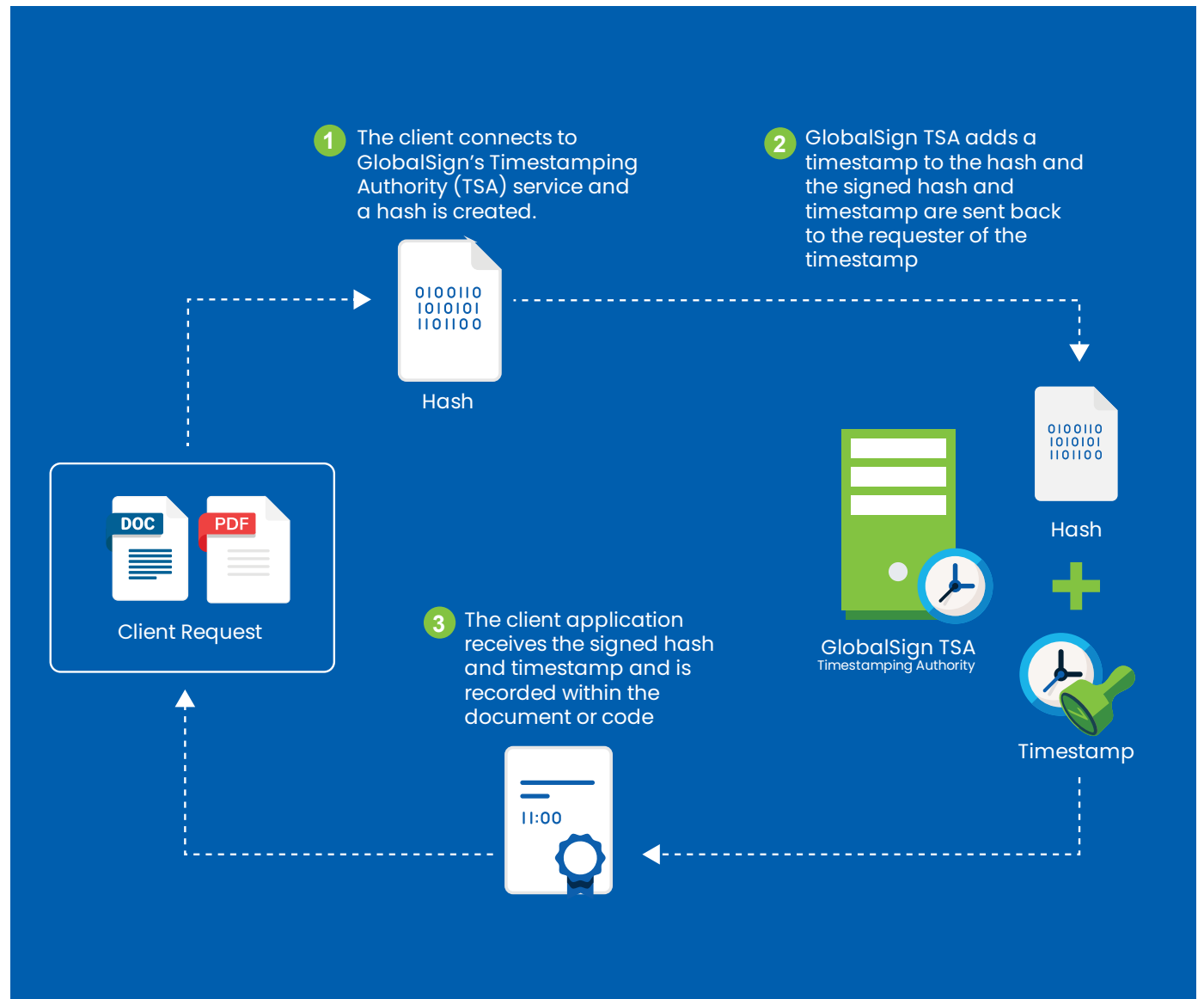
เพิ่มมูลค่าให้กับเอกสารที่ลงนามแบบดิจิทัลหรือลงนามแบบอิเล็กทรอนิกส์

- ✓ Protect intellectual property

ปกป้องทรัพย์สินทางปัญญา

- ✓ Provide strong legal auditable evidence

ให้หลักฐานทางกฎหมายที่เข้มแข็งตรวจสอบได้



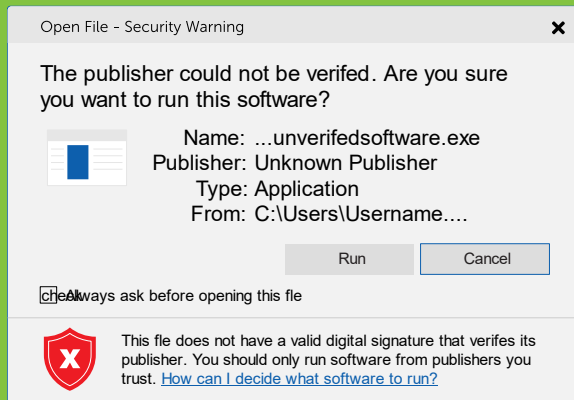
Benefits

ประโยชน์

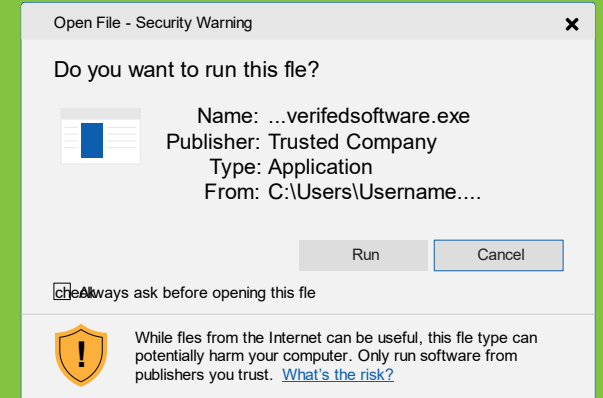
Unsigned Code

The end user is presented with a warning message that may cause them to abandon the install.

ผู้ใช้งานจะได้รับข้อความเตือนที่อาจทำให้พวกเขา
ละทิ้งการติดตั้ง



Unsigned
VS
Signed



Code Signed with Standard Certificate

The code has been digitally signed by a certificate from a trusted Certification Authority.

รหัสได้รับการลงนามแบบดิจิทัลโดยใบรับรองจากผู้ออกใบรับรองที่เชื่อถือได้

The end user is presented with the publisher's identity.

ผู้ใช้ปลายทางจะได้รับการนำเสนอตัวตนของผู้จัดพิมพ์.

Standard and EV

Benefits of Code Signing Certificates

- ✓ Signs applications and software
ลงนามแอปพลิเคชันและซอฟต์แวร์
- ✓ Proves legitimacy, identity, and prevents tampering
พิสูจน์ความถูกต้องตามกฎหมาย ตัวตน และป้องกันการปลอมแปลง
- ✓ Removes the "Unknown Publisher" pop-up
ลบป๊อปอัพ "ผู้เผยแพร่ที่ไม่รู้จัก"
- ✓ Full time stamping service included
รวมบริการประทับตราเต็มเวลา
- ✓ Increases the number of downloads and installs
เพิ่มจำนวนการดาวน์โหลดและการติดตั้ง

Code Signing

Use Cases

กรณีการใช้งานการลงนามโค้ด

Use Cases: Multiple Platform Support

กรณีการใช้งาน:

รองรับหลายแพลตฟอร์ม



Microsoft Authenticode

Code Sign any Windows 32 and 64 bit files including: .exe, .cab, .dll, .ocx, .msi, .xpi, and .xap, ActiveX controls, and kernel software



Microsoft Office

Code Sign any MS Office Macro or VBA file



Adobe AIR Office

Code Sign any Adobe AIR application.

Use Cases: Multiple Platform Support

กรณีการใช้งาน:

รองรับหลายแพลตฟอร์ม



Java

Code Sign any JAR applet.



Microsoft Office

Code Sign any MS Office Macro or VBA file



Mac

Code Sign any applications, plug-ins and content for Mac OS desktops

Difference From Regular Code Signing

Regular code signing certificates require less vetting to be performed.

ใบรับรองการเซ็นชื่อรหัสทั่วไปจำเป็นต้องมีการตรวจสอบน้อยกว่า

The Extended Validation Code Signing specification was developed and is maintained by the CA/Browser Forum (CABF) and is similar to EV SSL requirements:

ข้อมูลจำเพาะการลงนามรหัสตรวจสอบเพิ่มเติมได้รับการพัฒนาและดูแลโดย CA/Browser Forum (CABF) และคล้ายกับข้อกำหนด EV SSL:

1. Stricter Identity Verification: การยืนยันตัวตนที่เข้มงวดยิ่งขึ้น
 - Place of business address ที่อยู่สถานประกอบการ
 - Jurisdiction of Incorporation or Registration
เขตอำนาจศาลของการจดทะเบียนหรือจดทะเบียน
2. Insurance levels ระดับประกันภัย
3. Revocation and validation requirements
ข้อกำหนดการเพิกถอนและการตรวจสอบความถูกต้อง

EV CS guidelines can be found here <https://cabforum.org/ev-code-signing-certificate-guidelines/>



EV Code Signing

ใบรับรองการลงนามรหัส(EV)

EV Code Signing

What is EV Code Signing

EV Code Signing Certificates offer stronger levels of assurance that the identity of the publisher is correct and has been verified:

ใบรับรองการลงนามโค้ด EV มอบระดับความมั่นใจที่แข็งแกร่งยิ่งขึ้นว่าข้อมูลประจำตัวของผู้จัดพิมพ์นั้นถูกต้องและได้รับการตรวจสอบแล้ว:

- Higher level of assurance that code is free of viruses and spyware
ระดับความมั่นใจที่สูงขึ้นว่าโค้ดปราศจากไวรัสและสปายแวร์
- Intended to be used to verify the identity of the certificate holder (Subscriber) and the integrity of its code.

มีวัตถุประสงค์เพื่อใช้เพื่อตรวจสอบตัวตนของผู้ถือใบรับรอง (สมาชิก) และความสมบูรณ์ของรหัส

Why EV Code Signing

- Malware attacks continue to be a major threat
การโจมตีด้วยมัลแวร์ยังคงเป็นภัยคุกคามที่สำคัญ
- Higher assurances that code is safe to download
การรับประกันที่สูงขึ้นว่าโค้ดนั้นปลอดภัยในการดาวน์โหลด

Product Overview

✓ Client Certificate

✓ Code Signing - Standard and EV

- Displays company address and organization type
แสดงที่อยู่บริษัทและประเภทองค์กร

- Required for the Windows Hardware Development Center Dashboard Portal

จำเป็นสำหรับพอร์ทัลแพลตฟอร์มฮาร์ดแวร์ พัฒนาฮาร์ดแวร์

Windows

	Standard Code Signing Certificates	EV Validation (EV) Code Signing Certificates
Certificate Features		
Information displayed in Certificate	Organization Name	Organization Name Organization Address Type of Organization
Removes "Unknown Publisher" security warning	✓	✓
Signature does not expire when Time stamping is applied	Time stamping available & recommended	Time stamping available & recommended
Sign an unlimited number of applications	✓	✓
Compatible with major platforms (Authenticode, Office VBA, Java, Adobe AIR, Mac OS, Mozilla)	✓	✓
Key storage options	Cryptographic USB Token HSM Azure Key Vault Other hardware storage token SD Card or USB token	Cryptographic USB Token (included)^ HSM* Azure Key Vault
Certificate stored on hardware token	✓	✓

CodeSign Certificate Storage

Options for how the keys can be stored for both standard & EV

ตัวเลือกสำหรับวิธีจัดเก็บกุญแจสำหรับทั้งมาตรฐานและ EV



USB TOKEN



HSM (Hardware Security Module)



Azure Key Vault

GLOBAL

Questions?

คำถาม?

SIGN



We're here for you

A best-in-class partnering experience

