



Presenter: Chua Zhong Han



Enhancing Security:

The Push for Shorter Certificate Validity Periods

“การผลักดันให้มีระยะเวลาของใบรับรองที่สั้นลง”

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

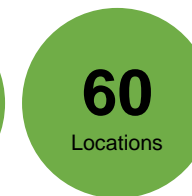
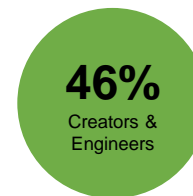
GLOBAL SCALE Developer

- 5,000 global partners
- 3 Global Data Centers

PROVEN EXPERTISE

- 30,000 customers
- 500 employees
- 60m identities issued
- 4m SSL Certificates
- 2b OCSP Responses/monthly

TRUSTED CERTIFICATE AUTHORITY



Trusted Around the World

เรา “GlobalSign” ได้รับ
ความไว้วางใจทั่วโลก



CUSTOMERS

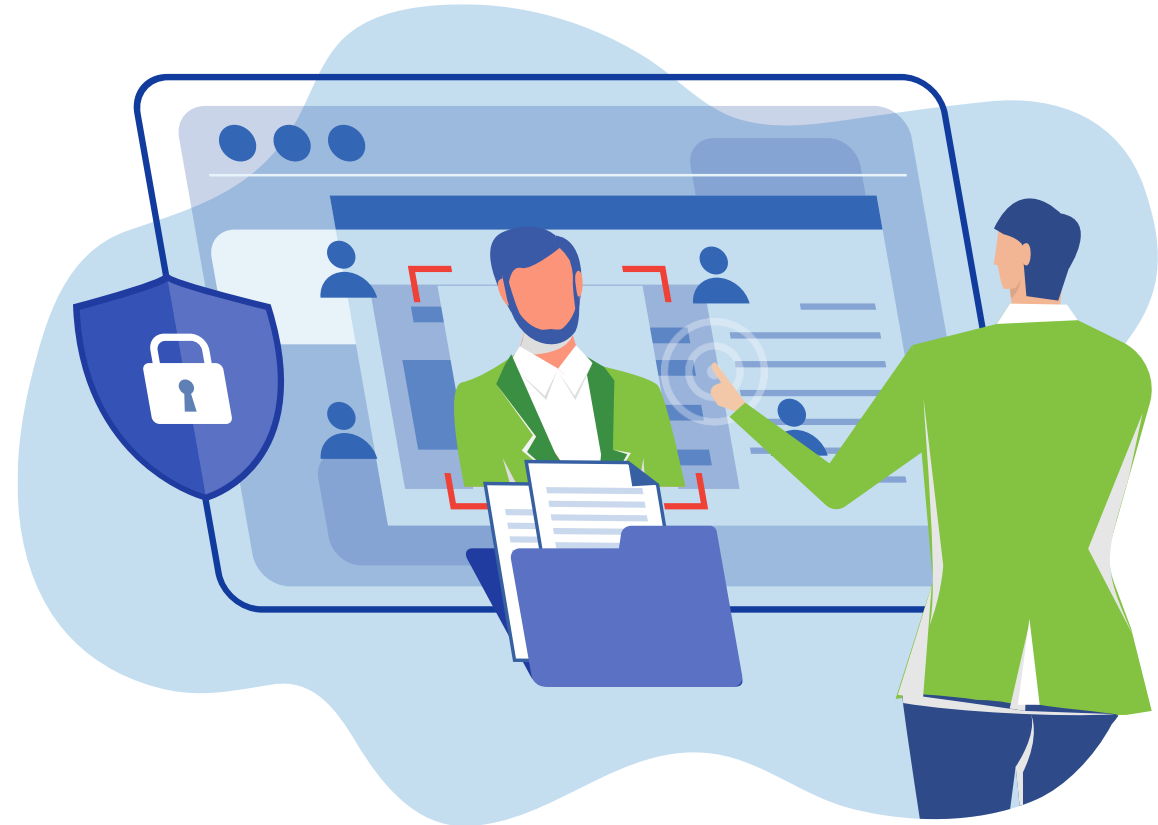


PARTNERS



Contents/สารบัญ

1. Shorter Certificate Validity Periods
(ใบรับรองดิจิทัลที่มีอายุสั้นลง)
2. GlobalSign's Solution (โซลูชันของ GlobalSign)
3. Certificate Automation Manager (CAM)
(ตัวจัดการใบรับรองอัตโนมัติ CAM)
4. GlobalSign's Integration
(การบูรณาการของ GlobalSign)
5. Questions? (คำถาม)



Shorter Certificate Validity Periods

ใบรับรองดิจิทัลที่มีอายุสั้นลง

Authorities are Shortening Validities (Why?)

Authorities are shortening certificate validity for several reasons, primarily related to security and the dynamic nature of digital environments

- **Enhanced Security:** Shorter certificate validity periods minimize the risk of prolonged exploitation of compromised certificates, limiting potential damage.
- การรักษาความปลอดภัยขั้นสูง: ระยะเวลาของใบรับรองที่สั้นลงจะช่วยลดความเสี่ยงในการใช้ประโยชน์จากใบรับรองที่ถูกบุกรุกเป็นเวลานาน ซึ่งลดความเสียหายที่อาจจะเกิดขึ้น
- **Cryptographic Agility:** Frequent updates due to shorter validity periods ensure the adoption of stronger cryptographic algorithms more quickly.
- ความคล่องตัวในการเข้ารหัส: การอัปเดตบ่อยครั้งและเนื่องจากระยะเวลาที่ใช้งานได้สั้นลง ช่วยให้มั่นใจได้ว่าการนำอัลกอริทึมการเข้ารหัสที่รัดกุมมากขึ้นมาใช้ได้อย่างรวดเร็วยิ่งขึ้น



- **Improved Management:** Regular renewals promote better control and adherence to best practices in certificate management.
- การจัดการที่ได้รับการปรับปรุง: การต่ออายุเป็นประจำส่งเสริมการควบคุมที่ดีขึ้นและการปฏิบัติตามแนวทางปฏิบัติที่ดีที่สุดในการจัดการใบรับรอง
- **Streamlined Administration:** Predictable renewal cycles reduce manual tasks and can be automated, simplifying certificate management.
- การดูแลระบบที่คล่องตัว: รอบของการต่ออายุที่คาดการณ์ได้ช่วยลดงานที่ต้องทำเองและสามารถทำให้เป็นแบบอัตโนมัติ และทำให้การจัดการใบรับรองนั้นง่ายขึ้น
- **Compliance and Trust:** Shorter lifetimes align with regulatory standards, ensuring up-to-date security practices and maintaining user trust.
- การปฏิบัติตามกฎระเบียบและความน่าเชื่อถือ: อายุการใช้งานที่สั้นลงสอดคล้องกับมาตรฐานด้านกฎระเบียบ ทำให้มั่นใจถึงแนวทางปฏิบัติด้านความปลอดภัยที่ทันสมัยและได้รับความไว้วางใจของผู้ใช้



Authorities (Who?)

- **Browser Vendors:** Companies like Google, Mozilla, Apple, and Microsoft advocate for shorter certificate validity periods to enhance security.
- **เป้าหมาย:** บริษัทอย่าง Google, Mozilla, Apple และ Microsoft สามารถปฏิบัติตามระยะเวลาของความถูกต้องที่สั้นลงเพื่อเพิ่มความปลอดภัย
- **Certificate Authorities (CAs):** Some Organizations would like to have a shorter validity to improve security practices and adapt to new cryptographic standards
- **ผู้ออกใบรับรอง (CA):** บางองค์กรต้องการให้มีความถูกต้องน้อยลงเพื่อปรับปรุงแนวทางปฏิบัติด้านความปลอดภัยและปรับให้เข้ากับมาตรฐานของการเข้ารหัสใหม่
- **Internet Security Organizations:** Groups such as the CA/Browser Forum, comprising browser vendors and CAs, recommend shorter lifetimes through guidelines.
- **องค์กรรักษาความปลอดภัยทางอินเทอร์เน็ต:** กลุ่มต่างๆ เช่น CA/Browser Forum ซึ่งประกอบด้วยผู้จำหน่ายเบราว์เซอร์และ CA แนะนำให้มีอายุการใช้งานที่สั้นลงตามหลักเกณฑ์
- **Cybersecurity Experts:** Professionals in cybersecurity endorse shorter validity periods to minimize the risk of compromised certificates and adopt newer, secure technologies.
- **ผู้เชี่ยวชาญด้านความปลอดภัยทางไซเบอร์:** ผู้เชี่ยวชาญด้านความปลอดภัยทางไซเบอร์รับรองระยะเวลาที่สั้นกว่าเพื่อลดความเสี่ยงของใบรับรองที่ถูกบุกรุกและนำเทคโนโลยีใหม่ที่ปลอดภัยมาใช้



What are the Impacts?

- **Increased Administrative Burden:** More frequent renewals require additional time and resources, potentially straining IT departments.
- **ภาระการบริหารที่เพิ่มขึ้น:** การต่ออายุบ่อยครั้งมากขึ้นต้องใช้เวลาและทรัพยากรเพิ่มเติม ซึ่งอาจทำให้แผนกไอทีมีความตึงเครียด
- **Higher Costs:** Regular renewals may increase the overall cost of certificate management, including purchase and administrative expenses.
- **ต้นทุนที่สูงขึ้น:** การต่ออายุเป็นประจำอาจเพิ่มต้นทุน โดยรวมในการจัดการใบรับรอง รวมถึงค่าใช้จ่ายในการซื้อและบริหาร
- **Risk of Expiration:** With more frequent renewals, there's a higher risk of certificates expiring if renewals are not managed properly, leading to potential service disruptions.
- **ความเสี่ยงของการหมดอายุ:** ด้วยการต่ออายุบ่อยขึ้น ใบรับรองจะหมดอายุมากขึ้นหากไม่ได้รับการจัดการการต่ออายุอย่างเหมาะสมส่งผลให้บริการนั้นหยุดชะงัก



What are the Impacts?

- **Need for Automation:** Organizations may need to invest in automated certificate management solutions to handle the increased frequency of renewals, which can be costly and complex to implement.
- **ความต้องการระบบอัตโนมัติ:** องค์กรต่างๆ อาจจำเป็นต้องลงทุนในโซลูชันการจัดการใบรับรองอัตโนมัติเพื่อรองรับความถี่ในการต่ออายุที่เพิ่มขึ้น ซึ่งอาจมีค่าใช้จ่ายสูงและมีความซับซ้อนในการดำเนินการ
- **Compatibility Issues:** Some older systems and applications may have difficulties handling frequent certificate changes, leading to potential compatibility issues.
- **ปัญหาความเข้ากันได้:** ระบบและแอปพลิเคชันรุ่นเก่าบางระบบอาจมีปัญหาในการจัดการกับการเปลี่ยนแปลงใบรับรองบ่อยครั้ง ซึ่งนำไปสู่ปัญหาความเข้ากันได้ที่น่าจะเกิดขึ้น
- **Increased Complexity:** The certificate management process becomes more complex with shorter validity periods, requiring more rigorous tracking and documentation.
- **ความซับซ้อนที่เพิ่มขึ้น:** กระบวนการจัดการใบรับรองมีความซับซ้อนมากขึ้น โดยมีระยะเวลาใช้งานได้สั้นลง ทำให้ต้องมีการติดตามและการจัดทำเอกสารที่เข้มงวดมากขึ้น



GlobalSign's Solution

โซลูชันของ GlobalSign's

GlobalSign's Solution

ACME: Automated Certificate Management Enrollment

ACME: การจัดการใบรับรองอัตโนมัติ

Designed by the Internet Security Research Group (ISRG)

ACME is a protocol for automated certificate issuance between an ACME agent on a web server and a CA's ACME service for issuance of TLS certificates

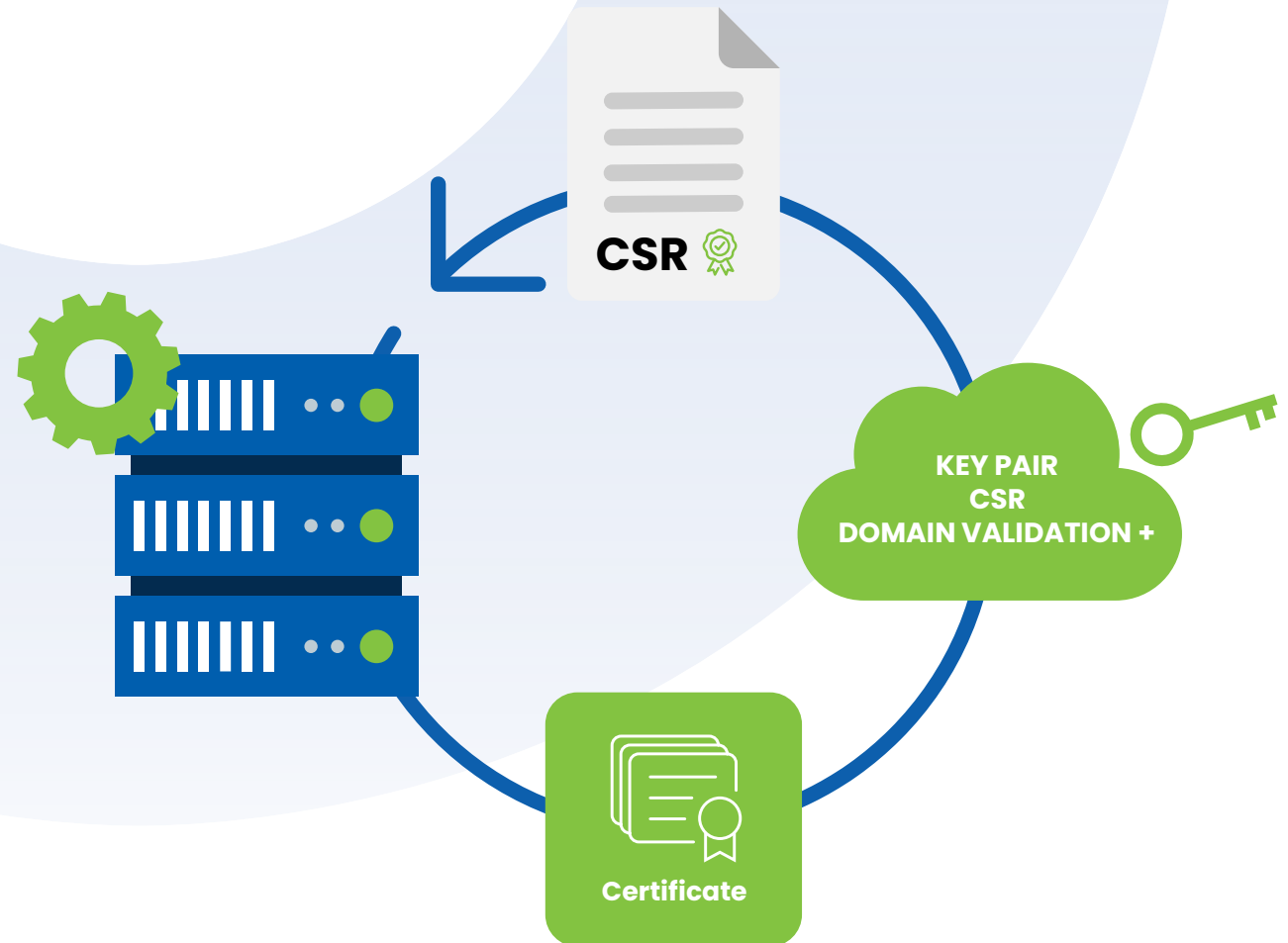
Internet standard (RFC8555) adopted by many CAs

Resembles a traditional CA's issuance process: domain validation + certificate issuance



ACME (How it works?)

- **Two players: ACME Server and ACME Agent on webserver**
 - **ACME Server: GlobalSign** (เซิร์ฟเวอร์ ACME: GlobalSign)
 - **ACME Agent: "Certbot"** (ตัวแทน ACME: "Certbot")
- **Agent generates key pair & CSR** (ตัวแทนสร้างคู่มือ & CSR)
- **Agent does domain validation** (ตัวแทนทำการตรวจสอบโดเมน)
- **Agent sends CSR to CA** (ตัวแทนส่ง CSR ไปยัง CA)
- **CA issues the certificate** (CA ออกใบรับรอง)
- **Agent installs certificate on webserver**
(ตัวแทนติดตั้งใบรับรองบนเว็บเซิร์ฟเวอร์)
- **Agent creates a scheduled task for autorenewal**
(ตัวแทนสร้างงานตามกำหนดเวลาสำหรับการต่ออายุอัตโนมัติ)



Certificates Available

- TLS DV & OV certificates
- HTTP/DNS validation methods
- Public trust certificates
- Private trust certificates
- Wild cards
- SANs
- Atlas only
- Available “globally”!



Certificate Automation Manager (CAM)

ตัวจัดการใบรับรองอัตโนมัติ (CAM)

What is CAM?

What Is It?

CAM is a fully featured certificate solution that allows for the automatic provisioning, management and reporting of all types of certificates in an organization.



Cam เป็นโซลูชันที่โดดเด่นที่มีวิธีการแก้ปัญหาที่อนุญาตสำหรับไฟล์การจัดเตรียมอัตโนมัติการจัดการและการรายงานทั้งหมดประเภทของใบรับรองในไฟล์องค์กร

What Does It Do?

It removes the manual process of managing requests, permissions, provisioning, configuring and overall management of certificates.

This significantly improves operation efficiency, as well as reducing risks of security breaches and downtime.



ลบกระบวนการแมนนวลของการจัดการคำขอการอนุญาต การจัดเตรียมการกำหนดค่าและการจัดการใบรับรอง โดยรวมสิ่งนี้ อย่างมีนัยสำคัญประสิทธิภาพการดำเนินงาน เช่นเดียวกับการลดความเสี่ยงของการละเมิดความปลอดภัย และการหยุดทำงาน

How Does It Work?

Leverages our APIs, it issues all certificate types by utilizing directory services and MDMS for policy distribution.

CAM is installed on Windows VMs and hosted using IIS.



ใช้ประโยชน์จาก APIs, ของเรา ทั้งหมดประเภทใบรับรอง โดยใช้บริการไดเรกทอรีและ MDMs สำหรับการกระจายนโยบาย CAM ติดตั้งบน Windows VMS และโฮสต์โดยใช้ IIS

KEY FEATURES



ACME SUPPORT

Automated issuance to any client application supporting ACME such as Linux servers and DevSecOps tools

Acme Support

การออกโดยอัตโนมัติให้กับลูกค้าทุกรายแอปพลิเคชันที่รองรับ ACME เช่น Linux Servers และเครื่องมือ Devsecops



SCEP SUPPORT

SCEP supports issuing certificates to mobile and networking devices alongside integrations with Microsoft Intune, JAMF and other MDMs

การสนับสนุน SCEP

SCEP สนับสนุนการออกใบรับรองไปยังอุปกรณ์มือถือและเครือข่ายควบคู่ไปกับการรวมเข้ากับ Microsoft, Intune, Jamf และ MDM อื่น ๆ



KEY ARCHIVAL, RECOVERY AND ROAMING

Allows for the secure archival of encryption keys to maintain consistent access and mitigate data loss caused by lost keys

คีย์เก็บถาวร,การกู้คืน และโรมมิ่ง

อนุญาตให้มีการเก็บถาวรที่ปลอดภัยของปุ่มเข้ารหัสเพื่อรักษาการเข้าถึงและลดข้อมูลที่สอดคล้องกันการสูญเสียที่เกิดจากคีย์สูญหายที่หายไป

KEY FEATURES

การจัดการที่ง่ายขึ้น และการรายงาน
เปิดใช้งานแดชบอร์ด UI ที่ใช้งานง่ายผู้ดูแลระบบเพื่อจัดการการปรับใช้
ตัวเลือกและโปรโตคอลสร้างกำหนดเวลาและกำหนดเองได้รายงาน

ระบบอัตโนมัติ PKI
ออกโดยอัตโนมัติและติดตั้งใบรับรองโดยไม่จำเป็นต้องใช้การ
แทรกแซงของพนักงานนโยบายและการกำหนดค่าในการใช้งาน
ไคลเอนต์และ Entra ID (Azure)

สภาพแวดล้อมปลายทางแบบผสมผสาน
ตัวแทนข้ามแพลตฟอร์ม (XPA)ติดตั้งได้อย่างง่ายดายบนเวิร์กสเตชัน
หรือเซิร์ฟเวอร์สำหรับ Windows, MacOS และ Linux



SIMPLIFIED MANAGEMENT AND REPORTING

Easy to use UI dashboard enables administrators to manage deployment options and protocols, generate scheduled and custom exportable reports



PKI AUTOMATION

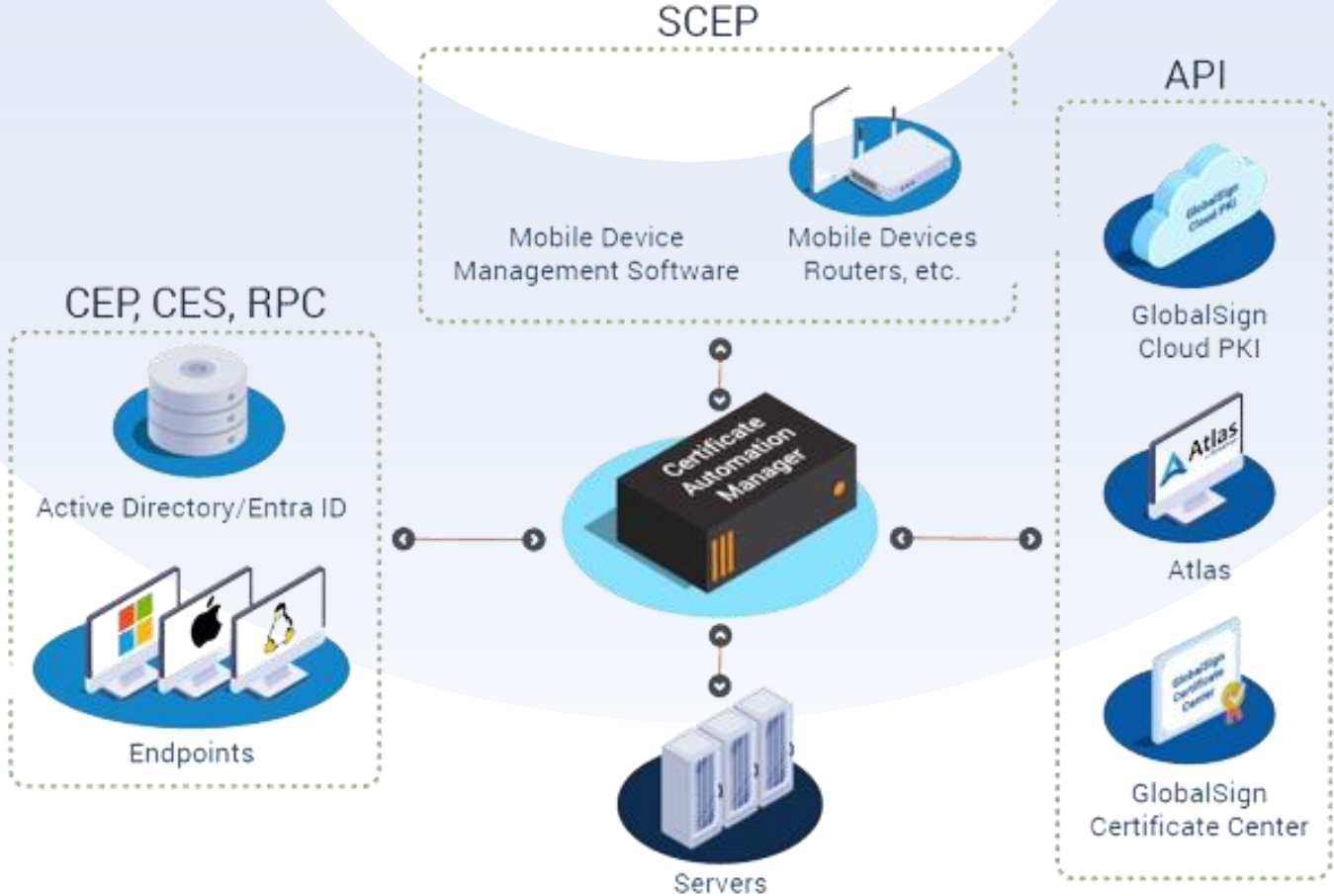
Automatically issue and install certificates without the need for employee intervention utilizing policies and configurations in Active Directory and Entra ID (Azure)



MIXED ENDPOINT ENVIRONMENTS

The Cross-Platform Agent (XPA) installs easily on any workstation or server for Windows, MacOS and Linux

CAM SOLUTION



What Endpoints are Supported?

อุปกรณ์ปลายทางใดบ้างที่รองรับ?

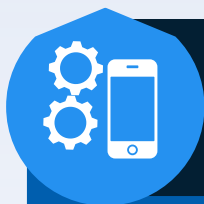


CERTIFICATE AUTOMATION
MANAGER SUPPORTS NATIVE
CERTIFICATE ENROLLMENT ON:

- From Windows Server 2016 and Windows 10.
- To latest windows platform.

ผู้จัดการสนับสนุนการลงทะเบียนใบรับรอง:

- จาก Windows Server 2016 และ Windows 10
- ไปยัง Windows ล่าสุดแพลตฟอร์ม

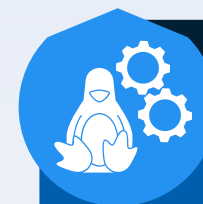


CERTIFICATE AUTOMATION
MANAGER SUPPORTS THE
SIMPLE CERTIFICATE
ENROLLMENT PROTOCOL
(SCEP) FOR:

- Network Devices
- MDM managed devices (Mobile, workstations etc)

ใบรับรองอัตโนมัติผู้จัดการรองรับใบรับรองง่ายๆ
โปรโตคอลการลงทะเบียน (SCEP) สำหรับ:

- อุปกรณ์เครือข่าย
- อุปกรณ์ที่มีการจัดการ MDM (มือถือเวิร์กสเตชัน ฯลฯ)



CERTIFICATE AUTOMATION
MANAGER SUPPORTS ACME
FOR ENROLLMENT OF:

- Linux Servers using existing ACME clients

ใบรับรองอัตโนมัติผู้จัดการสนับสนุน ACME สำหรับการลงทะเบียนของ:

- เซิร์ฟเวอร์ Linux โดยใช้ลูกค้า ACME ที่มีอยู่

SMIME: Key Archival and Recovery

(การกู้คืนคีย์และการเก็บถาวร)

- **The loss of private keys can jeopardize the confidentiality, integrity or availability of stored data**
- การสูญเสียคีย์ส่วนตัวอาจเป็นอันตรายต่อการรักษาความลับหรือความพร้อมใช้งานของข้อมูลที่จัดเก็บ
- **Every client certificate issued by Certificate Automation Manager has a unique private key**
- ใบรับรองไคลเอ็นต์ทุกใบที่ออกโดย Certificate Automation Manager จะมีคีย์ส่วนตัวที่ไม่ซ้ำกัน
- **Those private keys are used for encryption and decryption, either for digital signatures on data objects or data directly (S/MIME)**
- คีย์ส่วนตัวเหล่านั้นใช้สำหรับการเข้ารหัสและถอดรหัส ไม่ว่าจะเป็นการลายเซ็นดิจิทัลบนออบเจกต์ข้อมูลหรือข้อมูลโดยตรง (S/MIME)

Therefore, the ability to create a (highly secure) backup for private keys and being able to (securely) restore them is highly sought after

Archived keys are protected by encryption with another key, the so-called Key Recovery Agent (KRA) key and an associated certificate



Who is CAM for?

- **SME's to large Enterprise running Windows or hybrid environments and utilizing Active Directory or Medium organizations: up to 5,000 Users - Sweet Spot**
- SME ไปจนถึงองค์กรขนาดใหญ่ที่ใช้ Windows หรือสภาพแวดล้อมแบบไฮบริดและใช้ Active Directory หรือองค์กรขนาดกลาง: ผู้ใช้สูงสุด 5,000 คน
- **Large organizations (multi-AD Forests): 5,000+ users - Ideal Customers**
- องค์กรขนาดใหญ่ (หลาย AD Forests): ผู้ใช้มากกว่า 5,000 ราย
- **Those organizations requiring strong multi-factor mutual authentication based digital certificates (and optionally tokens)**
- องค์กรเหล่านั้นต้องการใบรับรองดิจิทัลที่ใช้การรับรองความถูกต้องร่วมกันแบบหลายปัจจัยที่แข็งแกร่ง (และโทเค็นเสริม)
- **Organizations looking to deploy S/MIME (Secure email) at scale**
- องค์กรที่ต้องการปรับใช้ S/MIME (อีเมลที่ปลอดภัย) ในวงกว้าง
- **Organizations with mission critical PKI operation requiring 24x7 service availability**
- องค์กรที่มีการปฏิบัติการ PKI ที่สำคัญต่อภารกิจซึ่งต้องการความพร้อมให้บริการทุกวันตลอด 24 ชั่วโมง
- **Organizations looking to reduce their TCO around PKI deployments.**
- องค์กรที่ต้องการลด TCO ของตนเกี่ยวกับการปรับใช้ PKI



Further information on CAM

Blogpost
<https://www.globalseg.com/en/enterprise/management-automation/certificate-automation-manager>
Support Information
<https://support.globalseg.com/Certificate-Automation-Manager>

Current CAM Customers

Company	REGION	DEDICATED CA/PUBLIC SHARED	USE CASE	CONTEXT
SHISEIDO	JP	DEDICATED CA	<ul style="list-style-type: none"> •Client Auth (VPN/BOX) •Intune / JAMF 	•Private trust
National Institute of Advanced Industrial Science and Technology (AIST)	JP	DEDICATED CA	<ul style="list-style-type: none"> •Client Auth (VPN) •Intune 	•Public Trust
China Trust Bank - CTBC Bank USA	AMER	DEDICATED CA	<ul style="list-style-type: none"> •TLS Server Authentication •Client Authentication 	
MidFirst Bank	AMER	PUBLIC SHARED	<ul style="list-style-type: none"> •TLS Server Authentication •Client Authentication 	
Swift	EMEA	BOTH	<ul style="list-style-type: none"> •TLS Server Authentication •Client Authentication (User) •SMIME •Key recovery & archival 	
Vlaamse Overheid (Flemish Government)	EMEA	DEDICATED CA	<ul style="list-style-type: none"> •TLS Server Authentication •Client Authentication •Intune 	

GlobalSign's Integration

การบูรณาการของ GlobalSign

GlobalSign's integration with other CLMs

	Extended Validation(EV)	Organization Validated(OV)	Domain Validated(DV)
Microsoft Azure KeyVault	-	<ul style="list-style-type: none">- Auto Renewal- Key Rotation- Auto CSR	-
ServiceNow	-	-	<ul style="list-style-type: none">- Auto Renewal- Key Rotation- Auto CSR
AppviewX	<ul style="list-style-type: none">- Auto Renewal- Key Rotation- Auto CSR	<ul style="list-style-type: none">- Auto Renewal- Key Rotation- Auto CSR	<ul style="list-style-type: none">- Auto Renewal- Key Rotation- Auto CSR

Questions?

คำถาม?



We're here for you

A best-in-class partnering experience

