Industry Update

Oct. 2022

digicert®

CA/BROWSER FORUM

CA/Browser Forum and Other Industry Updates

digicert®


WHOA

What’s an Industry Update w/o a History Lesson?





Who are these people?

What is the CA/B Forum (and more importantly what it isn't)?

CA/BROWSER FORUM

IS:

- A multi-stakeholder organization, seeking consensus among members to create best practices and standards around the issuance of digital certificates

IS NOT:

- An adjudication body
- A place to lodge complaints about CAs or Browsers
- A place to ask for an exception to compliance with standards

October 2022 CA/B Forum Meeting Berlin

CA/BROWSER FORUM

Useful links for monitoring CA/Browser Forum Activity

CA/BROWSER FORUM

- Monthly conversation threads: https://lists.cabforum.org/pipermail/validation/
  - Current activity: https://lists.cabforum.org/pipermail/validation/2022-October/thread.html

- CABF Meeting minutes: https://cabforum.org/category/minutes/
- CABF Plenary public list https://cabforum.org/pipermail/public/
  - Server Certificate WG public list https://cabforum.org/pipermail/servercert-wg/
  - Validation Subcommittee public list https://cabforum.org/pipermail/validation/
  - Code Signing Certificate WG public list https://cabforum.org/pipermail/cscwg-public/
  - S/MIME Certificate WG public list https://cabforum.org/pipermail/smcwg-public/
  - NetSec WG public list https://cabforum.org/pipermail/netsec/

- Joining the CA/B Forum: https://cabforum.org/information-for-potential-members
- CA/B Forum Ballots: https://cabforum.org/ballots/
- CA Incident dashboard: https://wiki.mozilla.org/CA/Incident_Dashboard

New Chairs/Vice Chairs starting November 1st

CA/BROWSER FORUM

Group	Chair	Vice Chair
Forum	Dimitris Zacharopoulos (HARICA)	Paul van Brouwershaven (Entrust)
Server Cert WG	Inigo Barreira (Sectigo)	Kiran Tummala (Microsoft)
S/MIME WG	Stephen Davidson (DigiCert)	Martijn Katerbarg (Sectigo)
Code Signing WG	Dean Coclin (DigiCert)	Bruce Morton (Entrust)
Network Security WG	Clint Wilson (Apple)	David Kluge (Google)

Code Signing Working Group

CA/BROWSER FORUM

Chair: Dean Coclin (DigiCert). Vice Chair: Bruce Morton (Entrust)

- Starting on June 1, 2023, private keys for OV code signing certificates to be stored on hardware certified as FIPS 140 Level 2, Common Criteria EAL 4+, or equivalent.
- Strengthens private key protection for code signing certificates and aligns it with EV (Extended Validation) code signing certificate private key protection.
- Current discussions around signing service requirements for key security

See Code Signing Baseline Requirements:

https://cabforum.org/baseline-requirements-code-signing/

S/MIME Working Group

Chair: Stephen Davidson (DigiCert). Vice Chair: Martijn Katerbarg (Sectigo)

S/MIME Baseline Requirements

- S/MIME BRs ballot concluded discussion period.
- Voting started October 25th
  - 60-day Intellectual Property review
    = Adoption Date
  - 8 months implementation per section 1.2.1
    = Effective Date
  - Coverage in audit reports after Effective Date

Network Security Working Group

CA/BROWSER FORUM

Chair: Clint Wilson (Apple). Vice Chair: David Kluge (Amazon)

To prepare a common approach to network security for other working groups to include in their respective guidelines

- Recent Activity:
  - Cloud Services Sub-Group Risk Assessment
  - Air Gap Systems

New Google Chrome Root Store

Chromium

Announcing the Launch of the Chrome Root Program

Monday, September 19, 2022

In 2020, Google announced that they were in the early phases of establishing the Chrome Root Program and launching the Chrome Root Store.

The Chrome Root Program ultimately determines which website certificates are trusted by default in Chrome and enables more consistent and reliable website certificate validation across platforms.

Why is Chrome making these changes?

Historically, Chrome integrated with the root store and certificate verification process provided by the platform on which it was running. Standardizing the set of CAs trusted by Chrome across platforms through the transition to the Chrome Root Store, coupled with a consistent certificate verification experience using the Chrome Certificate Verifier, will result in more consistent user and developer experiences.

Read More:

https://blog.chromium.org/2022/09/announcing-launch-of-chrome-root-program.html

Apple Root Program

New policy in effect Oct 2022:
https://www.apple.com/certificateauthority/ca_program.html

- Effective 2022-10-01

  “Full CRL Issued By This CA” must be disclosed to CCADB. This will assist with the revocation checking mechanisms implemented by Apple

Mozilla Root Program

Disclosure, Reporting, Auditing, Compliance

Root store policy 2.8 (June 2022):

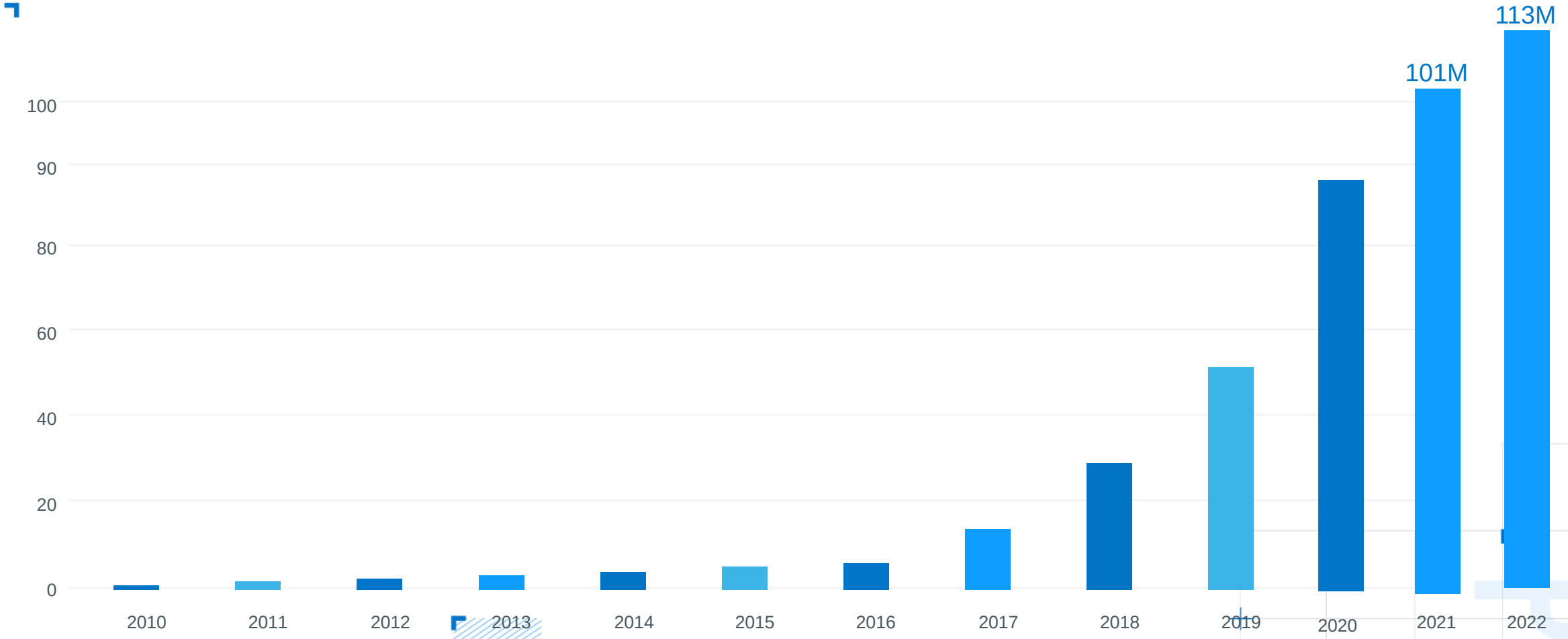
https://www.mozilla.org/en-US/about/governance/policies/security-group/certs/policy/

TLS and S/MIME Requirements

Revocation Reasons: https://wiki.mozilla.org/CA/Revocation_Reasons

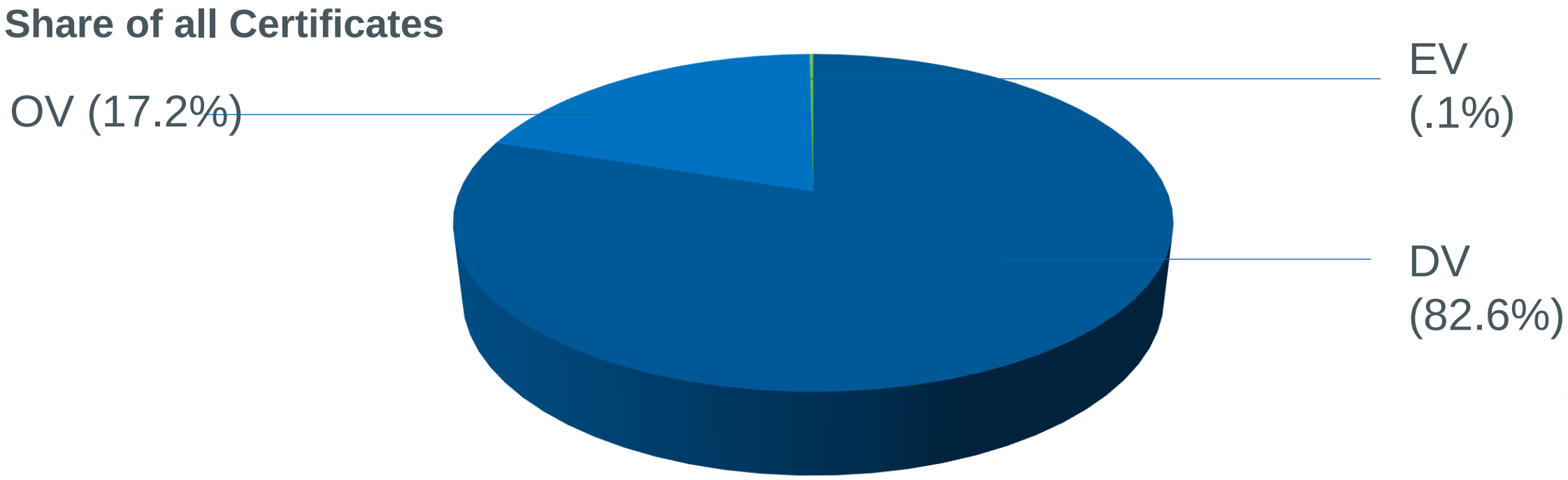
A fast and secure TLS handshake with a browser URL bar that is easy for end users to understand.

TLS Certs over Time



Courtesy of Netcraft

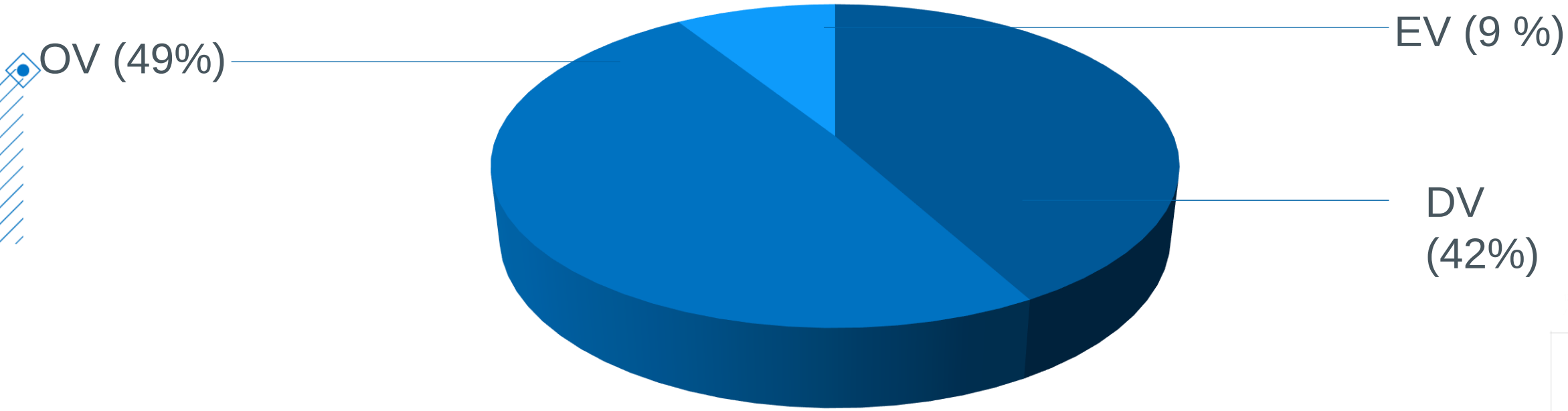
% by Certificate Type – only part of the story



% BY CERTIFICATE TYPE – SEPTEMBER 2022

HIGH ASSURANCE MATTERS

Top 100 e-commerce sites



Source: Data Provider: March 2022

Project Matter: The Origin

Industry leaders like **Apple, Google, Amazon**, and others recognized the challenges consumers were having getting smart home devices to seamlessly work together.

The group decided to form a project within the **connectivity standards alliance CSA** to develop a new standard and seal of approval that would drive interoperability and security of smart home devices.

Industry-unifying standard promises **reliable, secure connectivity** and serves as an important **seal of approval** for compliant devices.

Matter Guiding Principles

Simplicity

Easy to purchase and use.

Interoperability

Devices from multiple brands work natively together.

Reliability

Consistent and responsive local connectivity.

Security

Robust and streamlined for developers and users.

WHY DOES IT ‘MATTER’? – THE SOLUTION

matter

amazon · ASSA ABLOY · COMCAST · Google · HUAWEI · Infineon · Kroger · LEEDARSON · LUTRON · legrand · NXP · oppo · resideo · Schneider Electric · signify · somfy · Texas Instruments · Wulian · IKEA · ST

+ 250 others

Coming **Q4 2022**, customers will begin to see the matter logo on new devices and will know they can trust these will connect seamlessly and securely.

Surprise!

THANK YOU

digicert®