

it-sa 2023

Thursday, 12 October | 1pm CEST

Hall 6 | Speaker-Platform



HOME OF IT SECURITY



GlobalSign[®]
by **GMO**



m2trust

IT Security made in Germany.

Automating Trust: Navigating the Changes of PKI with Confidence.

it-sa
2023
Special

Speaker



Andreas Brix
Program Manger, GlobalSign



Daniel Dyroff
Operations Manager,
m2trust

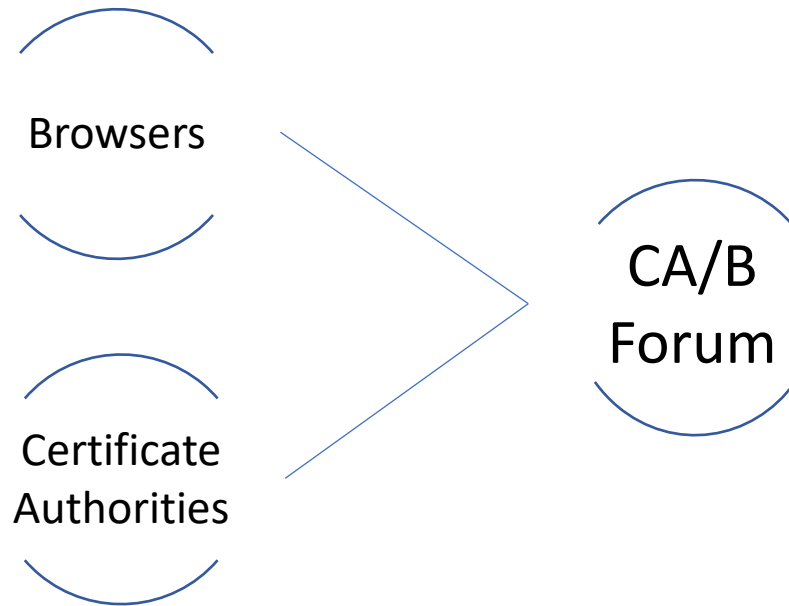


Melanie Faller
PR Manager, GlobalSign

Important changes in the X.509 world



CA/Browser Forum



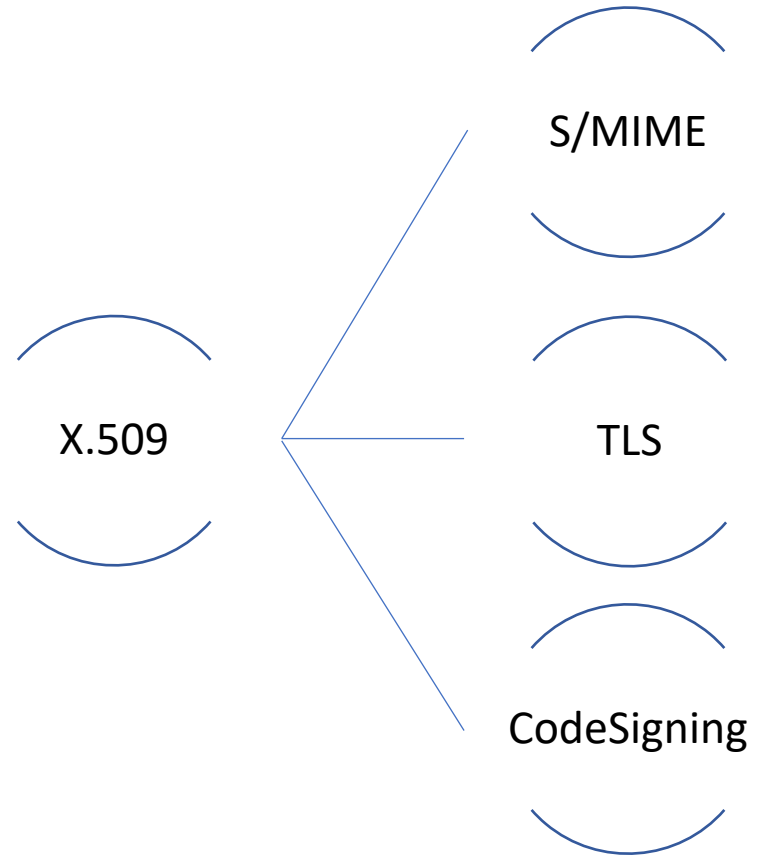
X.509 Standard



X.509

The X.509 standard has played a crucial role in shaping the landscape of digital certificates and secure communications. Its history reflects the ongoing efforts to adapt to changing security needs and technological advancements, making it a cornerstone of modern cryptography and cybersecurity.

X.509 Standard



X.509 Standard

A blue circular icon with a white outline, containing the text 'S/MIME' in the center.

S/MIME

S/MIME, or Secure/Multipurpose Internet Mail Extensions, is a widely adopted standard that provides a secure framework for email communication. It enhances the confidentiality, integrity, and authenticity of email messages by incorporating digital signatures and encryption.

A blue circular icon with a white outline, containing the text 'TLS' in the center.

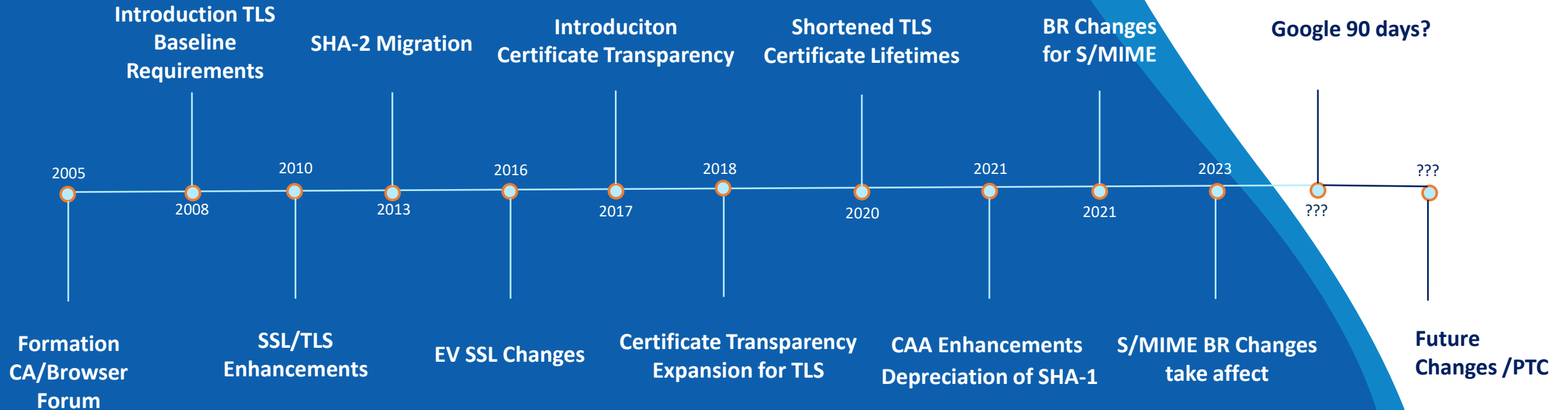
TLS

Transport Layer Security (TLS) is a fundamental cryptographic protocol that ensures secure and private communication over computer networks, notably the internet. It achieves this by establishing an encrypted and authenticated connection between two systems.

A blue circular icon with a white outline, containing the text 'Code Signing' in the center.

Code Signing

Code Signing is a vital cybersecurity practice that enhances software integrity and authenticity by applying cryptographic signatures to code and software applications. This standard ensures that software comes from a trusted source and has not been altered by unauthorized parties, safeguarding users from malicious software.



Google 90 days

- Encouraging **modern infrastructures** and **agility**
- Focusing on **simplicity**
- Promoting **automation**
- Reducing mis-issuance
- Increasing **accountability** and ecosystem **integrity**
- Streamlining and **improving domain validation** practices
- Preparing for a “**post-quantum**” world



ACME



The Automated Certificate Management Environment (ACME) protocol, as the name cleverly implies, automates certificate lifecycle management for SSL/TLS. ACME was originally designed by the Internet Security Research Group and is backed by the Electronic Frontier Foundation. It provides a framework for a client to communicate directly with a CA (Certificate Authority) to issue, install, revoke and replace SSL certificates.

it-sa 2023

Thursday, 12 October | 1pm CEST

Hall 6 | Speaker-Platform



HOME OF IT SECURITY



GlobalSign[®]
by **GMO**



m2trust

IT Security made in Germany.

Automating Trust: Navigating the Changes of PKI with Confidence.

Speaker



Andreas Brix
Program Manger, GlobalSign



Daniel Dyroff
Operations Manager,
m2trust



Melanie Faller
PR Manager, GlobalSign

it-sa
2023
Special

Uncovering the Unprepared:

GMO GlobalSign's Survey on PKI Automation Readiness Among Enterprises and SMBs

Technical, compatibility, security, and expertise hurdles for organizations worldwide



GMO GlobalSign inquired about the challenges businesses will face when Google reduces the maximum certificate to 90 days

30%

Administration and Complexity

About 30% of respondents were most concerned about increased administrative work and complexity. They were also worried about more frequent root certificate updates, like Mozilla's expected 2024 updates

20%

Manageable 7-year cycle

20% of respondents find a seven-year root certificate cycle manageable without a significant impact

15%

Cost and Overheads

15% of respondents, mostly from small businesses and websites, worried about costs and overhead not being justified

20%

Legacy systems and security

30% had concerns about older systems, frequent expirations, and security issues

Automation Hurdles

38%

Site technical constraints, compatibility issues, security, costs, expertise gaps, and infrastructure concerns.



25%

Highlight cost and resource limitations, encompassing custom system development and automated certificate management maintenance



20%

Express concerns about knowledge gaps in certificate automation, from system compatibility to a general lack of automation expertise.



10%

Raise security issues, particularly governance in fully automated systems, audit trails, and security oversight in free public Cas.



7%

Worry about infrastructure limitations, such as firewalled servers, equipment lacking management API's, and isolated networks.



The time is now

- Especially smaller and medium sized businesses are only able to do one step at a time when they restructure their IT-Infrastructure. Therefore, companies need to start the automation journey now considering the mandated 90-day automation might become a reality soon! Having certificate lifecycles automated will keep you secure!
- Keep in mind: **cybersecurity is not a luxury; it's a necessity!**

Before it is time so say goodbye...

**Meet us for a reception at our
booth 7-147 starting at 1:45 PM**

it-sa 2023

Thursday, 12 October | 1pm CEST

Hall 6 | Speaker-Platform



HOME OF IT SECURITY



GlobalSign[®]
by **GMO**



m2trust

IT Security made in Germany.

Automating Trust: Navigating the Changes of PKI with Confidence.

Speaker



Andreas Brix
Program Manger, GlobalSign



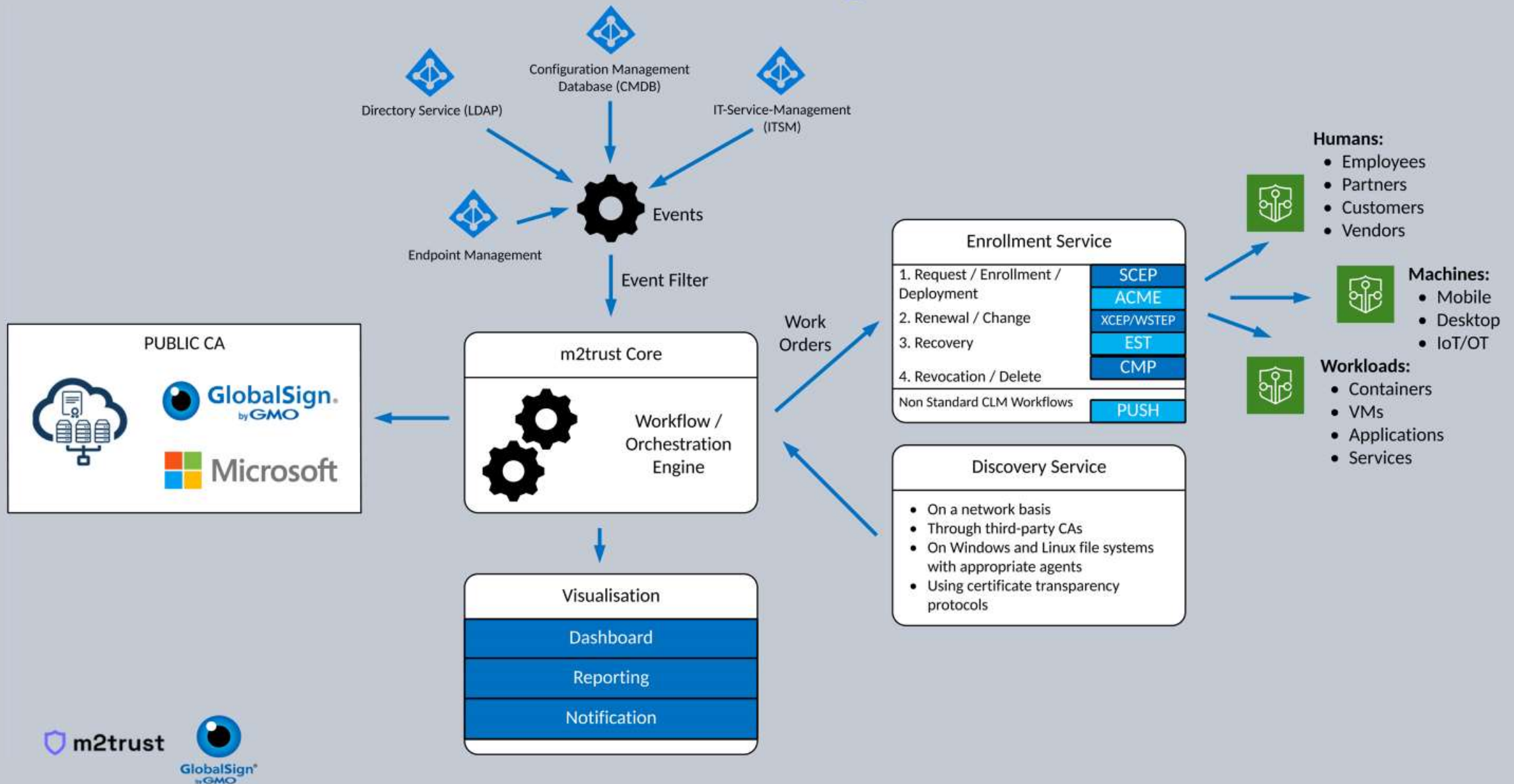
Daniel Dyroff
Operations Manager,
m2trust



Melanie Faller
PR Manager, GlobalSign

it-sa
2023
Special

m2trust Infrastruktur – kurz dargestellt



it-sa 2023

Thursday, 12 October | 1pm CEST

Hall 6 | Speaker-Platform



HOME OF IT SECURITY



GlobalSign[®]
by **GMO**



m2trust

IT Security made in Germany.

Automating Trust: Navigating the Changes of PKI with Confidence.

it-sa
2023
Special

Speaker



Andreas Brix
Program Manger, GlobalSign



Daniel Dyroff
Operations Manager,
m2trust



Melanie Faller
PR Manager, GlobalSign