INDUSTRY UPDATE

Dean Coclin

Trust Specialist

digicert®
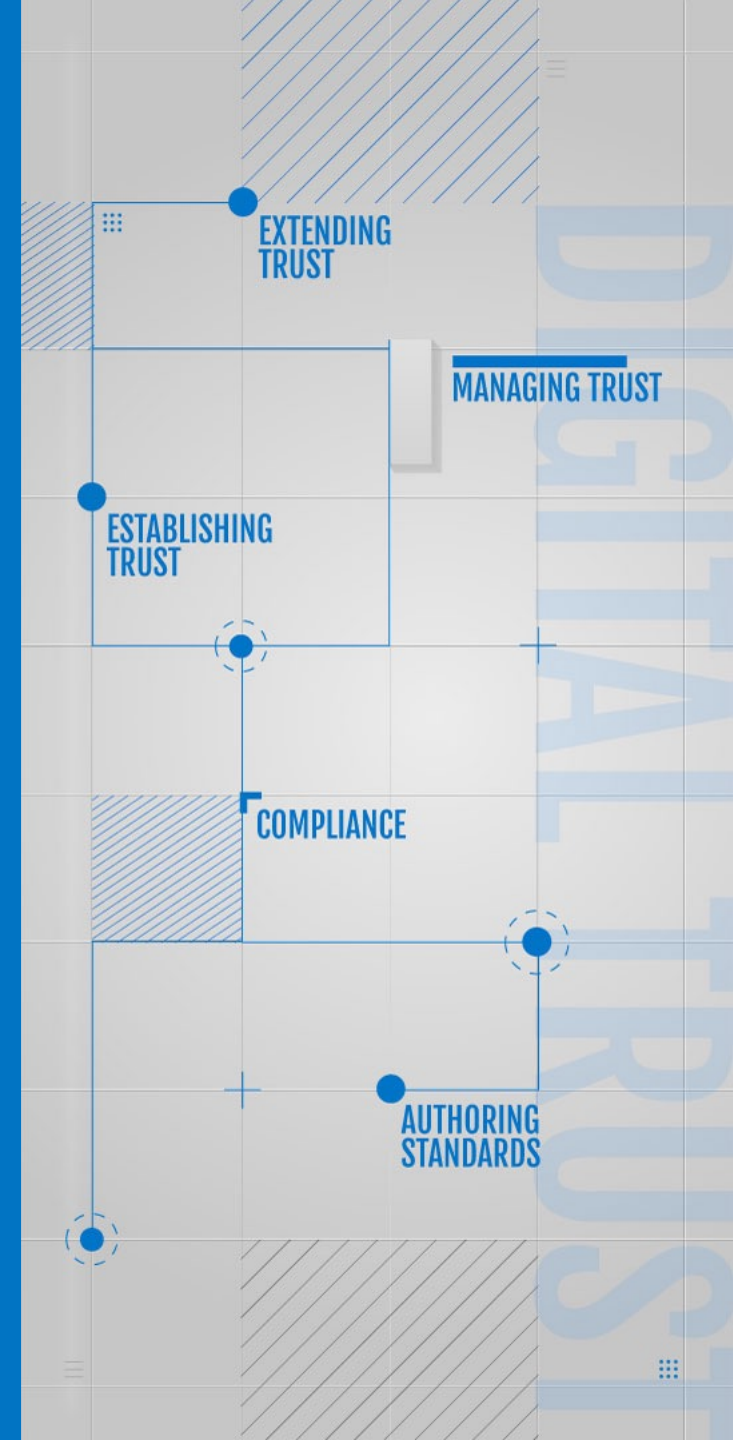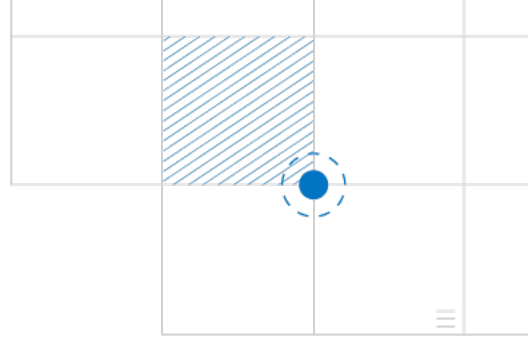
PKI STANDARDS

STANDARDS ARE THE FOUNDATION OF DIGITAL TRUST
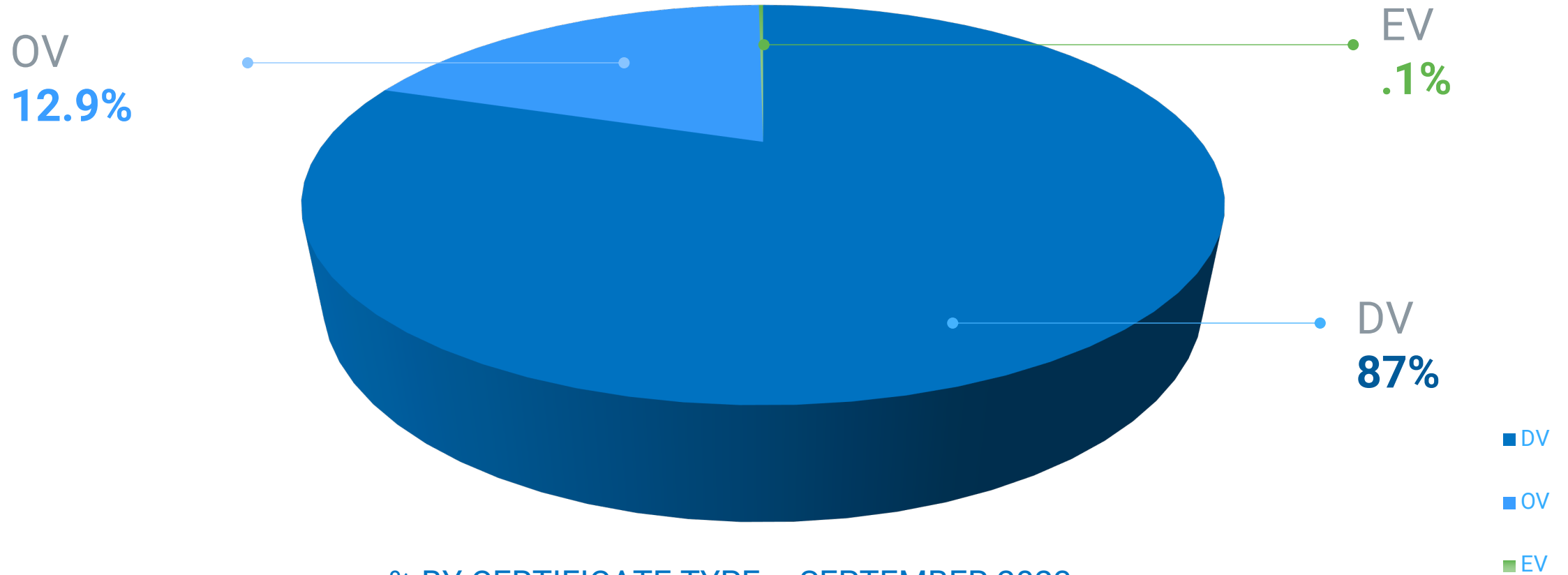
- CA/Browser Forum
  - Code Signing
  - SMIME
  - TLS (BR and EV)
  - NetSec
- ETSI
  - ESI
  - PQC
- VMC/AuthIndicators
- IETF
  - LAMPS
  - PQC

- Connectivity Standards Alliance / MATTER
- ASC X9 Financial Security PKI Study
- Cloud Signature Consortium
- ICANN / OARC
- Accredited Standards Committee X9
- US NIST NCCOE
- Electric Vehicles
  - Society of Automotive Engineers
  - DG Move

PUBLIC TLS CERTS OVER TIME

Certs in Millions

Year	Value
2019	—
2020	—
2021	101M
2022	113M
2023	125M
2024	128M
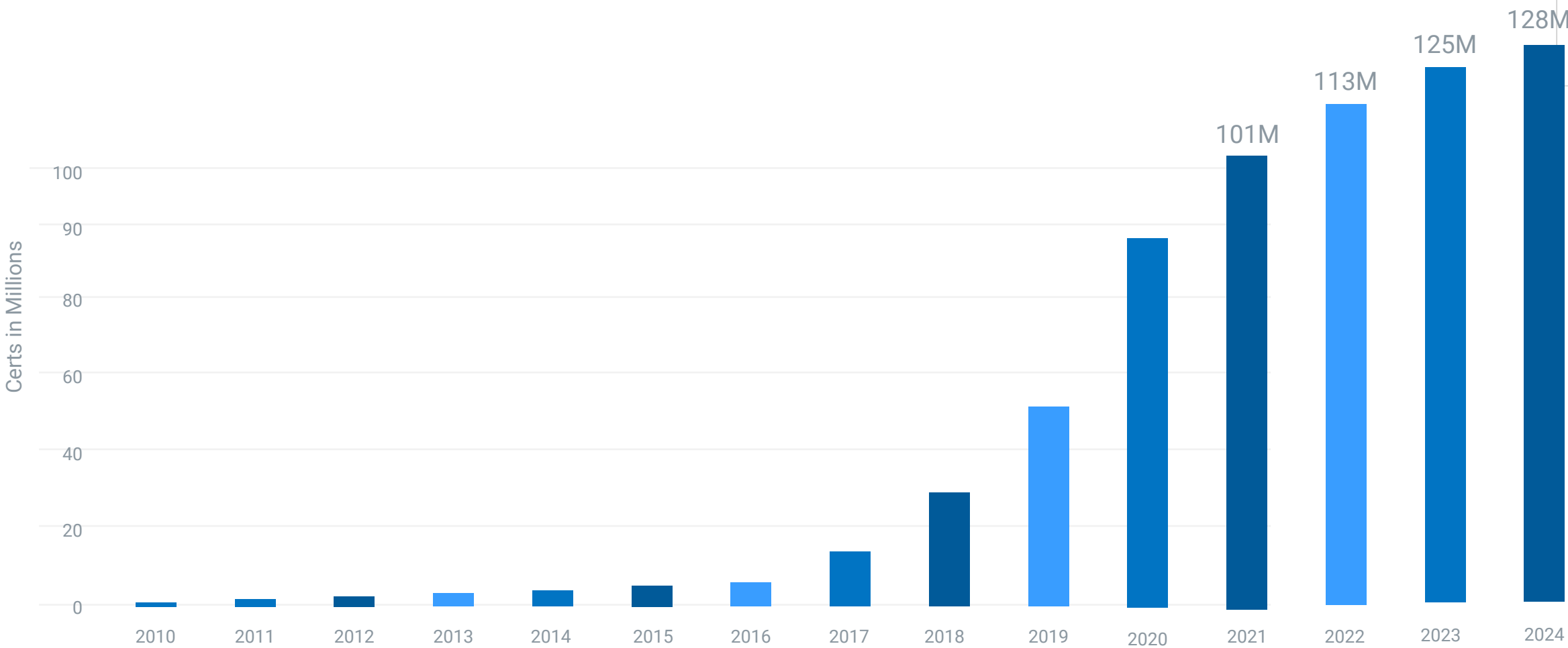
% BY CERTIFICATE TYPE (SNAPSHOT POINT IN TIME)

Share of all Certificates

OV
12.9%

EV
.1%

DV
87%

DV
OV
EV

% BY CERTIFICATE TYPE – SEPTEMBER 2023

RECENT NEWS

Entrust filed several Bugzilla reports for mis-issuance of EV TLS certificates

Viking Cloud (Trustwave) Bugzilla report shows mis-issued OV TLS certificates

Asseco (Certum) Bugzilla report – noncompliance with TLS requirements

CAA will soon be enforced for S/MIME certificates

PKILINT

DigiCert releases significant update for its open source linting framework, pkilint, to support linting certificates against the Ballot SC-62 profiles

- Bundled with 6 command line programs, each wrapping a different linter
    - CABF S/MIME end-entity certificate
    - CABF TLS certificate
    - PKIX certificate
    - PKIX and CABF CRL
    - PKIX OCSP
    - PKIX issuer and subject certificates relationship
- Easy-to-install Python package available on PyPi: https://pypi.org/project/pkilint/
- Source code available on Github: https://github.com/digicert/pkilint

CA/B FORUM NEWS

CA/B FORUM UPDATES

New S/MIME Baseline Requirements

- Effective as of September 1, 2023

- Affects all certs that:
  - Are Public trust
  - Have email Protection eKU
  - Include an email address

- First industry-wide rules for email certs
  - Verification of mailbox control as well as Organization and Individual identity
  - Cert profiles for both ICAs and lead certs
  - CA operations and compliance

- S/MIME Certificate Linter project open-sourced by Digicert

Chrome's phased approach

- **Support for automation**
- **Term limit for roots**
- *Establish minimum expectations for linting*
- *Phase out "multi-purpose" roots*
- *Phase out clientAuth use cases*
- Strengthen domain validation
- Shorter validity period for subCAs
- Shorter validity period for leaf certificates – **long term goal**

Current priorities
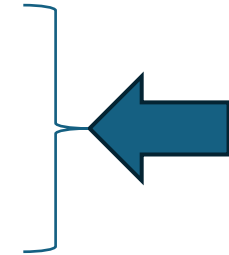
Next priorities

time

EIDAS 2

Article 45 – Qualified Website Authentication Certificates (similar to EV SSL)

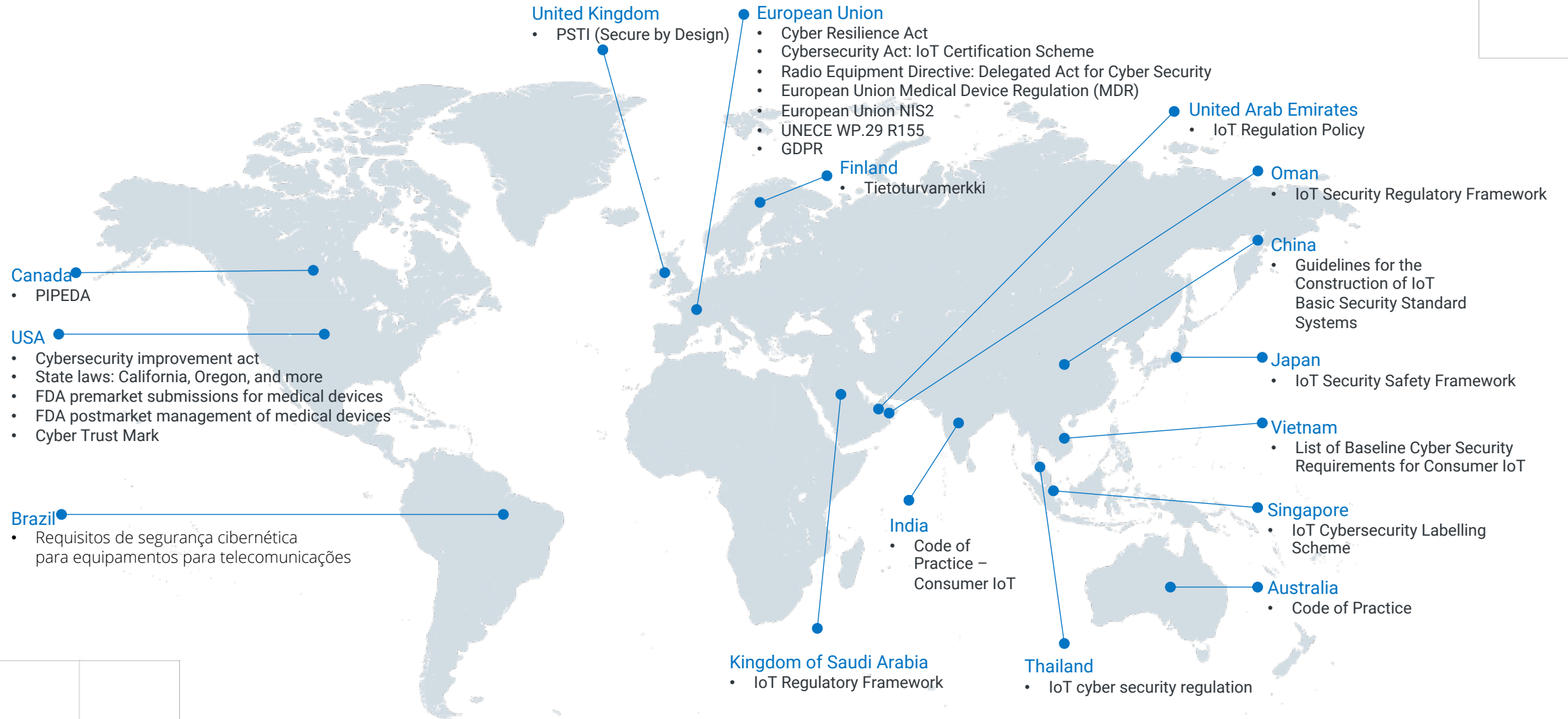Legislation finalized and approved late 2023

Ratification occurred Jan 2024

Implementing acts will follow

Browsers will be required to display information from QWACs

Web browsers shall ensure that the identity data attested in the certificate and…
…is displayed in a user-friendly manner

IOT

REGULATION DRIVING IOT SECURITY

United Kingdom
- PSTI (Secure by Design)

European Union
- Cyber Resilience Act
- Cybersecurity Act: IoT Certification Scheme
- Radio Equipment Directive: Delegated Act for Cyber Security
- European Union Medical Device Regulation (MDR)
- European Union NIS2
- UNECE WP.29 R155
- GDPR

Finland
- Tietoturvamerkki

United Arab Emirates
- IoT Regulation Policy

Oman
- IoT Security Regulatory Framework

China
- Guidelines for the Construction of IoT Basic Security Standard Systems

Japan
- IoT Security Safety Framework

Vietnam
- List of Baseline Cyber Security Requirements for Consumer IoT

Singapore
- IoT Cybersecurity Labelling Scheme

Australia
- Code of Practice

Canada
- PIPEDA

USA
- Cybersecurity improvement act
- State laws: California, Oregon, and more
- FDA premarket submissions for medical devices
- FDA postmarket management of medical devices
- Cyber Trust Mark

Brazil
- Requisitos de segurança cibernética para equipamentos para telecomunicações

India
- Code of Practice – Consumer IoT

Kingdom of Saudi Arabia
- IoT Regulatory Framework

Thailand
- IoT cyber security regulation

Source: LEVY-BENCHETON, Cédric. Panorama of IoT Cyber Security Regulations Across the World. cetome. https://cetome.com/panorama

POWERING PROGRESS IN EV CHARGING

Addressing Cybersecurity Risks, Ensuring Compliance and Driving Adoption

- $7.5B in NEVI funding is spurning an expanse of EV charging stations

- DigiCert awarded contract by SAE ITC's EV PKI Consortium

- Accelerating security implementation for EV charging stations (EVSE)

- DigiCert supporting wide scale interoperability testing of ISO 15118-2 certificates (PKI) with top EV, Chargepoint Operators (CPOs) and EV charging station companies

53%
of consumers reported their concern about EV security

64%
of drivers who already own an EV have expressed concern about the security of public charging stations

The automotive industry has experienced a

225%
increase in cyberattacks over the last **THREE YEARS**

US CYBER TRUST MARK

The 'US Cyber Trust Mark' finally gives device makers a reason to spend big on security

Apu Pavithran   7:00 AM CDT • August 23, 2023   Comment

U.S. CYBER TRUST MARK   U.S. CYBER TRUST MARK   U.S. CYBER TRUST MARK

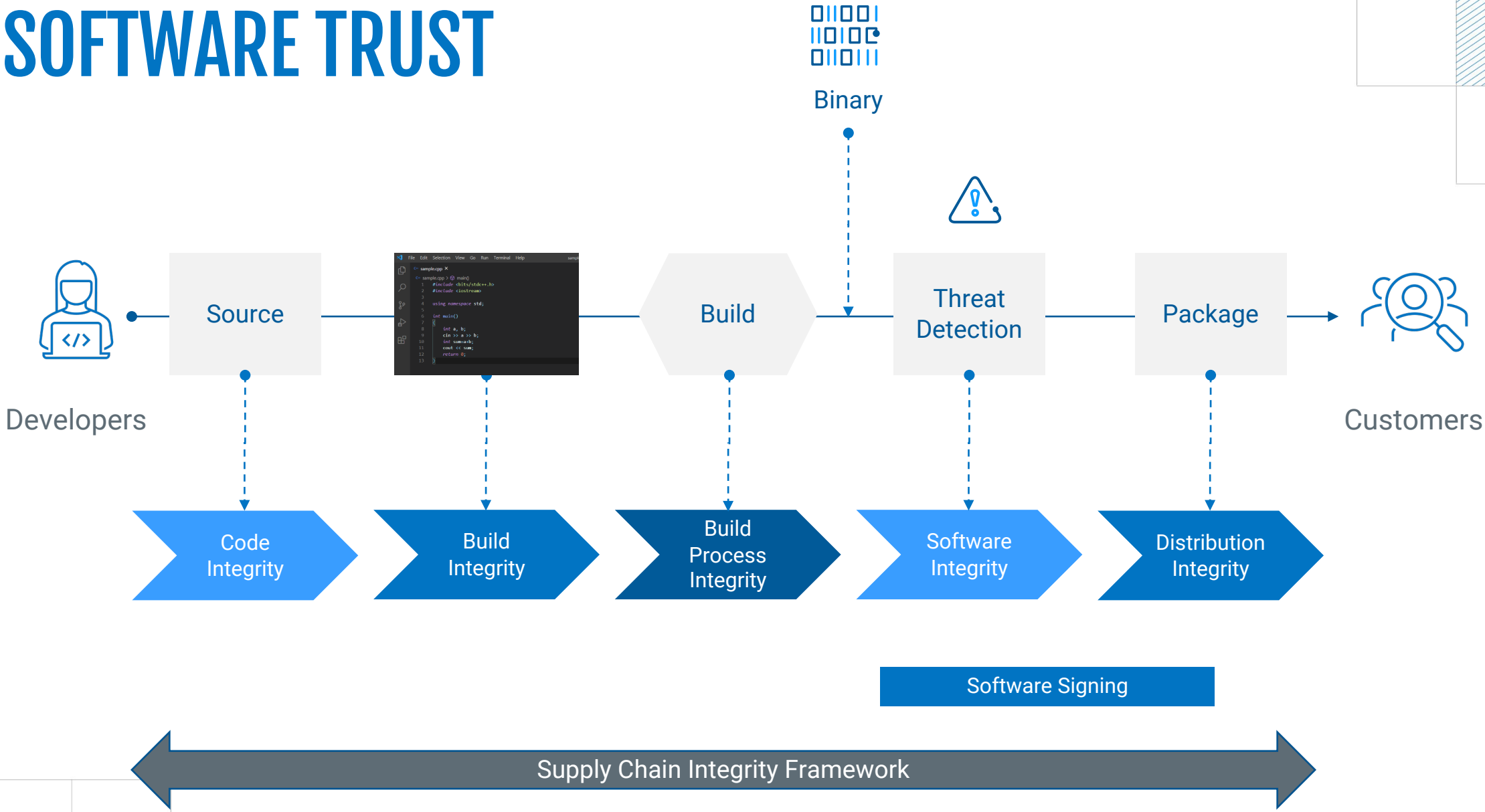U.S. CYBER TRUST MARK   U.S. CYBER TRUST MARK

Image Credits: FCC / FCC.gov

The Internet of Things (IoT) is in hacker crosshairs. Last year, more than 110 million IoT malware attacks took place — an 87% increase from the previous 12 months. And as connected devices take on more critical roles in the modern home and office, tens of billions more endpoints are coming online.

In this precarious landscape, both individual consumers and enterprises embracing IoT have made cybersecurity a top priority. Now the government is following suit. In July, the White House announced the launch of a "U.S. Cyber Trust Mark" as part of its voluntary labeling program for smart devices.
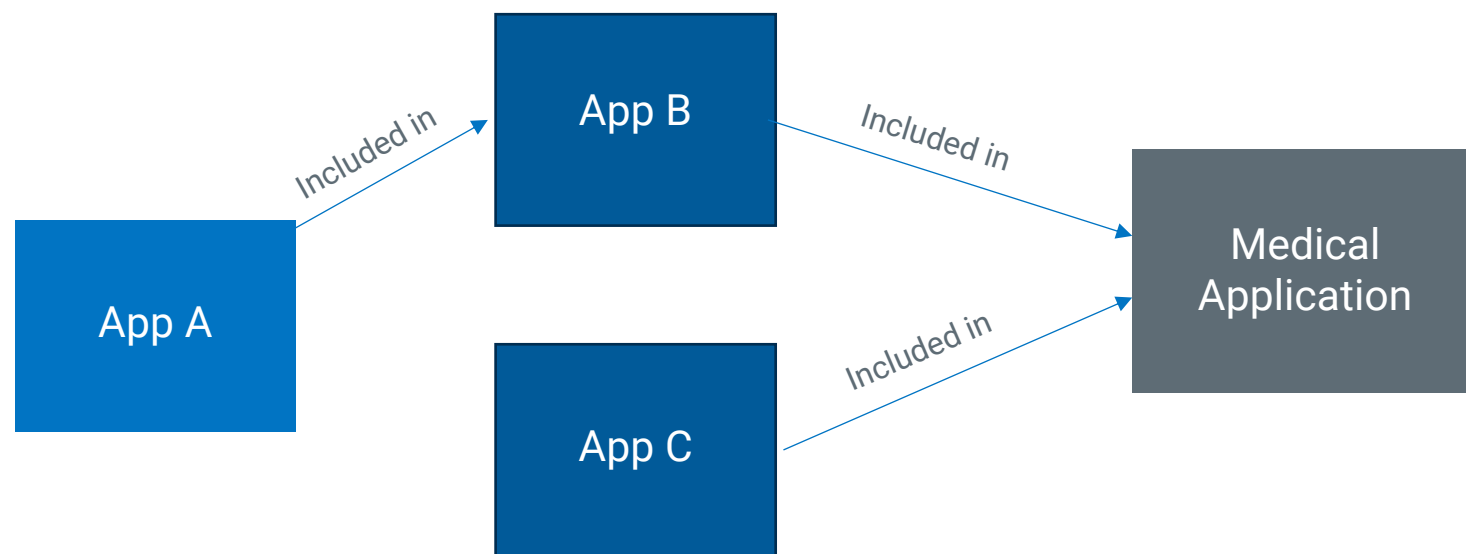
Apu Pavithran
Contributor

Apu Pavithran is the founder and CEO of Hexnode.

https://techcrunch.com/2023/08/23/the-us-cyber-trust-mark-finally-gives-device-makers-a-reason-to-spend-big-on-security/

SOFTWARE TRUST

Binary

Threat
Detection

Developers

Source

Build

Package

Customers

Code
Integrity

Build
Integrity

Build
Process
Integrity

Software
Integrity

Distribution
Integrity

Software Signing

Supply Chain Integrity Framework

SECURING MEDICAL DEVICES: SBOM

- US Food and Drug Administration's (FDA) software bill of materials (SBOM) mandate officially enforced from October 1st, 2023

- FDA is mandating that all medical devices running software must create and maintain an SBOM

App A → *Included in* → App B → *Included in* → Medical Application

App C → *Included in* → Medical Application

- Who built it?
- What's in it?
- Who signed it?
- When was it signed?

FDA SOFTWARE AND DEVICES FAQ'S

https://www.fda.gov/medical-devices/digital-health-center-excellence/cybersecurity-medical-devices-frequently-asked-questions-faqs

FDA Guidance on Regulatory Requirements for Device Software Functions
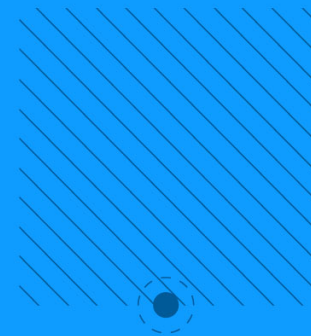
https://techcrunch.com/2023/08/23/the-us-cyber-trust-mark-finally-gives-device-makers-a-reason-to-spend-big-on-security/

C2PA

Coalition for Content Provenance and Authenticity – addresses misleading information

- Open standard for identifying and authenticating digital files

- Created by industry leaders Adobe, Microsoft, Sony, DigiCert and others
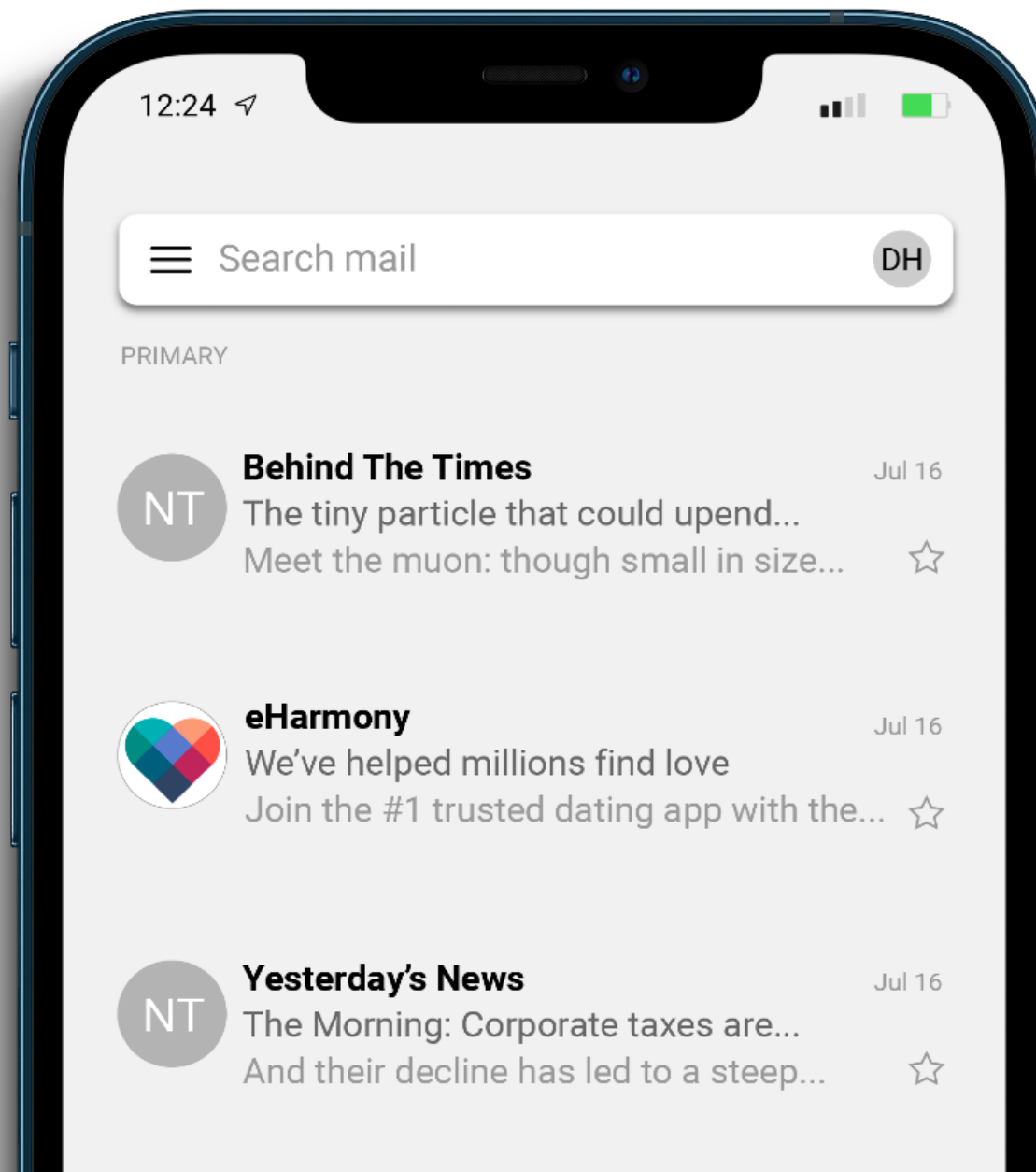
- Uses PKI to validate digital files

An Overview of the C2PA Life Cycle

Linda takes a photo using her C2PA-enabled camera. It creates a digital manifest containing provenance info.

Linda sends the photo to Erik, who can verify the credential. Erik edits the photo in PhotoShop before uploading the photo to his website.

Looking at the manifest, a user on the website can verify that Linda took the original photo and see that Erik made edits to it.

Content Creator Linda

Editor Erik

Website User Wendy

DIGICERT MARK CERTIFICATE

GET A HEAD START
ON STANDING OUT
FROM THE CROWD

VERIFIED MARK CERTIFICATES: DELIVER YOUR LOGO TO INBOXES

Key Benefits

- Improve email engagement rates by 10% (Verizon Media Study 2020)
- Protect your brand from spoofing or impersonation
- Certify DMARC enforcement and reduce phishing emails to customers

Brand Protection

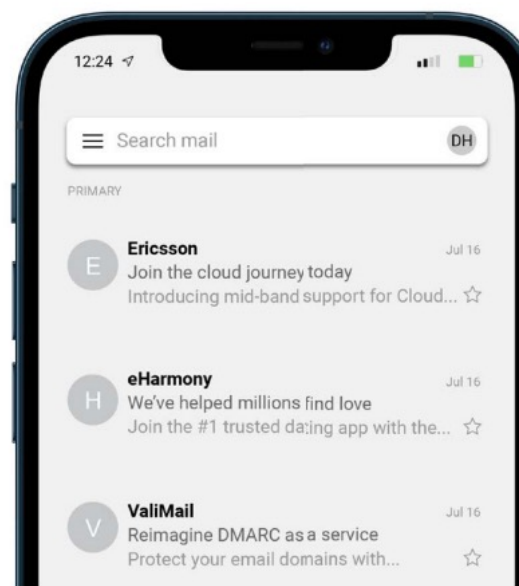- Millions of impressions
- Control brand consistency

Security
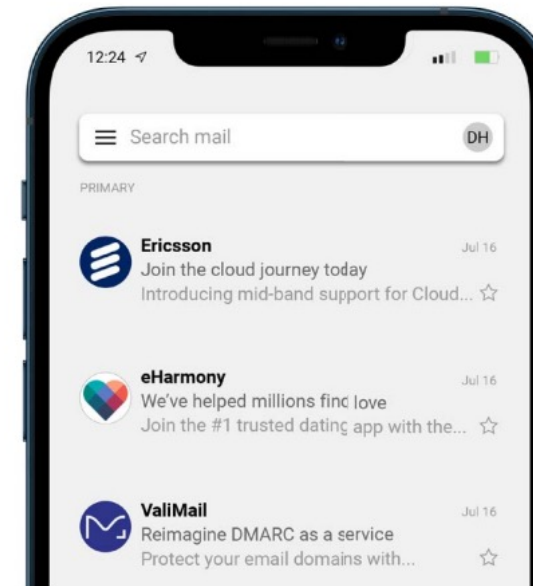
- Blocks unauthorized use of domain
- Decrease phishing, spam, fraud via DMARC

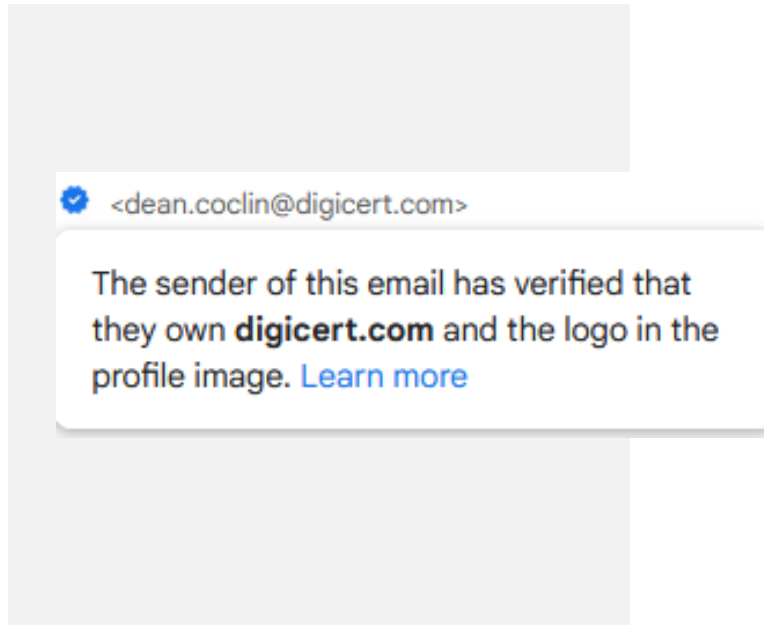## Deliverability

- 5-10% increase in engagements

WITHOUT VMC   WITH VMC

TWO THINGS TO REMEMBER ABOUT VMC

LOGOS

SECURITY

MARK CERTS REQUIRE STRONG AUTHENTICATION

1
Domain validation

2
Business validation

3
(Trade) Mark validation

4
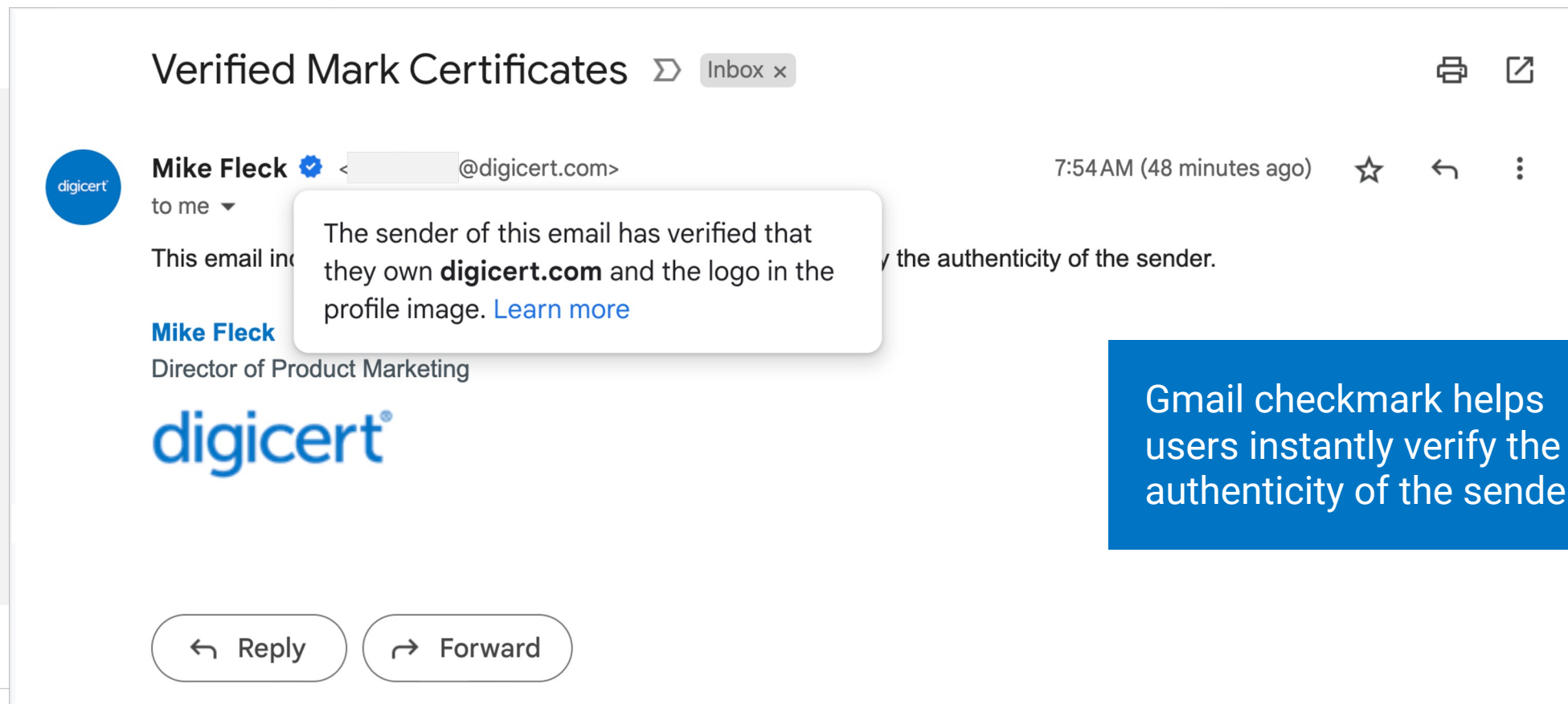Logo format validation

5
Applicant validation via video call

MAKE PHISHING MORE DIFFICULT: GMAIL DESKTOP DISPLAY
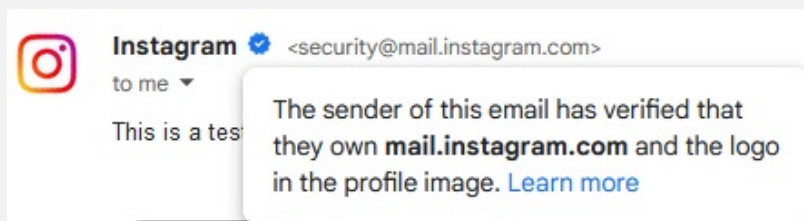

Gmail checkmark helps users instantly verify the authenticity of the sender

VMC VS CMC

VMC

- Trademark
- Verified with TM agency
  - Distinguished UI with check mark

CMC

- No Trademark (3 options)
  - Verify mark has been in use or,
  - Modify an existing TM or,
- Different UI, no check mark
- Pricing TBD
- Pilot Q1 2024

THANK YOU

digicert®