GlobalSign

VP Strategic Sales - EMEA

| Senior Executive GlobalSign - Belgium |

RONALD DE TEMMERMAN

T +32 (0) 16 891908 | **M** +32 (0) 495 581037

Email: ronald.detemmerman@globalsign.com

Web: www.globalsign.com | www.globalsign.eu

GlobalSign NV | Martelarenlaan 38 | Leuven | B-3010 | Belgium
GlobalSign Ltd | Springfield House | Sandling Road | Maidstone | Kent | ME14 2LP | UK

GlobalSign
GMO INTERNET GROUP

CIE of Lebanon (CIEL) / GlobalSign
Tel: +961 1 28 5666 x 201
Cell: +961 71 28 5666 x 201
https://www.globalsign.com.lb

CIEL
LEBANON

Dr Salah A. Rustum
President

Agenda for today

- Introduction
  - Presenter
  - Setting the Stage
  - About GlobalSign

- CA Services, an overview

- Identity & Access Management solutions
  – Insurance Business – IAM Changes
  – Sample Customers & Use Case

- PKI to Rescue
  – Role of Identity & Security
  – Fully automated, scalable PKI solutions

- AATL - Document Signing Solution

Setting the Stage

GlobalSign.

- Privacy, safety, and security are becoming more distinguishing factors in ANY consumer related business and for most industrial applications

- Increased Threats, Compliance Security is key

- The value of your business transactions cannot be realized without the implementation of strict (device) security and identity mechanisms

- Leverage existing technologies to build security and identity into the Insurance ecosystems

Identity for Everything™

Identity is Fundamental to Online Security.

GlobalSign uses its managed PKI & IAM experience and technology to build high-volume, high-scale identity management solutions for the billions of devices, people and things comprising the Internet of Everything.
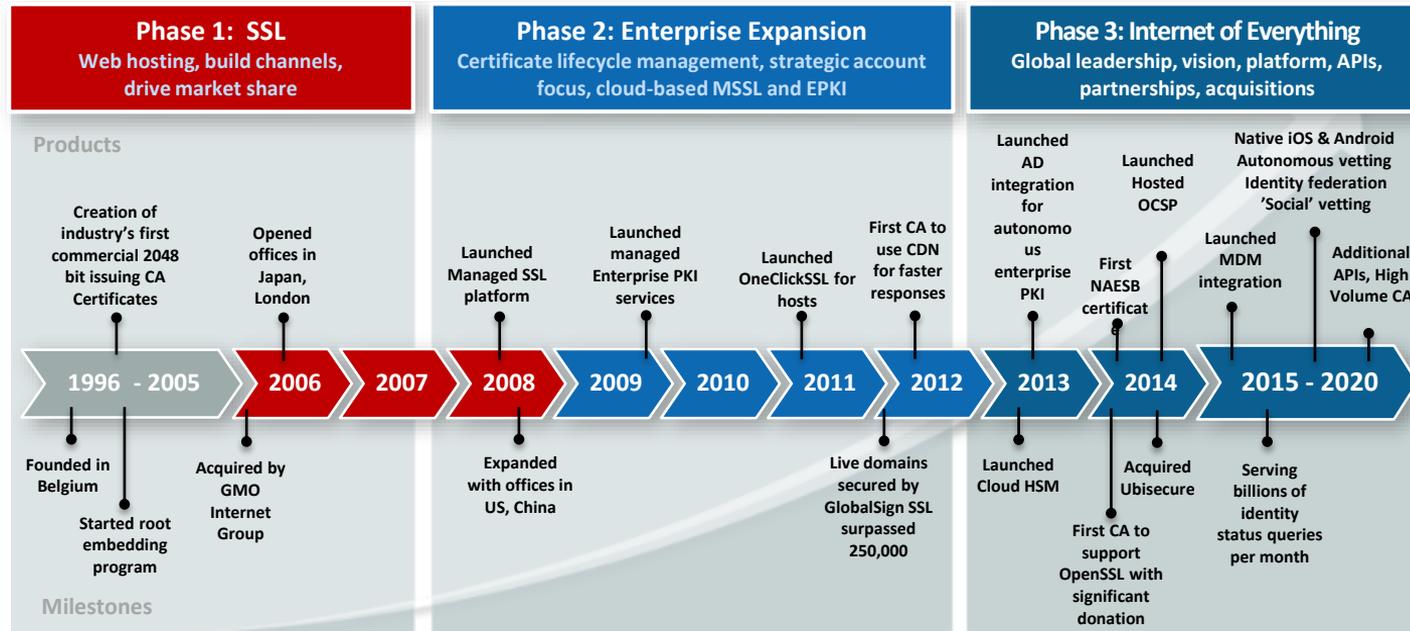
GlobalSign
GMO INTERNET GROUP

About GlobalSign

GlobalSign

Helsinki
IAM Center

London

Brussels & Paris
CA Infrastructure

Boston

India
Offshore services

Tokyo

Philippines
Offshore services

Singapore
CA Infrastructure

| 300 employees | >5,000 global partners | > 30,000 customers | >10m identities issued, 2.5M live SSL Certs |

Progress towards the mission

GlobalSign.

Phase 1: SSL
Web hosting, build channels, drive market share

Phase 2: Enterprise Expansion
Certificate lifecycle management, strategic account focus, cloud-based MSSL and EPKI

Phase 3: Internet of Everything
Global leadership, vision, platform, APIs, partnerships, acquisitions

Products

Creation of industry's first commercial 2048 bit issuing CA Certificates

Opened offices in Japan, London

Launched Managed SSL platform

Launched managed Enterprise PKI services

Launched OneClickSSL for hosts

First CA to use CDN for faster responses

Launched AD integration for autonomous enterprise PKI

Launched Hosted OCSP

Native iOS & Android Autonomous vetting Identity federation 'Social' vetting

First NAESB certificate

Launched MDM integration

Additional APIs, High Volume CA

1996 - 2005	2006	2007	2008	2009	2010	2011	2012	2013	2014	2015 - 2020

Founded in Belgium

Started root embedding program

Acquired by GMO Internet Group

Expanded with offices in US, China

Live domains secured by GlobalSign SSL surpassed 250,000

Launched Cloud HSM

Acquired Ubisecure

First CA to support OpenSSL with significant donation

Serving billions of identity status queries per month

Milestones

kuppingercole
ANALYSTS

"GlobalSign is a Product Leader. Innovation Leader."

10

Challenges GlobalSign solves

- Increase security and online trust by providing strong identities

- Reduce costs and time taken to deploy enterprise wide PKI

- Manage certificate related risk (weak crypto, expirations, self-signed, unknown inventory)

- Reduce time taken to deploy IAM solutions from months to weeks

- Manage high volumes of identities for IoT/IoE deployments
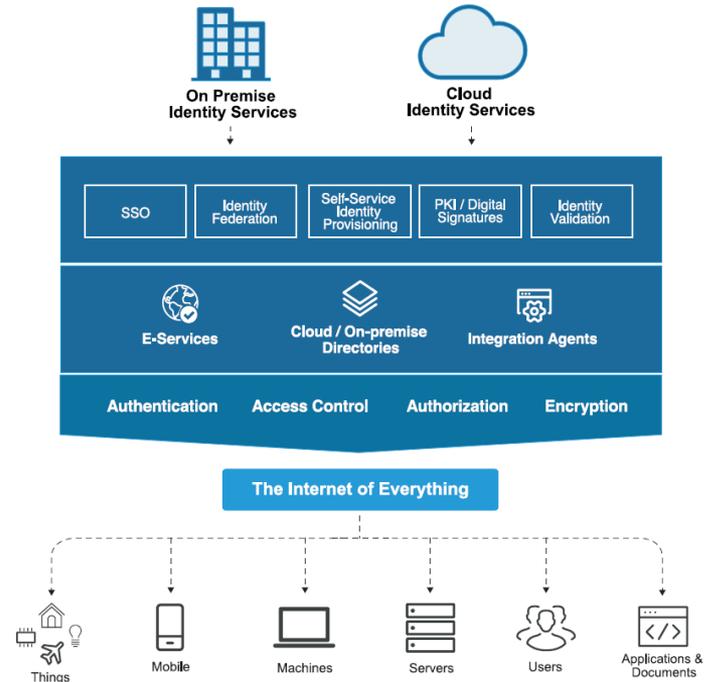
Identity Service Ecosystem
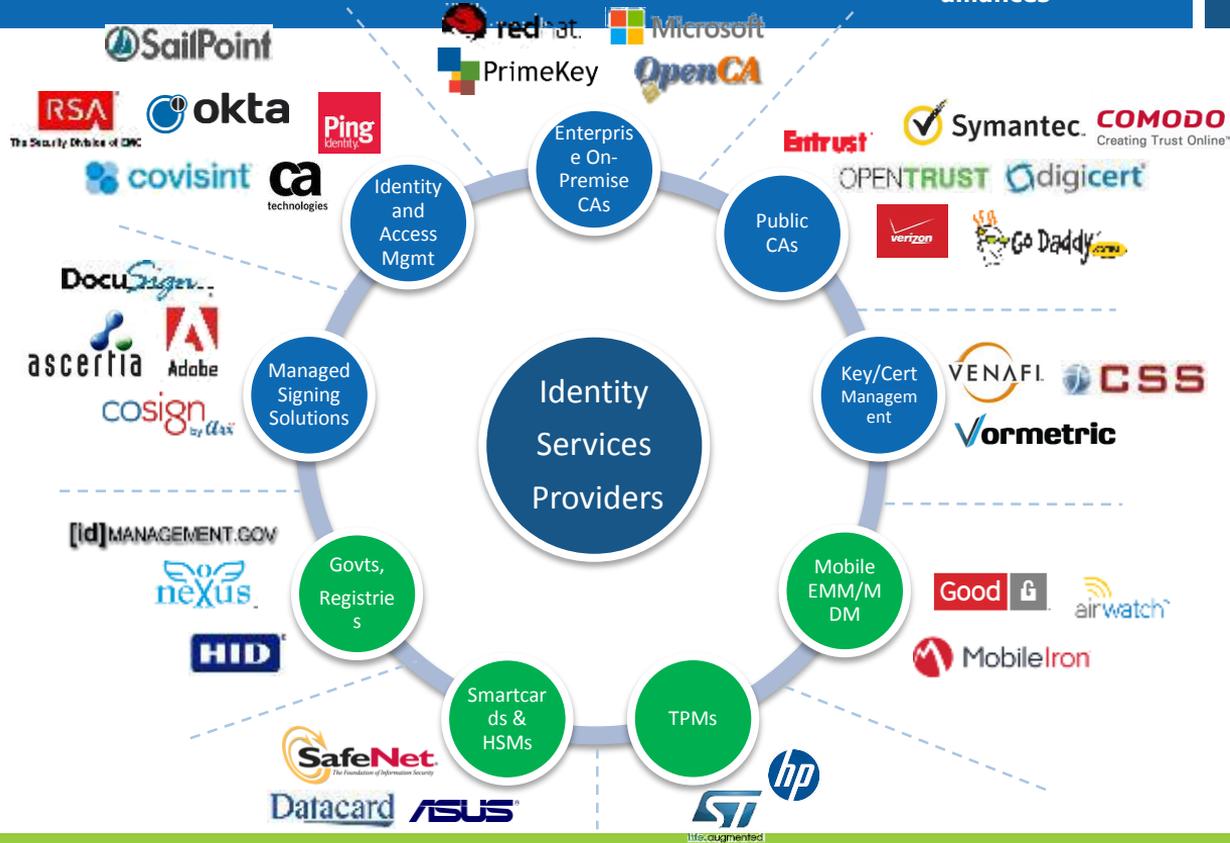
Example Customers & Partners

CA Services

PDF Signing Service Providers

Partners

Technology & Solutions

Identity for Everything – Core Technologies

- High-volume, high-scale identity management

- Cloud and on premise solutions

- Ease of deployment, automation capabilities

- Integration with enterprise services

CA Services

Identity and Access Management

GlobalSign CA Services

Digital certificates

PKI Development

CA Services – Value Proposition

- Holistic approach to enterprise Certificate Lifecycle Management to reduce risk and ensure compliance

- API driven automation of high volume PKI deployments with AD integration and MDM agents, ideal for IoT use cases

- Various pricing / business models (unlimited issuance licenses, deposit method, pay-as-you-go)

- Full suite of CA services (timestamping, Hosted OCSP, Hosted HSM, root signing, etc.)

CA Platform continues to evolve

- WebTrust Certified
- CA/B Forum compliant
- Revocation Services
- CDN
- Scalable
- Geo Redundancy

CA Operations

Lifecycle Management

- SaaS CA
- Portal for easy management
- Auto-Enrolment Gateway for MSFT Active Directory
- API for custom development

Extended Services

- Root Signing, hosted or private
- Timestamping
- Doc Signing
- HSM, hosted or private
- OCSP responses

PKO

- SSL
- Smartcard / token-based Authentication
- S/MIME
- Code Signing
- Document Signing

GlobalSign – Identity and Access Management Solutions
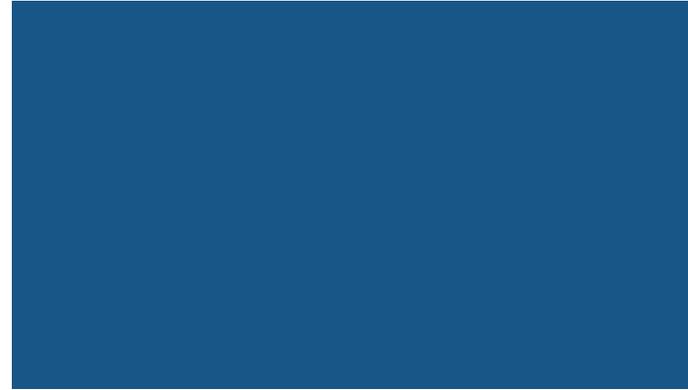
Customer-Centric Out-of-the-box IAM solution
for *securing e-Services*

1) eService Provider Challenges
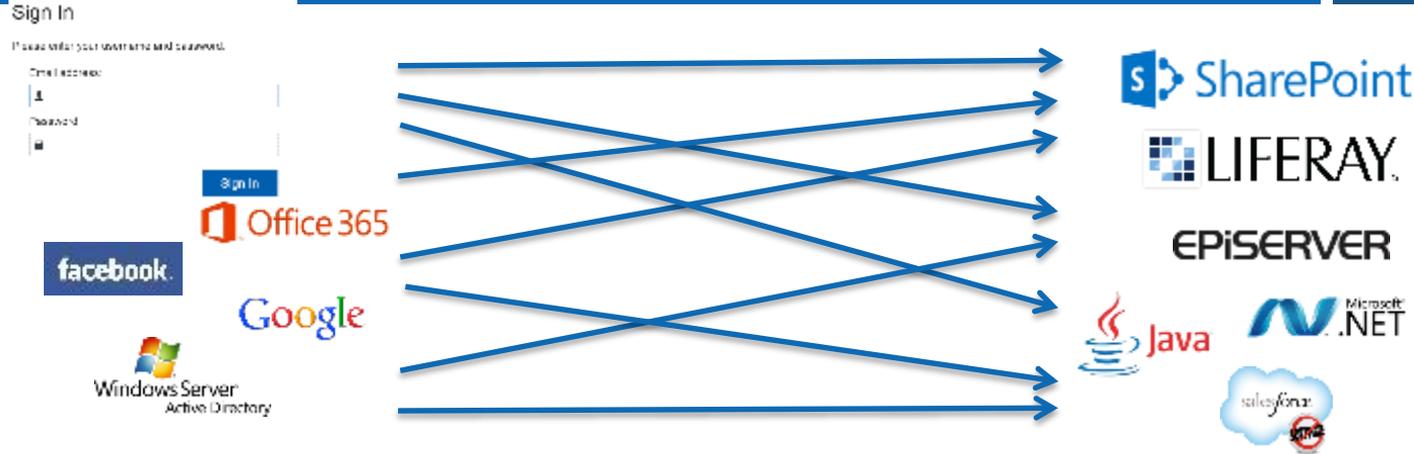
- Multiple eService specific credentials / passwords
- On-boarding inconvenient for the user and costly for you
- User identity management creates customer service costs
- Difficult to determine if user is authorized to access the service
- Online transactions are costly to confirm

2) Identity and Access Management Evolution

Employee-Centric IAM

Customer-Centric IAM

Flat

Connected

- Internal, employee focus
- HR and IT driven
- Access based on job role
- Process and cost efficiency

- External, customer focus
- Marketing and on-line driven
- Access based on relationship
- Customer intake and efficiency

3) Improving the User Experience

Customers can manage their own identity lifecycle

- Bring your own ID, identity self-service
- Tiered delegated administration

Convenient access to online servic

- Web SSO
- Role based access
- Federation
- Social Login

4) Actionable Business Intelligence

How Well Do You Know Your Customers?

- Leverage your IAM solution to update your customer data
  - Customer data is your greatest asset
  - No visibility into customers identity lifecycle
- Bi-directional data synching
  - Customers maintain identity

Changes in the Insurance Business…

- "…technological change has created new and potentially superior distribution and communication channels that are changing both the nature of the business and relationship management." *– PWC*

- "Eventually, insurers will need to position themselves to respond quickly to changing customer expectations in an increasingly digital and connected life." *– InformationWeek*

25

Digital Business Implications

- "Right Here, Right Now" Expectations
- Omni-channel & Self-service
- Multiple Personas Per Customer
- Strict Compliance Requirements
- Providing Appropriate Access

Unique Offering

Able to address industry trends:

- Flexible & Scalable
- Extensive APIs
- Service contracts for Delegated Role Management
- Extensive Authentication Methods
- CRM Integration

Business Proposition

In Summary…

With the unique offerings of GlobalSign's IAM Solution, you will be able to address the key aspects of the online Insurance business by:

- Faster launching of online services to maintain competitive advantage

- Address the multiple interactions and identities each customer has with your organization online

- Empower the customer to manage their own identity and relieve the amount of effort required from your customer service teams

Insurance IAM Ecosystem

Relationships and Integrations
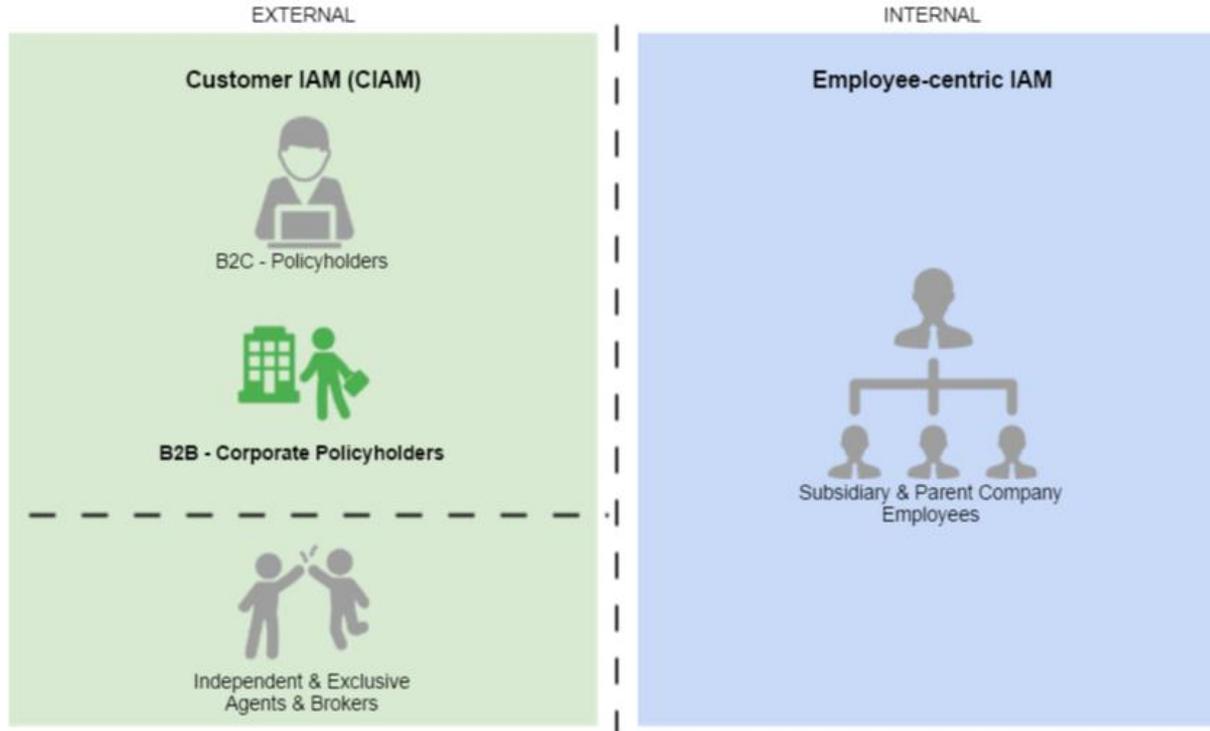
Relationships:
- Service Contracts
- Technological Contracts

Integrations:
- APIs
- CRM

DIY - Identity Self-Service

Up-to-date user information through self-service identity management

DIY - Tiered Delegation

GlobalSign.

Customer care cost savings by empowering customers to manage their own services.

CRM Account Linking

Cost savings and security risk mitigation by linking the user roles to the CRM contract life-cycle

Etera: Insurance Company

Etera is a mutual employment pension insurance company providing pension cover for employees and self-employed persons.

Challenges

- Employers need to report paid salaries on a monthly basis to the pension insurance company, and handling paper based reports was very expensive
- There was no way for Etera customers to conveniently review their own pension information

Solution

- GlobalSign SSO was deployed to provide strong authentication for the customers to access their pension information
- For the organizations reporting paid salaries on a monthly basis Etera selected to use the password method of GlobalSign SSO and GlobalSign Trust enabled Danske-Bank employees to single sign-on to Etera services

Benefits

- Considerable cost savings by enabling online and automated reporting for the customer organizations and accounting companies
- Increased customer satisfaction as employees could now access their pension information conveniently – better user experience

GlobalSign - IAM Services

TCO and e-service lifecycle benefits

Business growth benefits

CustomerID

Customer and user registration

Increase your inflow of customers!

SSO

SSO and access management

Benefit of delegated management!

TRUST

Federated identities and access

Use e-mandates and e-Power of Attorney

CONFIRM

Business transaction confirmation

Let your customers enter securely without obstacles!

- Out-of-the-box IAM solution for *securing e-Services*

- One platform – 4 products for

  1. Single Sign-On
  2. Role and customer data mgmt
  3. Identity federation
  4. Transaction confirmation

- Robust and proven with standard interfaces

- Rapid deployment

Fully automated, scalable PKI solutions for mixed enterprise environments

Keeping your emails private and protecting against spear phishing with PKI

PKI is tried and true InfoSec solution

Server security

User, Machine, & Device Authentication

Network Security

PKI

Document Signing

Email Security & Encryption

PKI is tried and true InfoSec solution

GlobalSign.
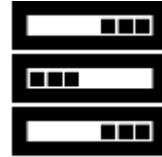
But can it handle modern enterprise environments?

PKI Hurdles

- Most of the concerns about higher volume deployments and mixed environments come down to certificate provisioning and management
  - Registering for the certificates
    - How do you get the correct identifying information onto the certificate?

PKI Hurdles

- Most of the concerns about higher volume deployments and mixed environments come down to certificate provisioning and management
  - Registering for the certificates
  - Provisioning and installing the certificates
    - How do you actually get the certificates onto the endpoints?
    - How do you know which endpoints get which types of certificates?

PKI Hurdles

- Most of the concerns about higher volume deployments and mixed environments come down to certificate provisioning and management
  - Registering for the certificates
  - Provisioning and installing the certificates
  - Ongoing lifecycle management
    - New hires, new devices and machines will require new certificates
    - Lost devices or employee turnover will require revocation
    - Renewals

You already have some of the key pieces!

- Leverage existing technology investments
  - You already have a repository of authenticated users and machines.
  - You already have a robust policy management solution.
  - Your clients already support certificate lifecycle management.

Active Directory and PKI

GlobalSign.
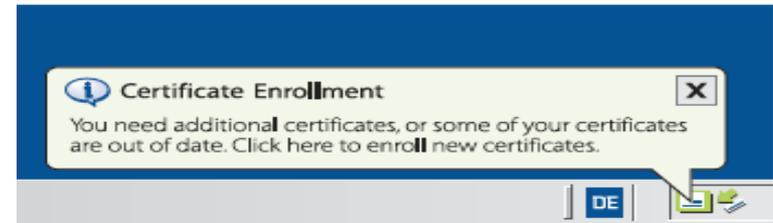
- Automatically provision certificates to all domain-joined endpoints
- Silent installs
- Support a range of templates and use cases
- Configure Active Directory Group Policies to control which objects receive which certificates

Running a Microsoft CA is Complicated

- Need dedicated resources and staff
  - PKI expertise and detailed logging, documentation
- Manage CA operations
  - Maintain uptime and reliability
  - Keep up with PKI best practices
  - Secure operations and infrastructure

What about non-Windows endpoints?

Provisioning to non-domain endpoints
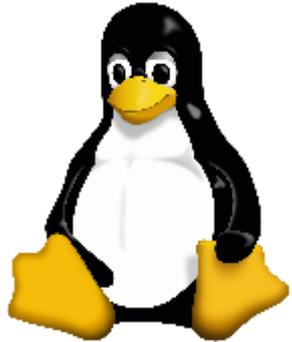
- SCEP
- ACME protocol
- MDM connectors

- **SCEP-based Enrollment**
  - Widely used protocol for issuing certificates to mobile devices
  - Not all CAs support

- **MDM/EMM Integration**
  - Automatically issue certificates to any devices registered with the MDM
  - Not all CAs support

One solution for all endpoints!
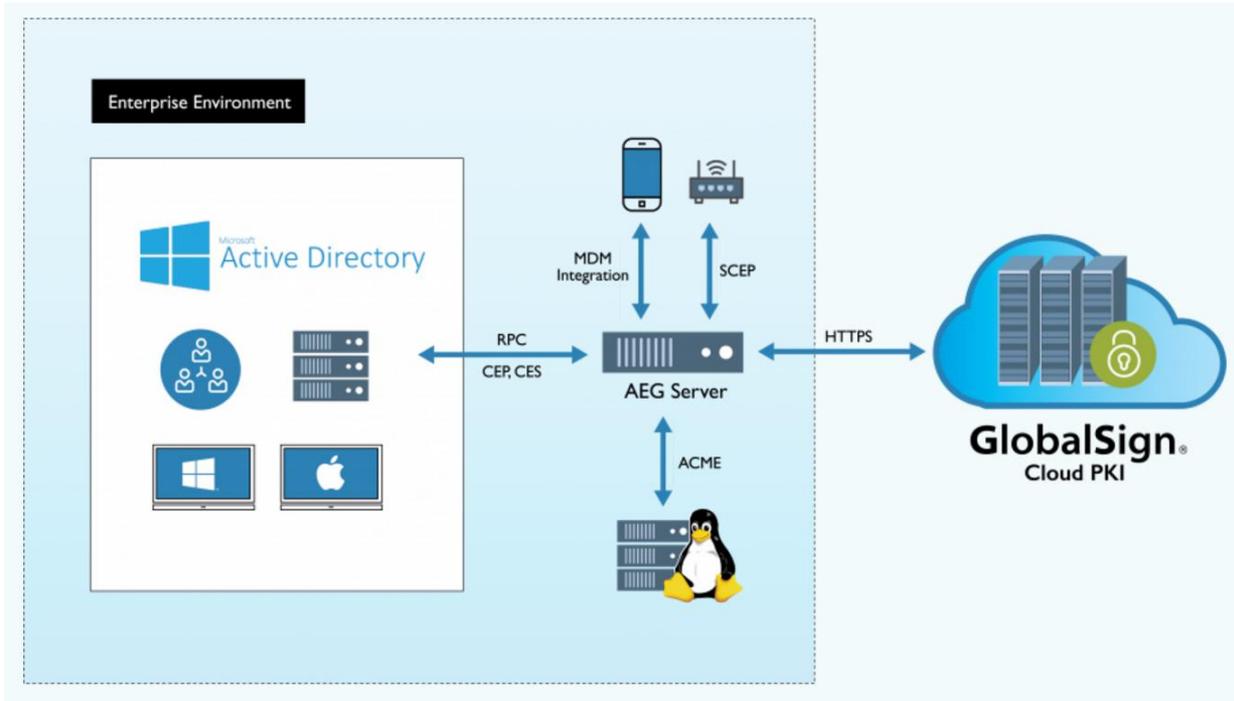
GlobalSign Auto Enrollment Gateway

PKI Automation for Mixed Environments

- Outsource PKI management to a trusted, third party CA

- Reduce total cost of ownership by as much as 50%

- Support mixed environments, variety of use cases, public or private trust models
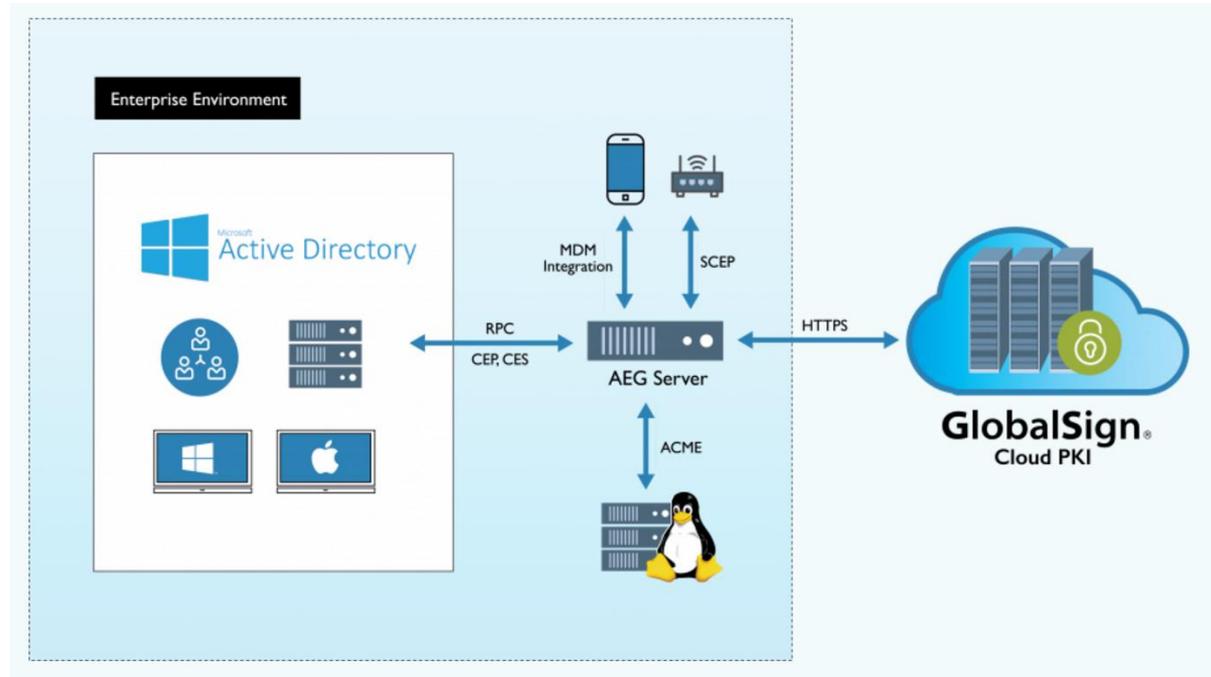
Identity for Everything

AATL - Document Signing Solution
Digital Signing Services

GlobalSign
GMO INTERNET GROUP

Digital Signatures Overview

The Need for Electronic Signatures

Digital Signatures are a secure and trusted type of electronic signatures, and today's B2B, B2C, and governmental markets all shift towards adopting electronic signatures for its many benefits including:

- Go **Paperless**: Save time, money, effort, and the environment.
- **Easier Business Process**: Doing your signing electronically makes every transaction a smoother process for you and your clients.
- Go **Mobile**: collaboration within your organization or with your clients just got easier.

The Need for Digital Signatures

Digital Signatures go beyond answering to all of the market needs for electronic signatures, the growing need for digital signatures is in particular to:

- **Securely Sign:** Enable secure electronic document workflows
- Meet **Compliance** requirements on digital signatures
- Ensure document **integrity** and **authorship**
- **Timestamping** services included to support time sensitive document transaction and audit trails

Adobe Approved Trust List

The Adobe Approved Trust List is a program that allows millions of users around the world to create digital signatures that are trusted whenever the signed document is opened in

Adobe® Acrobat® or Reader® software.

GlobalSign AATL certificates you can use our timestamping service enabling you to have a trusted time of signing and helping to preserve the document content integrity.

Signing Legislation

eIDAS
READY

**State Engineering
Board Regulations**

FDA
21 CFR Part 11

- With the adoption of eIDAS regulation across the EU setting the requirements and standards for signatures across 28 countries, and it is expected to influence and have some levels of adoption beyond the EU within highly integrated economies with the EU like the UK.

- The FDA regulation Title 21 CFR Part 11 sets the criteria under which the FDA considers electronic records, electronic signatures, and handwritten signatures executed to electronic records to be trustworthy, reliable, and generally equivalent to paper records and handwritten signatures executed on paper.

Overview

When you receive a digitally signed document, both Reader and Acrobat ask three key questions to validate the signature:

1. Is the digital certificate that signed the document still valid? Has it expired or been revoked?

2. Has the document been changed since it was signed? Has the integrity of the document been affected? If there are changes, are they allowed changes or not?

3. Finally, does this certificate chain up to a certificate listed in the Trusted Identity list? If so, the signature will be trusted automatically.

| Adobe Reader Version	Certification VALID	Validity of author NOT confirmed	Certification INVALID	Approval Signature
Version 9 onwards				

Why is this important?

It provides an easy way for all your certificate holders, to sign documents confidently, knowing that recipients will not only get the cost savings and a resulting "green" benefit from staying with an electronic document, but also the integrity-checking and trusted green checkmark/blue ribbon experience when they open the document.

Overview

AATL Certificates are compatible with the following **signing applications** – allowing users to sign **multiple document types with one certificate**:

- Adobe Acrobat
- Microsoft Office
- LibreOffice
- BlueBeam Revu

- Add **customizable** approval signatures, such as <u>image of physical signature</u> or an engineering seal

- **Certify** documents to <u>prove authorship</u>, finalize contents and secure against future tampering
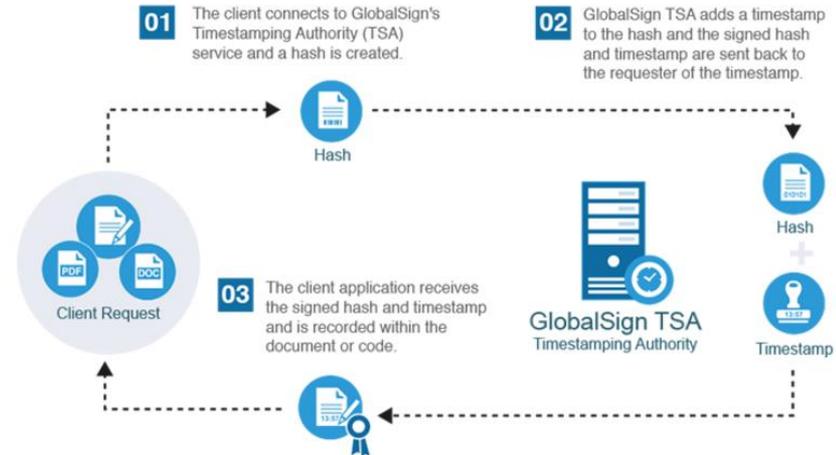

Signature formats
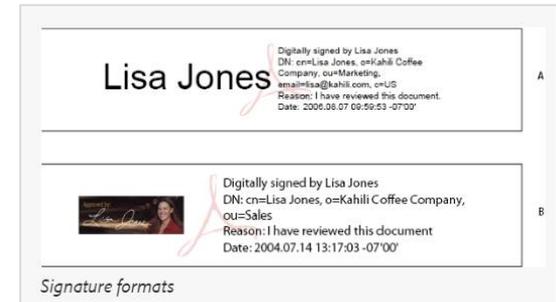
Trusted Timestamping Services

GlobalSign AATL Certificates include RFC 3161 trusted timestamping services. With a timestamping URL included in the AATL Certificate, a timestamp is recorded when a document is digitally signed.

Timestamping services help organization reduce the potential liability associated with time-sensitive transactions by providing a long term validation and non-repudiation of the time and date a transaction took place.

Features & Benefits:
- Add value to digitally signed or electronically signed documents
- Protect intellectual property
- Provide strong legal auditable evidence

01 The client connects to GlobalSign's Timestamping Authority (TSA) service and a hash is created.

Hash

02 GlobalSign TSA adds a timestamp to the hash and the signed hash and timestamp are sent back to the requester of the timestamp.

Hash

03 The client application receives the signed hash and timestamp and is recorded within the document or code.

Client Request

GlobalSign TSA
Timestamping Authority

Timestamp

Sample Signed Document

Valid Signature in Status Bar

Signature Properties (click signature to view signature properties)

Signed and all signatures are valid.

Signature Panel

Signature Properties

Signature is VALID, signed by Cally Cooke <cally.cooke@globalsgin.com>.

Signing Time: 2017/02/22 11:21:12 -05'00'

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

Valid Signature

Validity Summary

The document has not been modified since this signature was applied.

The certifier has specified that Form Fill-in, Signing and Commenting are allowed for this document. No other changes are permitted.

The document is signed by the current user.

Timestamp details

The signature includes an embedded timestamp. Timestamp time: 2017/02/22 11:21:26 -05'00'

Signature was validated as of the secure (timestamp) time: 2017/02/22 11:21:26 -05'00'

Cally Cooke

Digitally signed by Cally Cooke Date: 2017.02.22 11:21:12 -05'00'

Visible Signature

Deployment Options for AATL

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

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

Hosted HSM

TOKEN

Dedicated HSM

Integrations with Service Providers

Deployment Options for AATL - Token

GlobalSign

Token-based –

Ideal for **Individuals and Organizations** who need to digitally sign a moderate amount of PDF documents (**under 5,000/year**) or **do not use** an automated PDF generation solution.

With token-based deployments, the AATL Certificate is issued to an end user via email and then downloaded and installed onto a secure SafeNet USB token (password protected/ cryptographic storage device)

Use GlobalSign's secure cloud-based Certificate Management Platform to issue and manage AATL Digital Certificates.

- No Hidden Fees – you only pay for certificates. There are no setup, hosting, or re-issuance fees
- SafeNet tokens are included in the AATL Certificate price

TOKEN

Deployment Options for AATL - HSM

GlobalSign.

Hosted HSM –

Ideal for organization using **automated** PDF generation software, such as Adobe LiveCycle, Ascertia DSS, or iText Java/C Sharp to generate and **manage large volumes of documents** that **do not have** the desire, internal PKI knowledge or capacity needs to **warrant owning and operating their own HSM**.

GlobalSign provides affordable and secure Hosted HSM partitions to host your AATL certificate and perform digital signing operations.

- Fast set-up
- No in-house cryptographic expertise needed
- Lower total cost of ownership

Dedicated/ Owned HSM –

Ideal for organization using **automated** PDF generation software, such as Adobe LiveCycle, Ascertia DSS, Eldos Secure Black Box, or iText Java/C Sharp to generate and **manage large volumes of documents** that have the desire and internal support **to operate and manage their own HSM** *(on premise or dedicated cloud HSM).*

- Can support larger capacity requirements
- Since on-site, can more readily provide access to data for compliance auditing
- Requires internal resources to manage, ensure baseline requirements and SLAs are met
- Large storage capacity may go unused

Deployment Options for AATL - Workflow

Integrated Signing Workflow Providers

Providing with you with a seamless end to end solution for digital signatures, we are integrated with leading signing workflow providers such as Ascertia. Our integrations enable you to use AATL certificates for individual or organizational signing, and make the best of the service provider's document management and signing workflow system.

ascertia

**Integrations with
Service Providers**

Sample Customers

Resources:

https://www.globalsign.com/en/digital-signatures/resources/

Thank you

T +32 (0) 16 891908 **| M** +32 (0) 495 581037

Email: ronald.detemmerman@globalsign.com

Web: www.globalsign.eu | www.globalsign.com.lb