TRANSATLANTIC PERSPECTIVES ON EIDAS

and a little more…

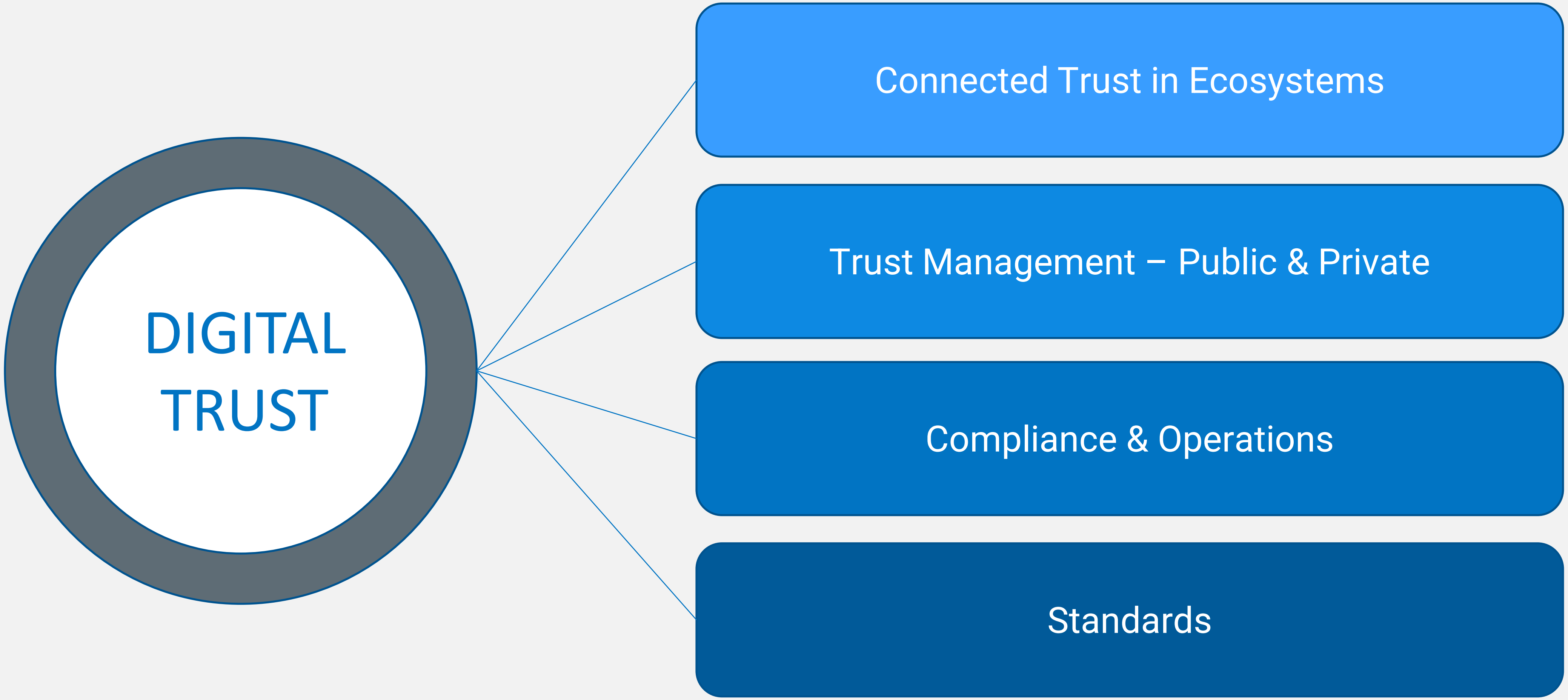
Dean Coclin September 26, 2024

digicert®

STANDARDS

01

THE BUILDING BLOCKS OF DIGITAL TRUST



DIGITAL TRUST

Connected Trust in Ecosystems

Trust Management – Public & Private

Compliance & Operations

Standards

STANDARDS: THE FOUNDATION OF DIGITAL TRUST

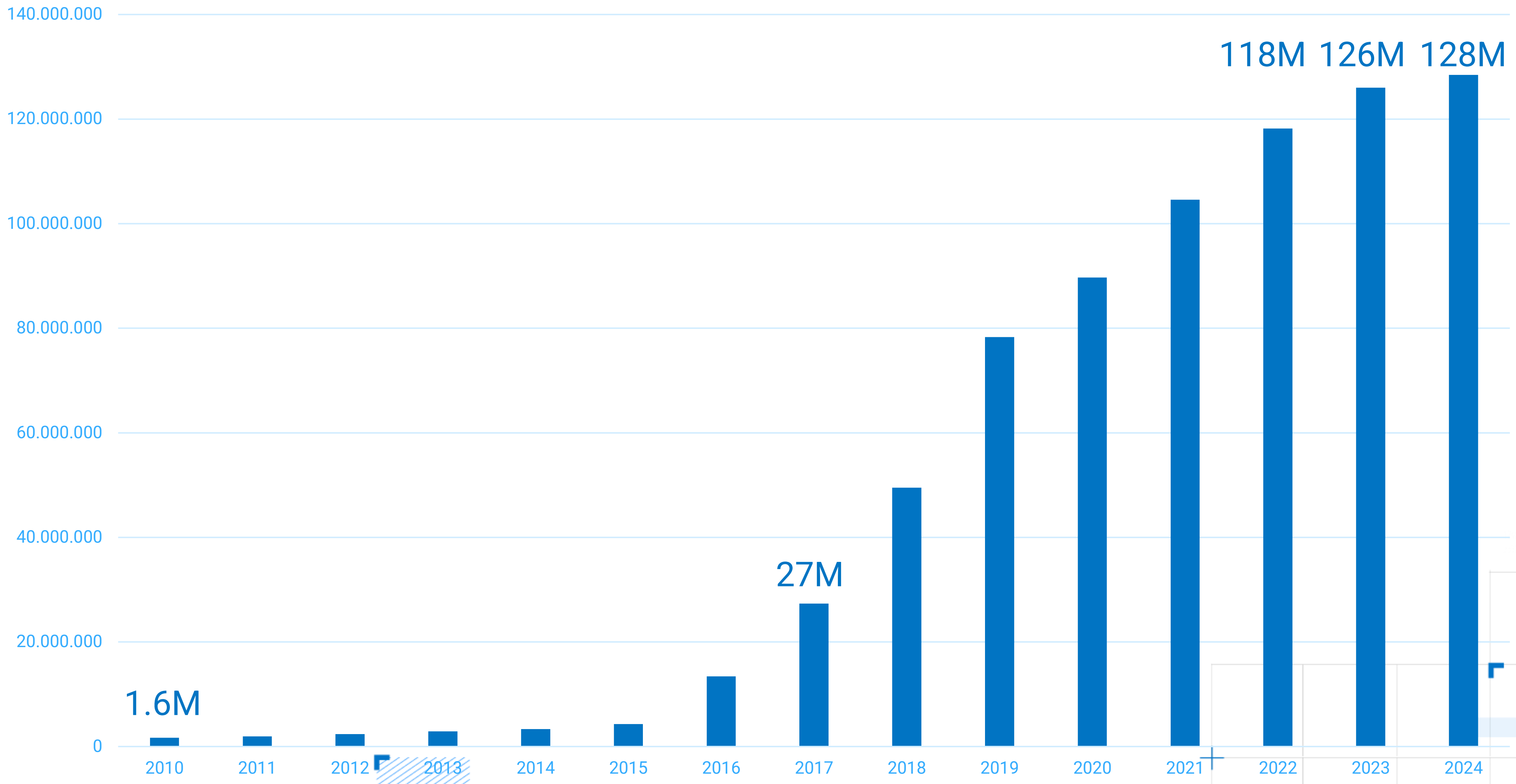
- CA/Browser Forum
  - Code Signing
  - SMIME
  - TLS (BR and EV)
  - NetSec
- ETSI
  - ESI
  - PQC
- VMC/AuthIndicators
- IETF
  - LAMPS
  - PQC

- 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 (SAE)
  - DG Move

TLS UPDATE

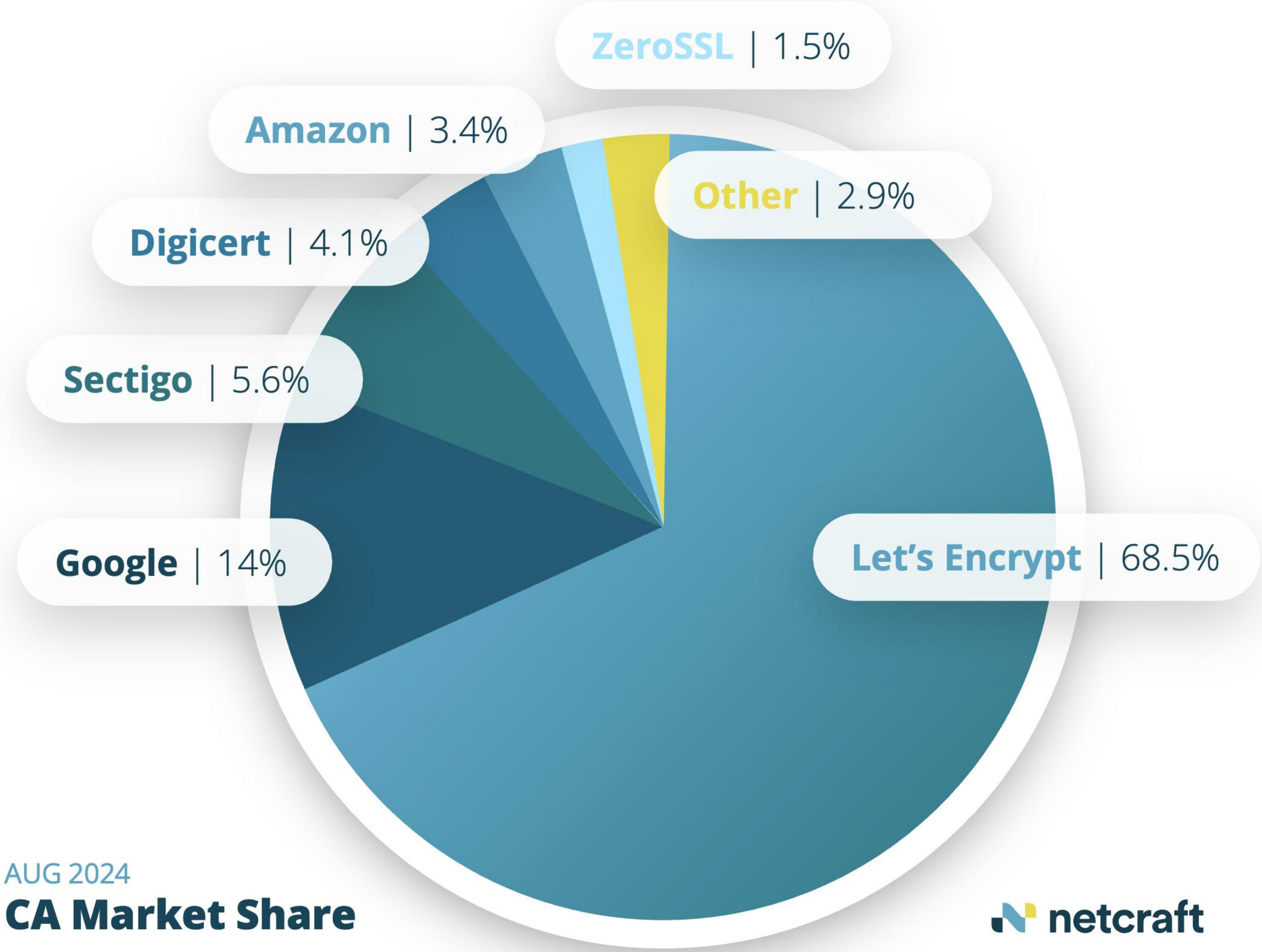
02

ACTIVE PUBLIC TLS CERTS OVER TIME



Courtesy of Netcraft

OVERALL TLS MARKET SHARE

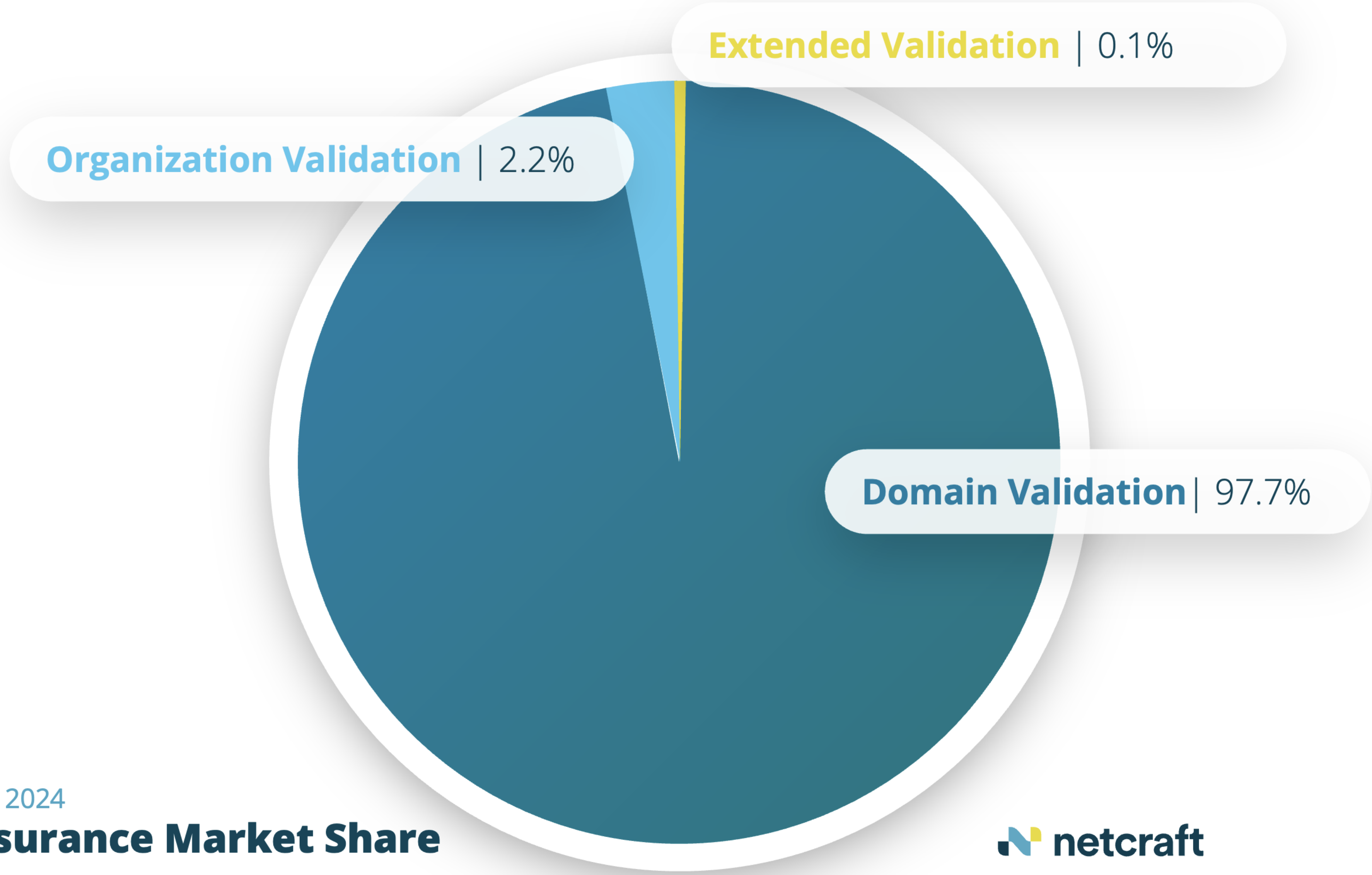


AUG 2024

CA Market Share

netcraft

TLS MARKET SHARE BY ASSURANCE TYPE



AUG 2024

Assurance Market Share

netcraft

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 (SC-67 MPIC)
- Shorter validity period for subCAs
- Shorter validity period for leaf certificates – **long term goal**

Former priorities, addressed in v1.5 policy

Current priorities

Time

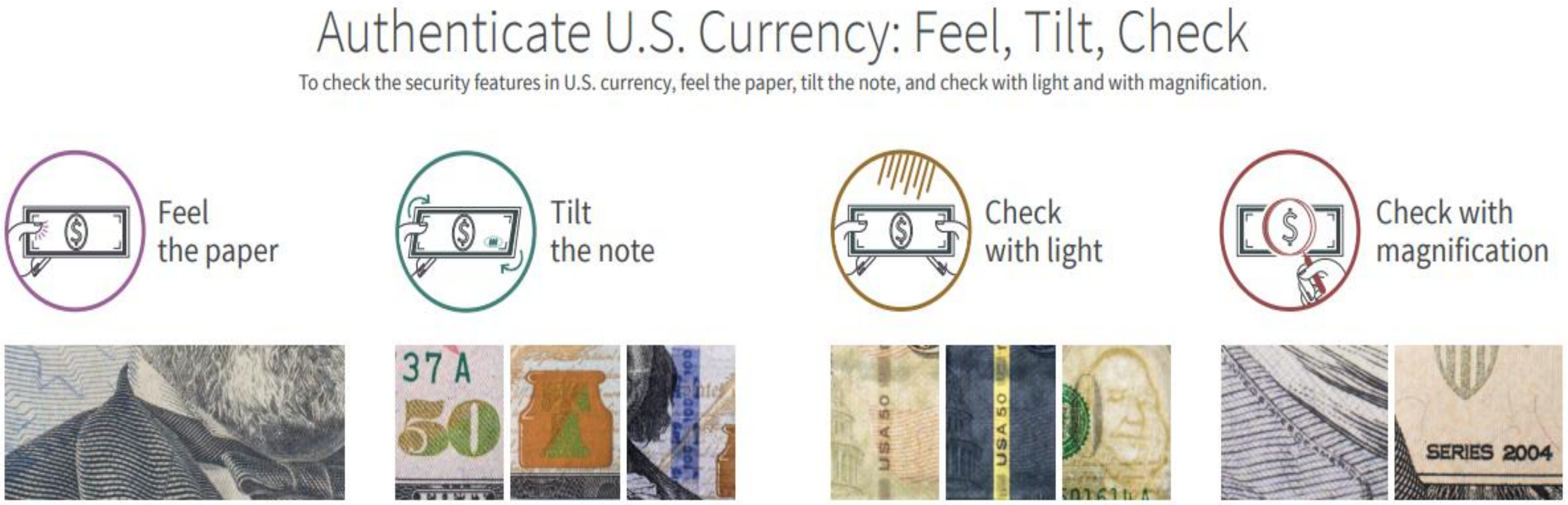
Reference: https://cabforum.org/2024/05/28/minutes-of-the-f2f-62-meeting-in-bergamo-italy-may-28-29-2024/4-CABF-F2F-62-Chrome-Browser-Update.pdf

AUTHENTICATION

03

AUTHENTICATING IN THE PHYSICAL WORLD

CASH



Authenticate U.S. Currency: Feel, Tilt, Check

To check the security features in U.S. currency, feel the paper, tilt the note, and check with light and with magnification.

Source: US Treasury

AUTHENTICATING IN THE PHYSICAL WORLD

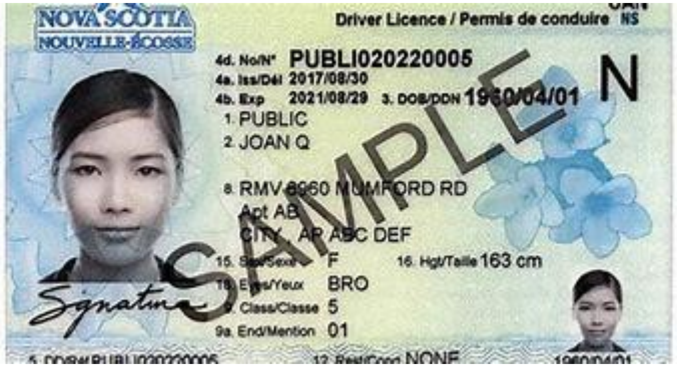
PEOPLE/IDs

VOZAČKA DOZVOLA REPUBLIKA HRVATSKA

HR

1. UZORAK
2. SPECIMEN
3. 01.01.1977
4a. 01.07.2013 4c. PU DUBROVAČKO - NERETVANSKA
4b. 01.07.2023
5. 12345678
7.
9. B

D112345671234567890121012017<2



NOVA SCOTIA NOUVELLE-ÉCOSSE

Driver Licence / Permis de conduire CAN NS

4d. No/N° PUBLI020220005

4a. Iss/Dél 2017/08/30

4b. Exp 2021/08/29 3. DOB/DDN 1960/04/01 N

1. PUBLIC
2. JOAN Q

8. RMV 6960 MUMFORD RD
Apt AB
CITY, AP ABC DEF

15. Sex/Sexe F 16. Hgt/Taille 163 cm

18. Eyes/Yeux BRO

9. Class/Classe 5

9a. End/Mention 01

5. DD/Ref PUBLI020220005 12. Rest/Cond NONE 1960/04/01

SAMPLE

Signature

HELLAS

PASSPORT

Τύπος/Type P Χώρα/Country ΕΛΛ/GRC Αρ. Διαβατηρίου/Passport No. AE0000005

1. Επώνυμο/Surname
ΕΛΛΗΝΑΣ
ELLINAS

2. Όνομα/Name
ΓΕΩΡΓΙΟΣ
GEORGIOS

3. Ιθαγένεια/Nationality ΕΛΛΗΝΙΚΗ / HELLENIC

4. Φύλο/Sex M

5. Ημ. γέννησης/Date of birth 04 Apr 65

6. Τόπος γέννησης ΣΠΑΡΤΗ GRC
Place of birth SPARTI

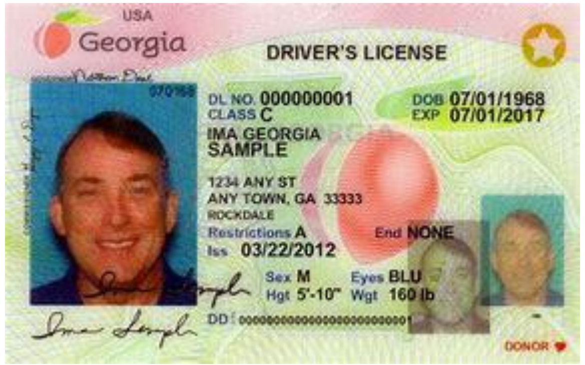
7. Ημ. έκδοσης/Date of issue 29 Aug 07

8. Ημ. λήξης/Date of expiry 28 Aug 12

9. Εκδ. Αρχή/Issuing office Α.Ε.Α./Δ.Δ. - N.P.C. 10. Ύψος/Height 1,82

P<GRCELLINAS<<GEORGIOS<<<<<<<<<<<<<<<<<<<<<<<<

AE00000057GRC6504049M1208283<<<<<<<<<<<<<<<00



USA Georgia

DRIVER'S LICENSE

DL NO. 000000001 DOB 07/01/1968

CLASS C EXP 07/01/2017

IMA GEORGIA
SAMPLE

1234 ANY ST
ANY TOWN, GA 33333
ROCKDALE

Restrictions A End NONE

Iss 03/22/2012

Sex M Eyes BLU

Hgt 5'-10" Wgt 160 lb

DD 0000000000000000000000001

DONOR

AUTHENTICATING IN THE PHYSICAL WORLD

PHYSICAL SIGNATURES

https://www.youtube.com/watch?v=-DKJwtW6NaE

AUTHENTICATING IN THE PHYSICAL WORLD

MEDICINE

Tamper proof, laser coding

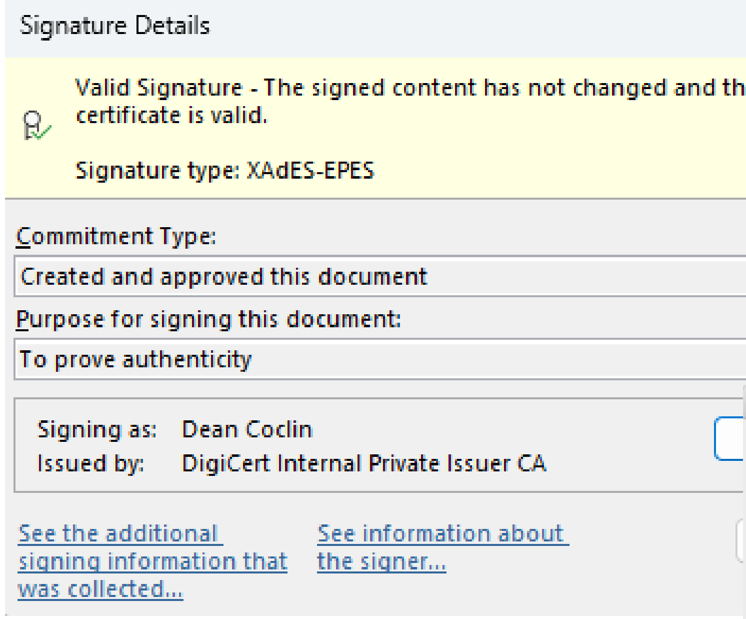
AUTHENTICATING IN THE PHYSICAL WORLD

COLLECTIBLES

https://www.youtube.com/watch?v=buHFfvNuSSw

AUTHENTICATING IN THE DIGITAL WORLD

DOCUMENTS – Adobe, Apple, Microsoft



Signature Details

Valid Signature - The signed content has not changed and the signer's certificate is valid.

Signature type: XAdES-EPES

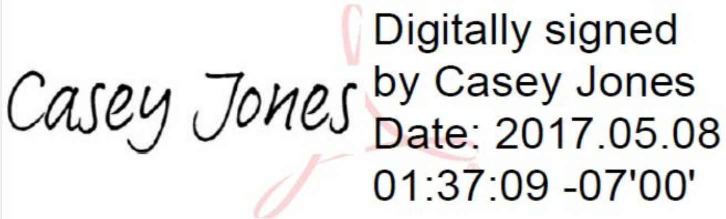
Commitment Type:
Created and approved this document

Purpose for signing this document:
To prove authenticity

Signing as: Dean Coclin
Issued by: DigiCert Internal Private Issuer CA

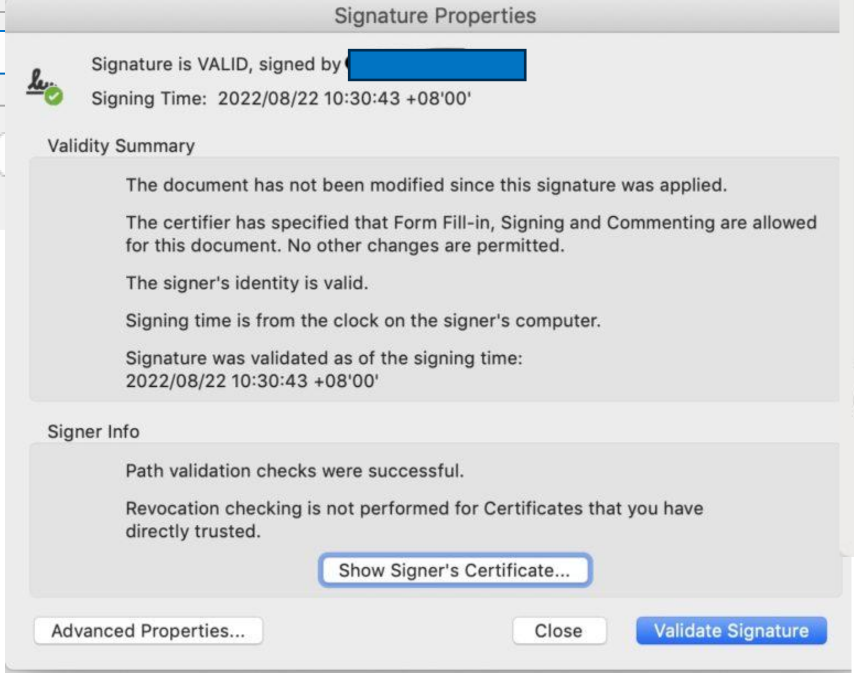
See the additional signing information that was collected...

See information about the signer...



Casey Jones

Digitally signed by Casey Jones
Date: 2017.05.08 01:37:09 -07'00'



Signature Properties

Signature is VALID, signed by [redacted]
Signing Time: 2022/08/22 10:30:43 +08'00'

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 signer's identity is valid.

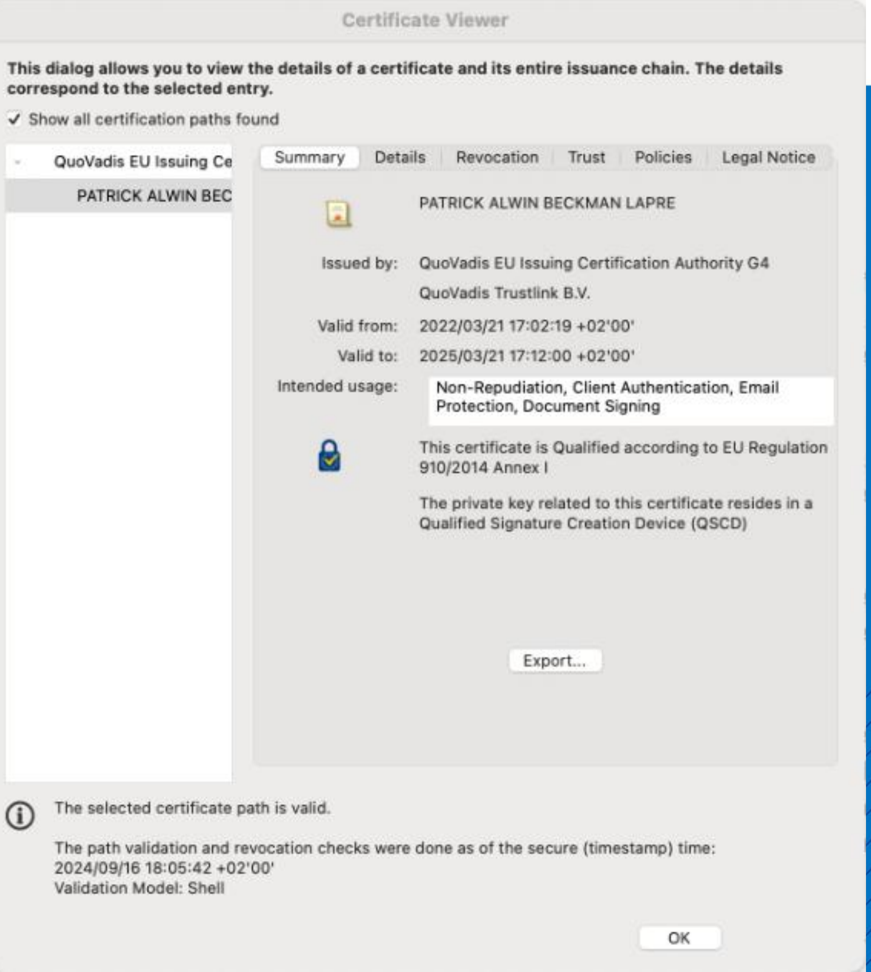
Signing time is from the clock on the signer's computer.

Signature was validated as of the signing time:
2022/08/22 10:30:43 +08'00'

Signer Info

Path validation checks were successful.

Revocation checking is not performed for Certificates that you have directly trusted.



Certificate Viewer

This dialog allows you to view the details of a certificate and its entire issuance chain. The details correspond to the selected entry.

✓ Show all certification paths found

PATRICK ALWIN BECKMAN LAPRE

Issued by: QuoVadis EU Issuing Certification Authority G4
QuoVadis Trustlink B.V.

Valid from: 2022/03/21 17:02:19 +02'00'

Valid to: 2025/03/21 17:12:00 +02'00'

Intended usage: Non-Repudiation, Client Authentication, Email Protection, Document Signing

This certificate is Qualified according to EU Regulation 910/2014 Annex I

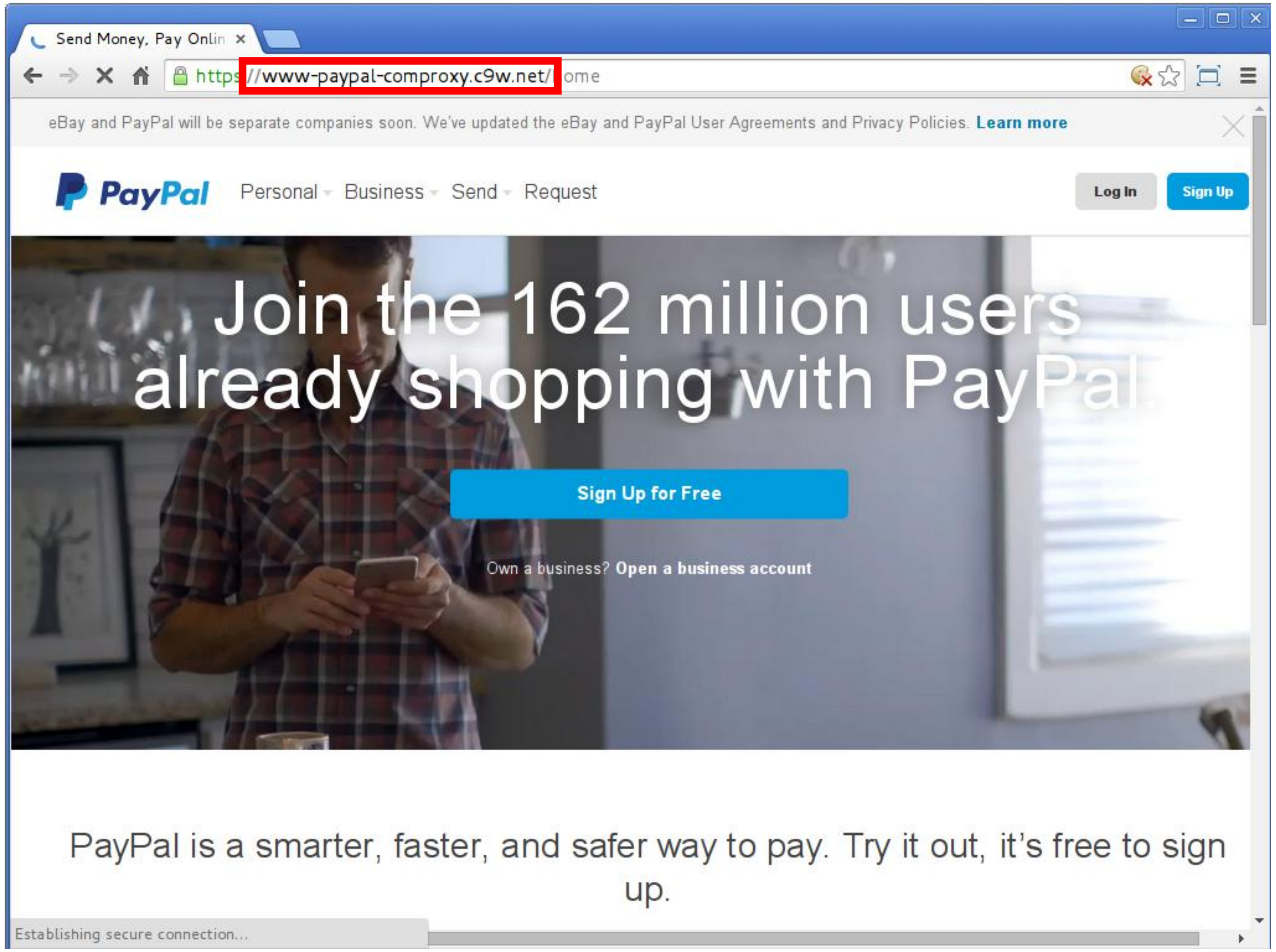
The private key related to this certificate resides in a Qualified Signature Creation Device (QSCD)

The selected certificate path is valid.

The path validation and revocation checks were done as of the secure (timestamp) time:
2024/09/16 18:05:42 +02'00'
Validation Model: Shell

BUT WHAT ABOUT WEBSITES?

How do we trust we are on the page we think we should be at?



eBay and PayPal will be separate companies soon. We've updated the eBay and PayPal User Agreements and Privacy Policies. Learn more

Join the 162 million users already shopping with PayPal

Own a business? Open a business account

PayPal is a smarter, faster, and safer way to pay. Try it out, it's free to sign up.

Why don't we identify who owns the website?

How can we authenticate it?

EIDAS TO THE RESCUE

Requirements from Article 45 and Annex IV

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

Providers of web-browsers shall ensure support and interoperability with qualified certificates for website authentication

QWACS will contain an indication, at least in a form suitable for automated processing, that the certificate has been issued as a qualified certificate for website authentication

Is it perfect? No
Is it bad? No

Is it workable? **Yes**

SECURITY DISPLAYS HAVE TO BE.....

Innovative

Something that users want to try and play with

Intuitive, Familiar

Remember my street sign presentation?

Why did they move the START menu in Win 11?

User friendly

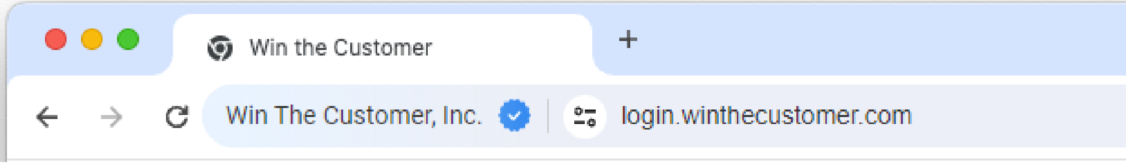
Enhance experience for the user

Sticky, Consistent

If it’s not there, you miss it

Remember PRNDL?

WHAT'S POSSIBLE IN AN INTUITIVE DISPLAY?

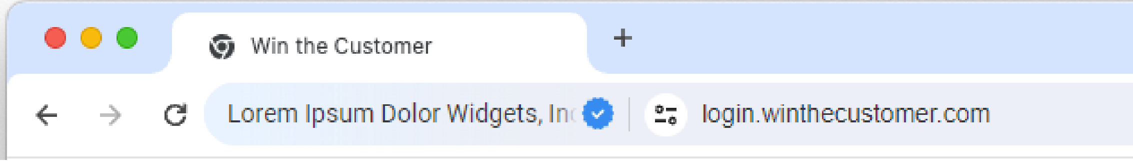

Win the Customer

Win The Customer, Inc.

login.winthecustomer.com

Max Character Count

Organization name fades to the right if longer than a set character count, similar to treatment of overflow text


Win the Customer

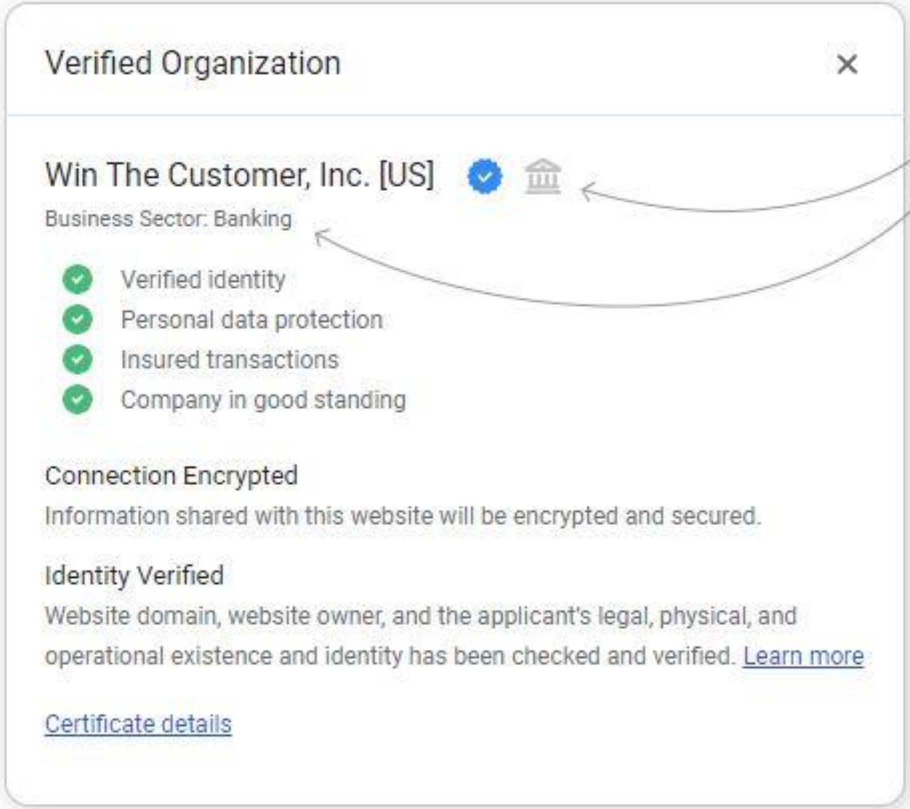
Lorem Ipsum Dolor Widgets, Inc

login.winthecustomer.com

Popup display

Display card that shows when organization name is clicked.

- Closely follows Chrome's UI patterns for a seamless user experience.
- Displays to the non-technical user that the domain and identity of the website owner has been vetted.
- Possible additional attribute represented with an icon and business sector designation.


Verified Organization

Win The Customer, Inc. [US]

Business Sector: Banking

- ✓ Verified identity
- ✓ Personal data protection
- ✓ Insured transactions
- ✓ Company in good standing

Connection Encrypted

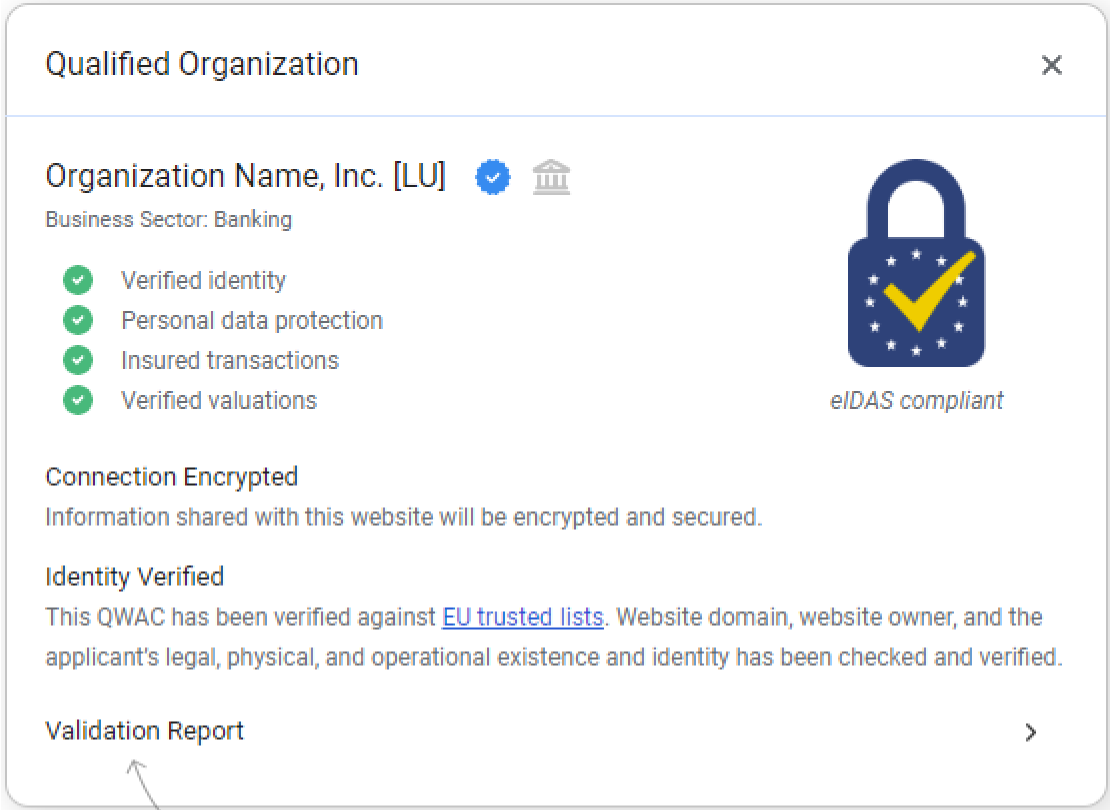
Information shared with this website will be encrypted and secured.

Identity Verified

Website domain, website owner, and the applicant's legal, physical, and operational existence and identity has been checked and verified. Learn more

Certificate details

QWAC DISPLAY



Qualified Organization ✕

Organization Name, Inc. [LU] ✓

Business Sector: Banking

- ✓ Verified identity
- ✓ Personal data protection
- ✓ Insured transactions
- ✓ Verified valuations

eIDAS compliant

Connection Encrypted

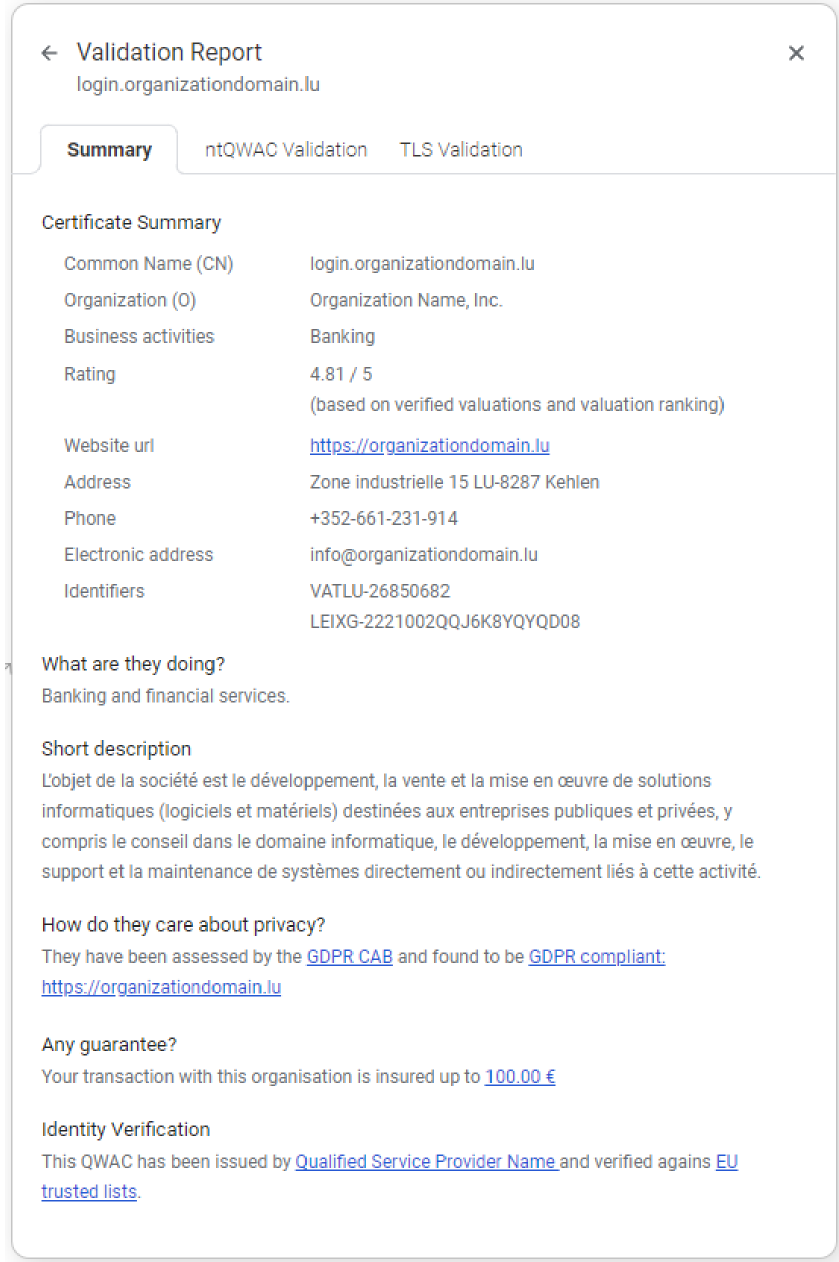
Information shared with this website will be encrypted and secured.

Identity Verified

This QWAC has been verified against EU trusted lists. Website domain, website owner, and the applicant's legal, physical, and operational existence and identity has been checked and verified.

Validation Report >

Clicking Validation Report reveals further details within the pop-up display.



← Validation Report ✕

login.organizationdomain.lu

Summary | ntQWAC Validation | TLS Validation

Certificate Summary

Common Name (CN)	login.organizationdomain.lu
Organization (O)	Organization Name, Inc.
Business activities	Banking
Rating	4.81 / 5 (based on verified valuations and valuation ranking)
Website url	https://organizationdomain.lu
Address	Zone industrielle 15 LU-8287 Kehlen
Phone	+352-661-231-914
Electronic address	info@organizationdomain.lu
Identifiers	VATLU-26850682 LEIXG-2221002QQJ6K8YQYQD08

What are they doing?

Banking and financial services.

Short description

L'objet de la société est le développement, la vente et la mise en œuvre de solutions informatiques (logiciels et matériels) destinées aux entreprises publiques et privées, y compris le conseil dans le domaine informatique, le développement, la mise en œuvre, le support et la maintenance de systèmes directement ou indirectement liés à cette activité.

How do they care about privacy?

They have been assessed by the GDPR CAB and found to be GDPR compliant: https://organizationdomain.lu

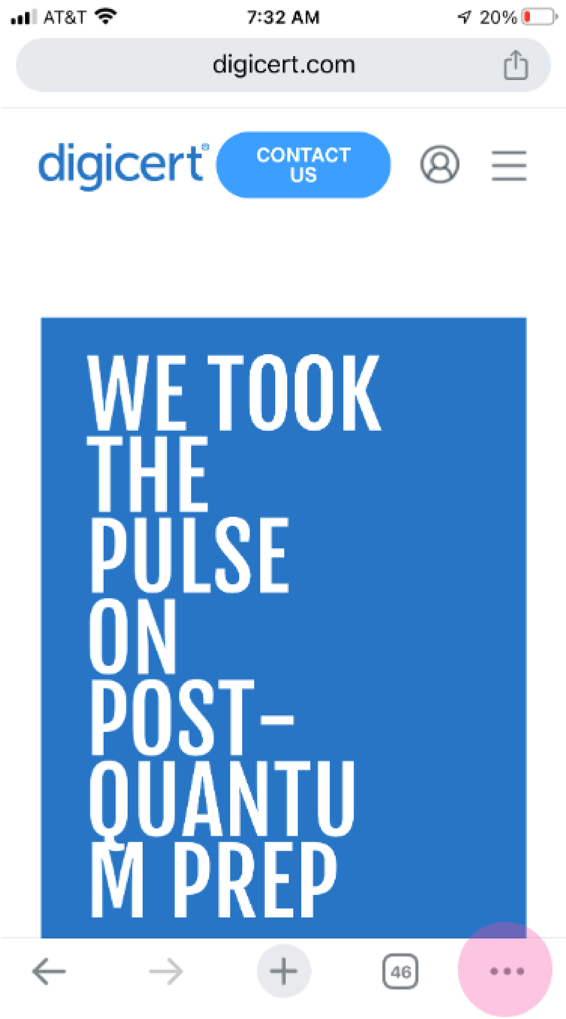
Any guarantee?

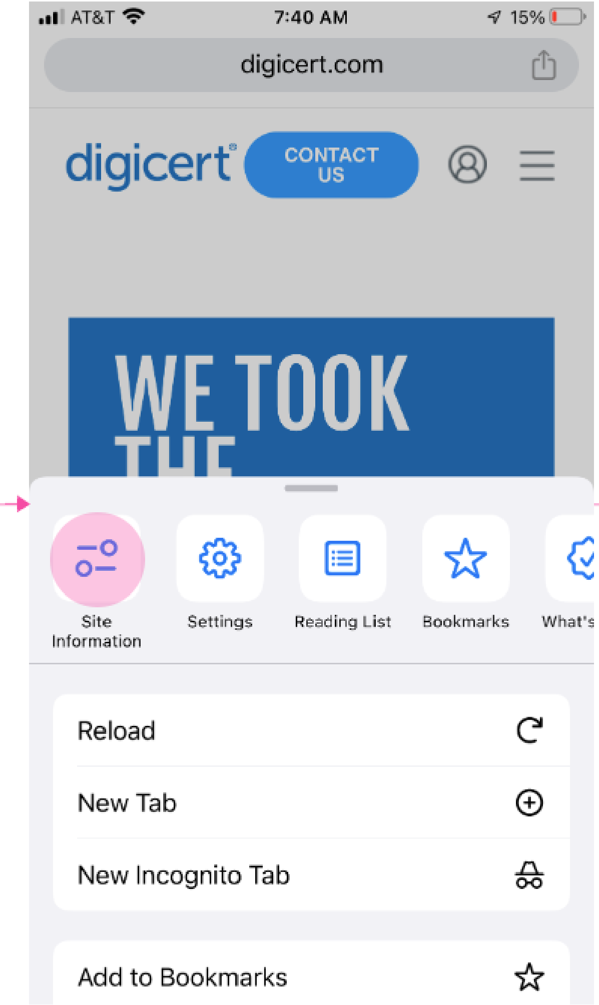
Your transaction with this organisation is insured up to 100.00 €

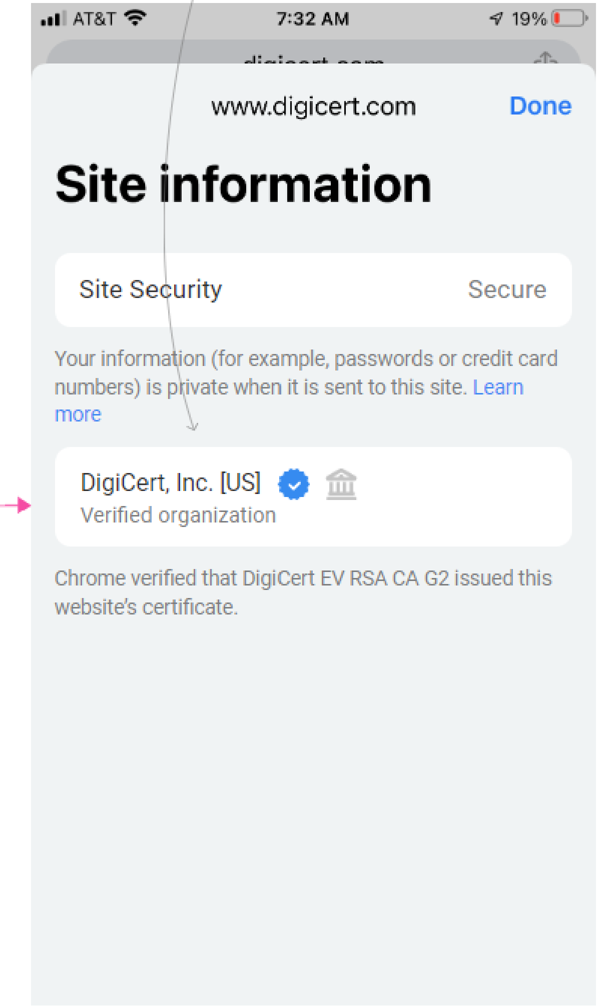
Identity Verification

This QWAC has been issued by Qualified Service Provider Name and verified agains EU trusted lists.

MOBILE DISPLAY (CHROME ON IOS)







AT&T 7:32 AM 19%

www.digicert.com Done

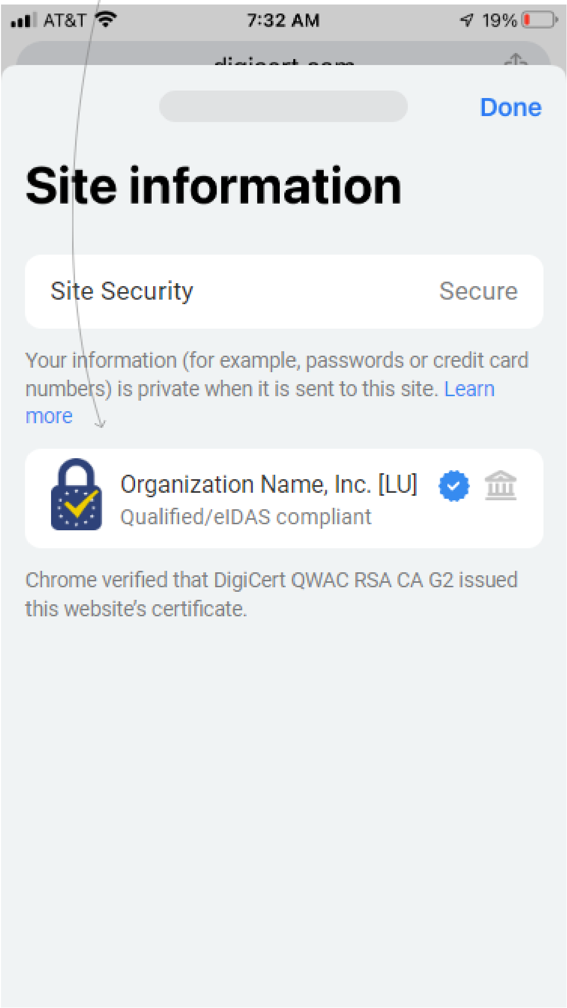
Site information

Site Security: Secure

Your information (for example, passwords or credit card numbers) is private when it is sent to this site. Learn more

DigiCert, Inc. [US]
Verified organization

Chrome verified that DigiCert EV RSA CA G2 issued this website's certificate.



AT&T 7:32 AM 19%

Done

Site information

Site Security: Secure

Your information (for example, passwords or credit card numbers) is private when it is sent to this site. Learn more

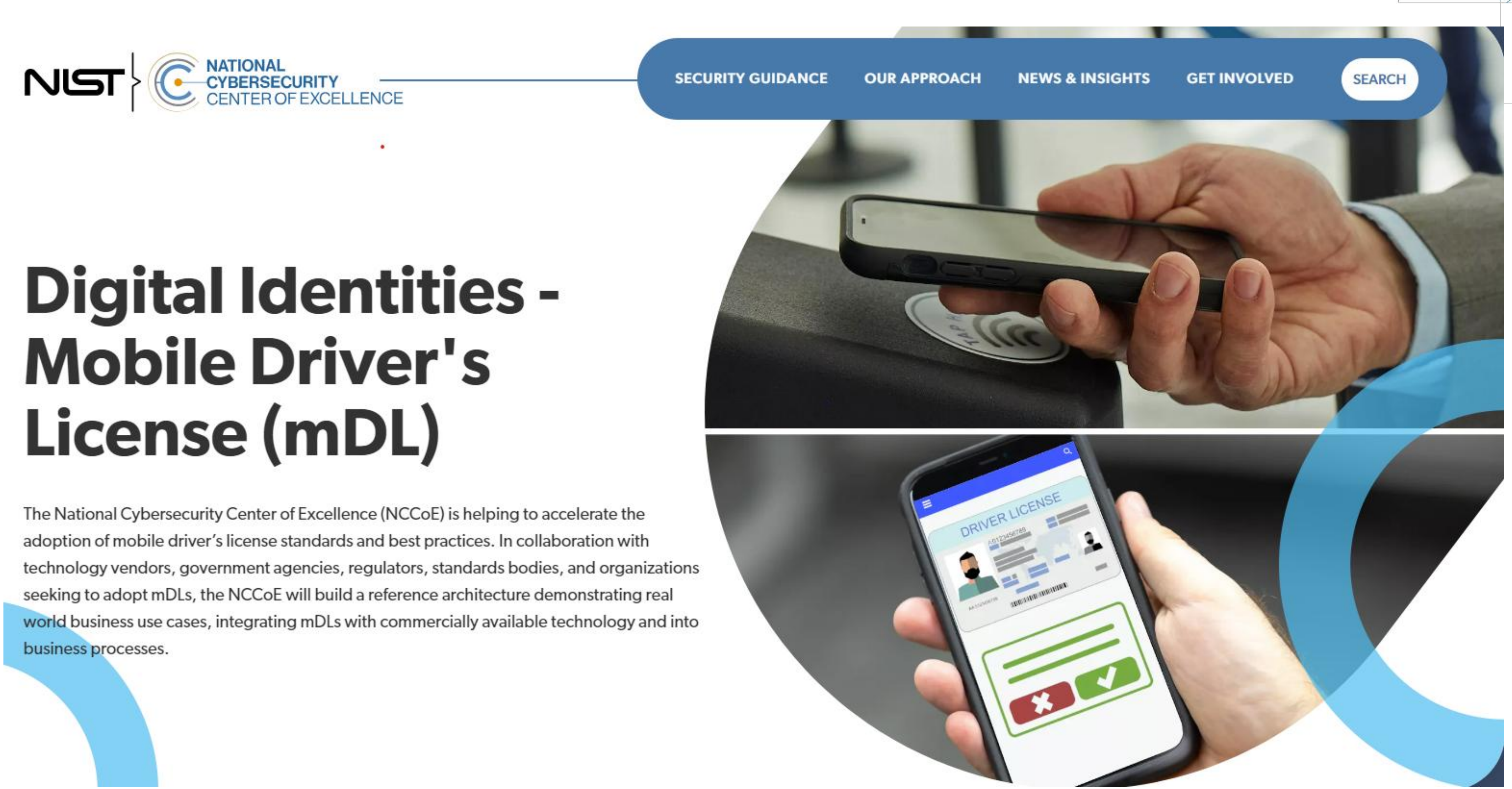
Organization Name, Inc. [LU]
Qualified/eIDAS compliant

Chrome verified that DigiCert QWAC RSA CA G2 issued this website's certificate.

USA PROJECTS

04

US MOBILE DRIVERS LICENSE PROOF OF CONCEPT



Digital Identities - Mobile Driver's License (mDL)

The National Cybersecurity Center of Excellence (NCCoE) is helping to accelerate the adoption of mobile driver's license standards and best practices. In collaboration with technology vendors, government agencies, regulators, standards bodies, and organizations seeking to adopt mDLs, the NCCoE will build a reference architecture demonstrating real world business use cases, integrating mDLs with commercially available technology and into business processes.

https://www.nccoe.nist.gov/projects/digital-identities-mdl

PKI LINTING FOR EIDAS

- Open-source contribution from DigiCert
- Support added to check compliance of eIDAS web authentication certificates, including QWACs, against relevant technical standards
- Checks certificates' compliance with requirements of ETSI EN 319 411 and ETSI EN 319 412, as well as ETSI TS 119 495 (for PSD2 certificates)

SUMMARY

05

SUMMARY

Standards are the foundation for digital trust, whether in the US or EU

Compliance

Audits

Tools (PKIlint)

Managing Trust

Clear, user-friendly displays

Innovative, Intuitive, not needing instructions (tool tips are OK!)

Sticky and consistent

Enhancing Trust

Web PKI

eIDAS

Digital Wallets

iOT devices

digicert®

EXTENDING TRUST
MANAGING TRUST
ESTABLISHING TRUST
COMPLIANCE
AUTHORING STANDARDS
DIGITAL TRUST