

Industry Update (International Market for Trust Services)

October 2023

Dean Coclin

Sr. Director, DigiCert

CA/B Forum Code Signing Chair
X9 PKI Study Group Chair



What does this spell?

NLPDR
PRNDL

How did PRNDL come about?

- Cars became popular in the 1920s and 30s
- Was it a standard? NO
- Didn't become a standard until 1971!
- Why?



Everyone wants freedom to innovate

But if standards aren't followed, bad things can happen



Did Jeep that killed Anton Yelchin in freak accident have a design flaw? Cars 'were previously recalled'

The actor passed away after being pinned against the gate guarding his San Fernando Valley home

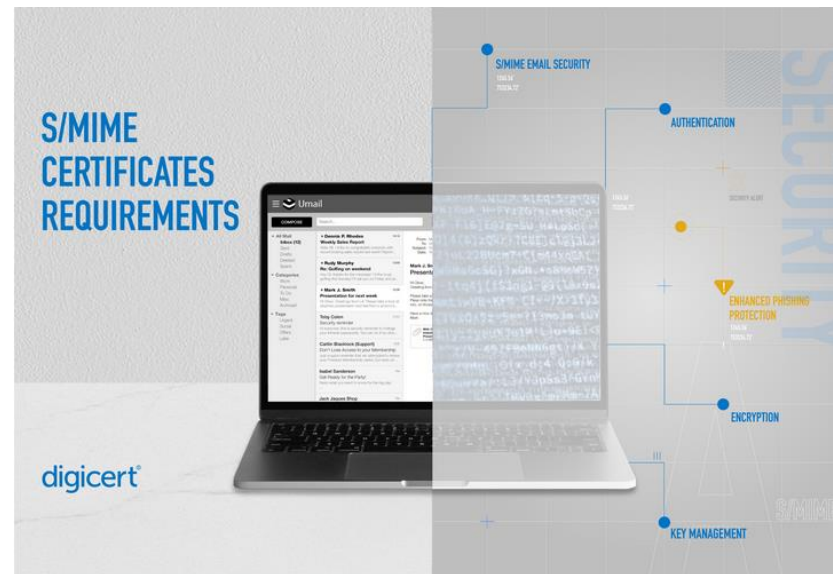
➤ Recall of Jeeps and design change

Consistency and User Friendliness are key to successful designs

What's an example of something that took 20 years to become a standard?



Class 1
Class 2
Class 3



S-MIME

01-05-2023

CA/BROWSER FORUM ADOPTS FIRST BASELINE REQUIREMENTS FOR S/MIME CERTIFICATES

STEPHEN DAVIDSON



S/MIME Types

Mailbox-validated	Subject is limited to (optional) subject:emailAddress and/or subject:serialNumber attributes.
Individual-validated	Includes only Individual (Natural Person) attributes in the Subject.
Organization-validated	Includes Organization details (legal entity) in Subject. Example uses include invoice or statement mailers, etc.
Sponsor-validated	Effectively an Organization certificate that also includes “sponsored” Individual (Natural Person) attributes. Often issued via an Enterprise RA.

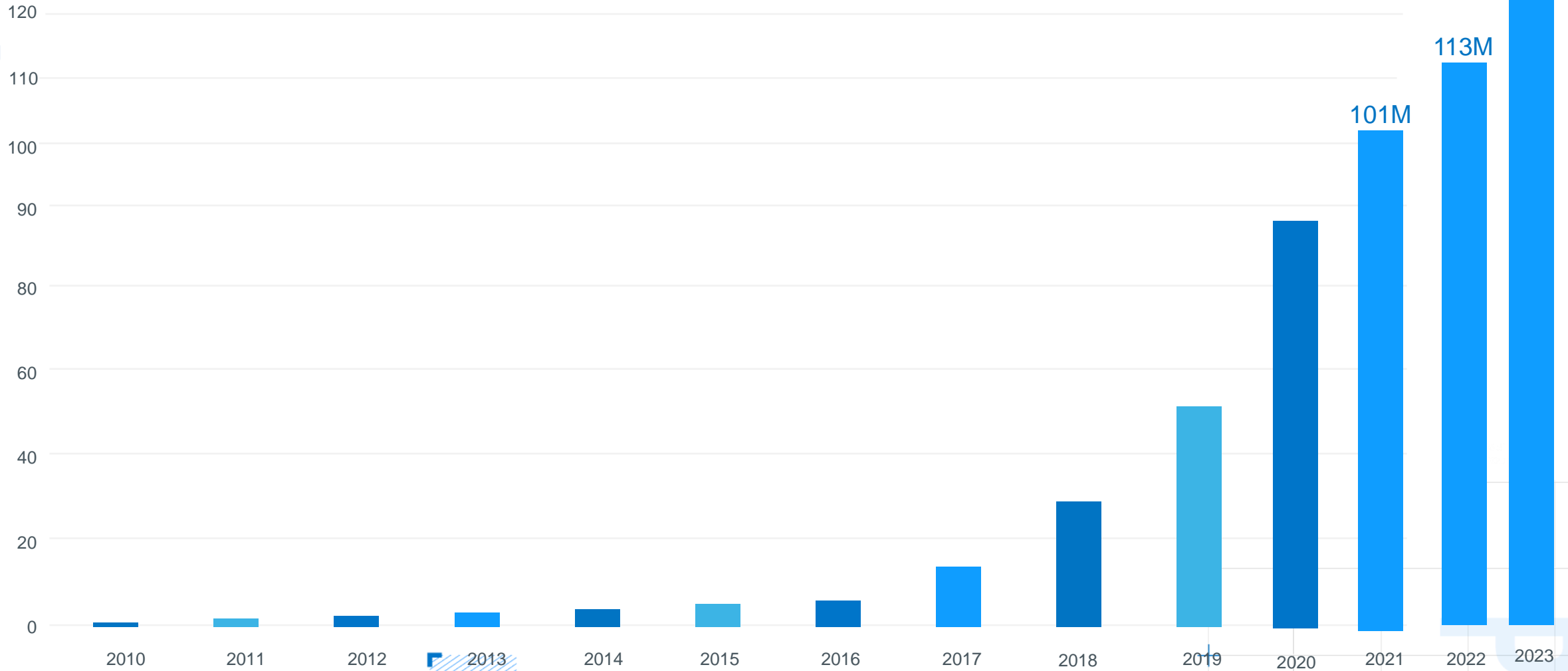
Design Considerations

- **Consistency and User Friendliness**
 - **Easily recognizable and understandable across browsers/platforms**
 - **Obvious benefit of keeping consistency**
- **Minimal Education**
 - **Tool tips and pointers to more information**

*Web browsers shall ensure that the identity data attested in the certificate and...
...are displayed in a user friendly manner*

Other Industry News

TLS Certs over Time

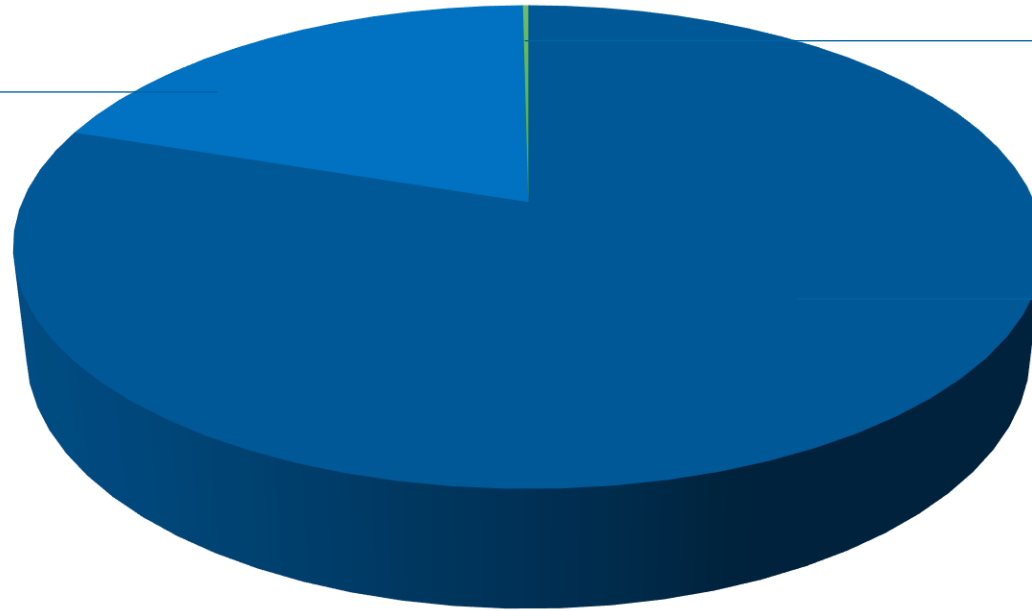


Courtesy of Netcraft: Sept 2023

% by Certificate Type (Snapshot point in time)

Share of all Certificates

OV (12.9%)

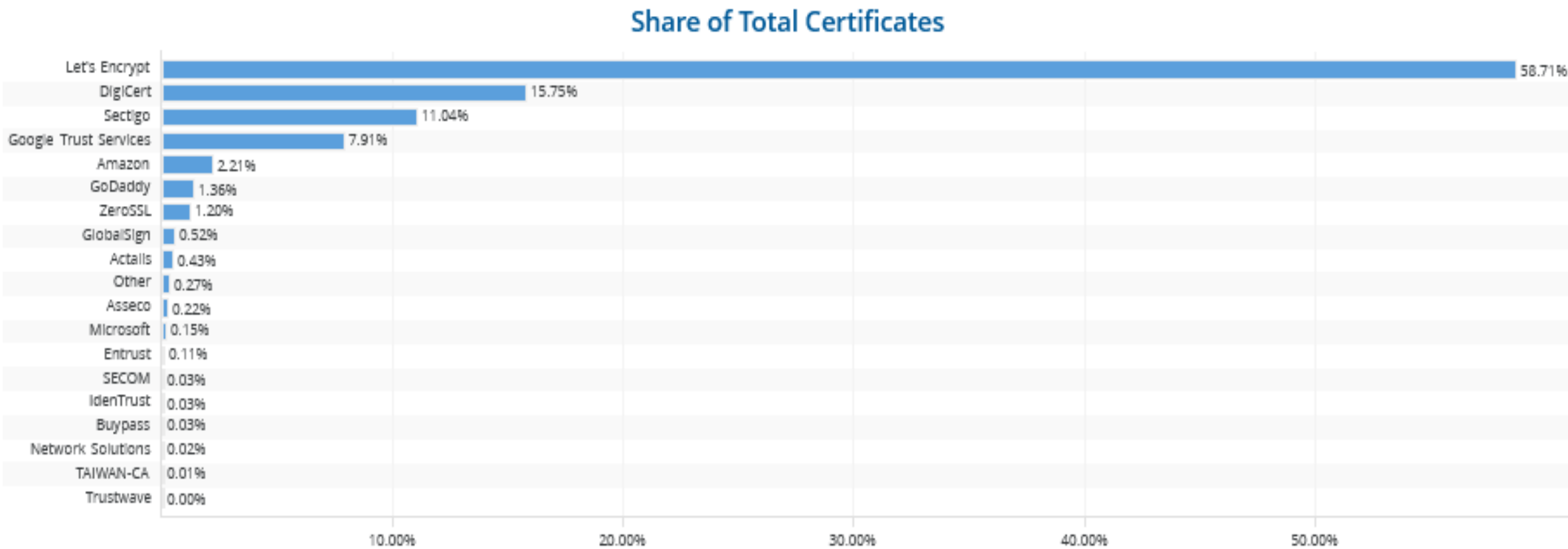


EV
(.1%)

DV
(87%)

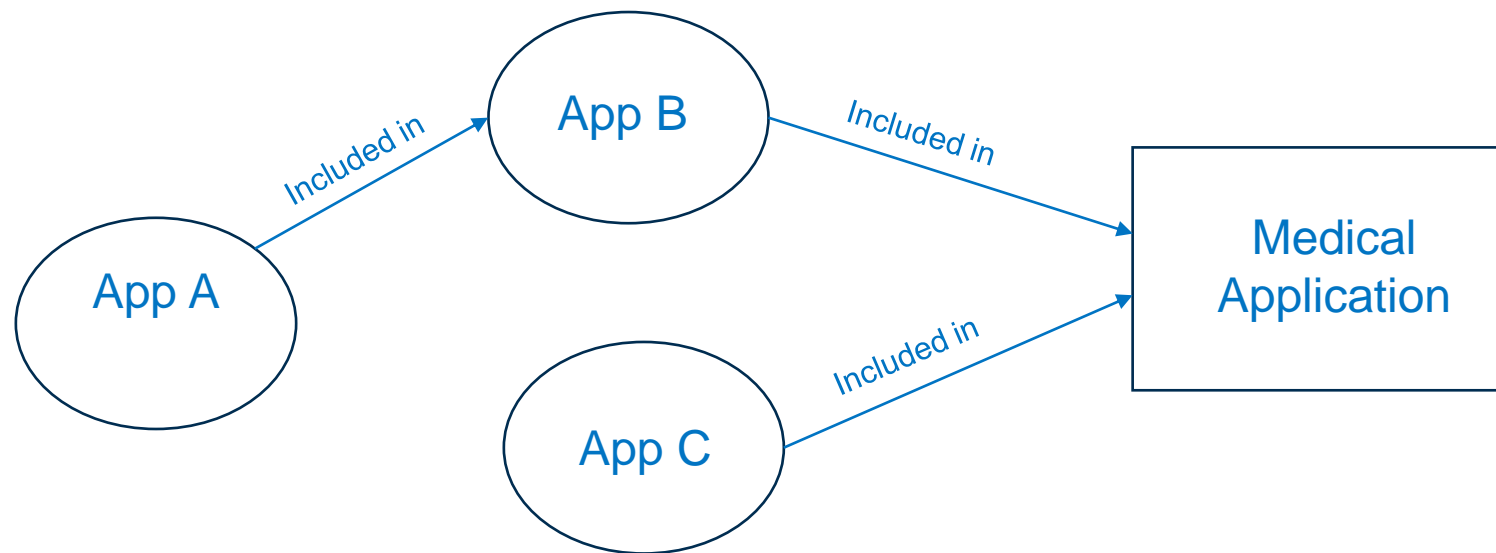
% BY CERTIFICATE TYPE – SEPTEMBER 2023

CA share of total certificates



Securing Medical Devices

- US Food and Drug Administration's (FDA) software bill of materials (SBOM) mandate officially enforced from October 1st
- FDA is mandating that all medical devices running software must create and maintain an SBOM



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

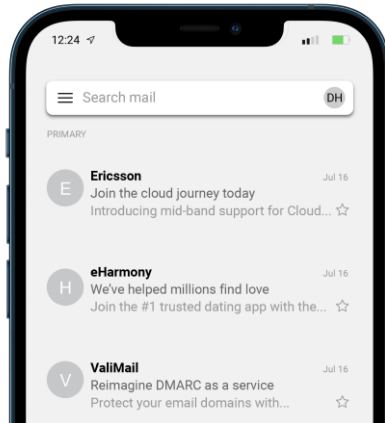
DigiCert releases significant update for its open source linting framework, pkilint, to support linting certificates against the Ballot SC-62 profiles

- 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>

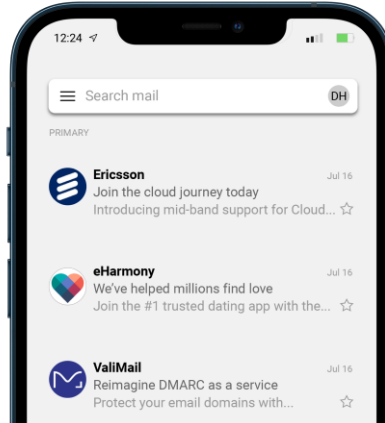
VERIFIED MARK CERTIFICATES: DELIVER YOUR LOGO TO INBOXES



Without VMC



With VMC



KEY BENEFITS

Improve email open rates by 10%*

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

- Massive increase – you're whitelisted

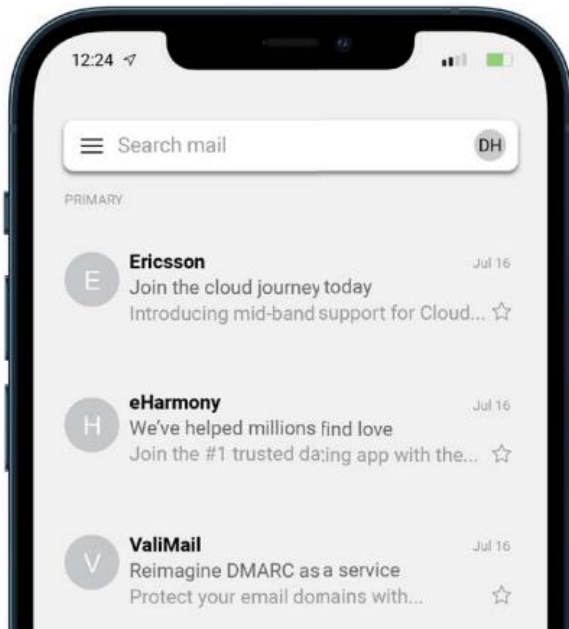


Visibility

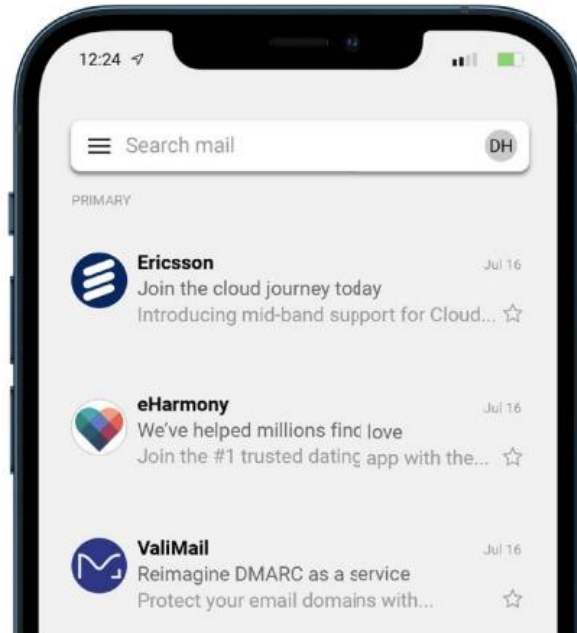
- DMARC provides a detailed report of email from your domain

Where do VMCs show your logo?

WITHOUT VMC



WITH VMC



SUPPORTED BY



Gmail owns the most users, with over 1.8 billion active users¹. Additionally, 75% of Gmail users access their email via their mobile device².

¹ Source: SaaS Scout

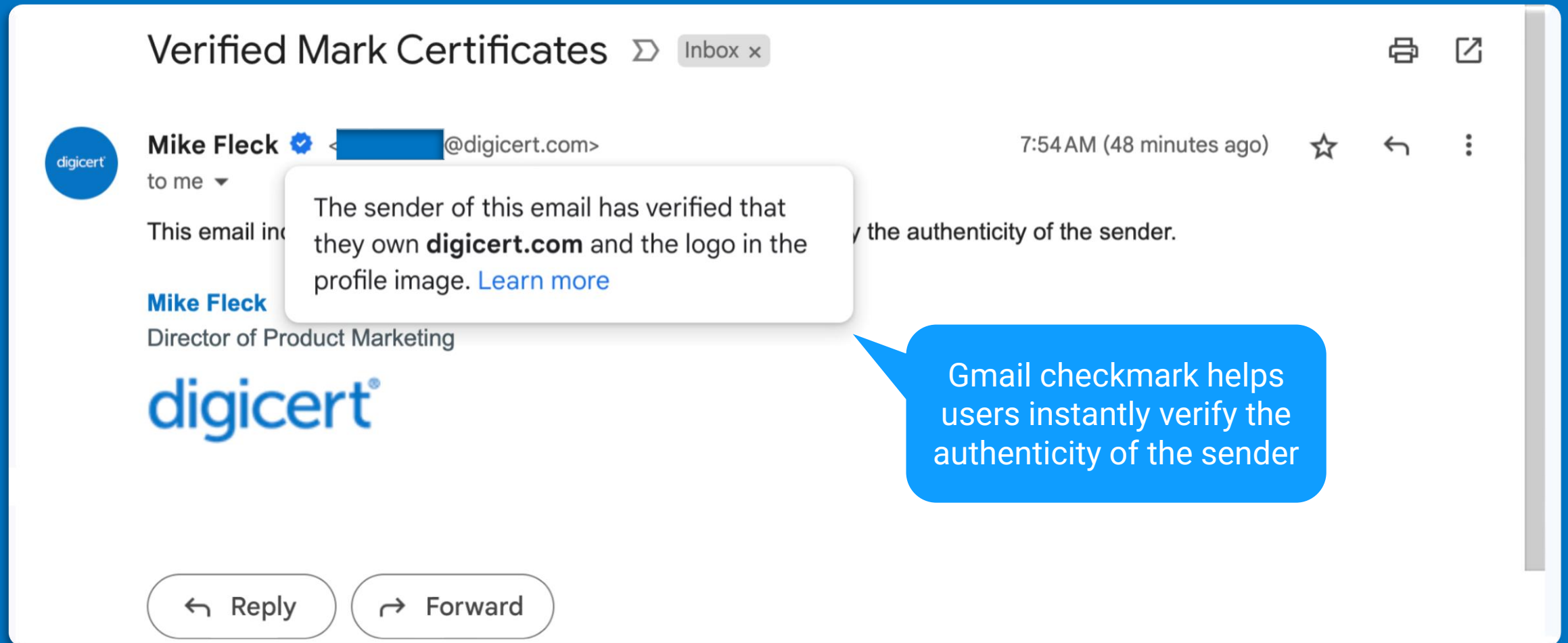
² Litmus, 2021

Mark Certificates 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



VMC TM Logo origin – ACTIVE certs

Logo Origin	Total Count
Government Mark - DK	1
Registered Mark - AU	90
Registered Mark - BR	8
Registered Mark - BX	3
Registered Mark - CA	43
Registered Mark - CH	2
Registered Mark - DE	70
Registered Mark - DK	1
Registered Mark - EM	353
Registered Mark - ES	20
Registered Mark - FR	6
Registered Mark - GB	273
Registered Mark - IN	85
Registered Mark - JP	49
Registered Mark - NZ	3
Registered Mark - US	860
TOTAL	1867

Mark Certificates: VMC vs. Common Mark Certificate (CMC)

VMC

- Trademark
- Verified with TM agency
- Distinguished UI with checkmark



Dean Coclin 
to me ▼

The sender of this email has verified that they own **digicert.com** and the logo in the profile image. [Learn more](#)


CMC

- No Trademark (2 options)
 - Verified mark has been in use or,
 - Modify an existing TM
- Different UI – no checkmark
- Pilot Q4 2023



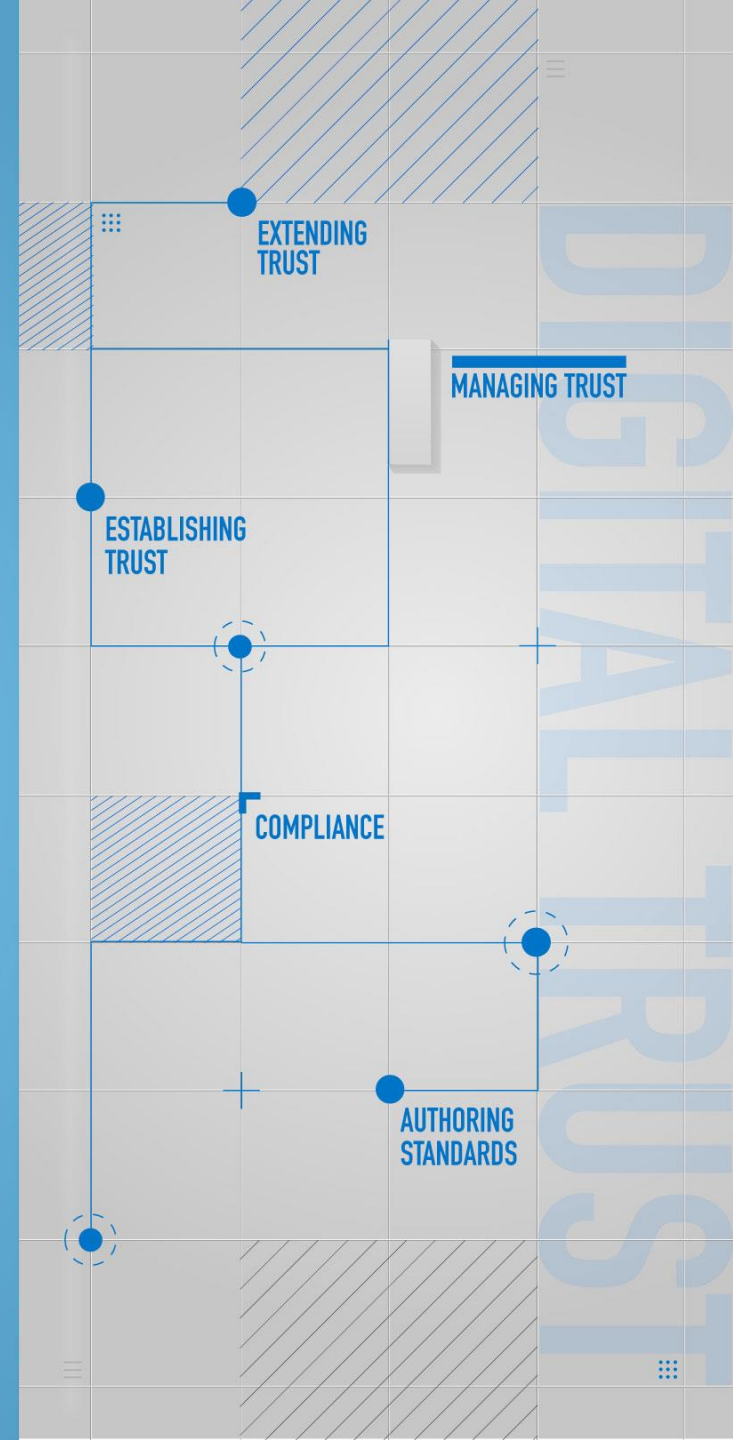
The Washington Post <email@washingtonpost.com> [Unsubscribe](#)
to me ▼

SUMMARY and PREDICTIONS

- QWACs → PRNDL
 - Consistent, Understandable, Intuitive
- S/MIME Standards → VeriSign
- New certificate use cases will continue to evolve:
 - Mark Certificates for email logo validation
 - Increased software signing (DEVSEC/OPS) and SBOMs
 - IoT: Vehicles, EV Chargers, Medical devices, Telephone call authentication
 - Protection from Deepfakes and Generative AI
 - https://c2pa.org/specifications/specifications/1.3/specs/C2PA_Specification.html

We are not just a certificate authority.
We are the authority on
DIGITAL TRUST

digicert®



THANK YOU