CA Day – Wednesday, 23th September 2020 at ESMT, Schloßplatz 1, 10178 Berlin

Time	Title	Speaker	Organisation	
09:00	Welcome by D-TRUST; TÜVIT and ESMT Moderation: Patrick von Braunmühl	Kim Nguyen Dirk Kretschmar Martin Schallbruch Patrick von Braunmühl	D-TRUST TUVIT ESMT Bundesdruckerei	Anwesend Anwesend Anwesend Anwesend
09:20	eIDAS Updates in 2020	Norbert Sagstetter	EC DG Connect H.4	**Remote**
09:40	ETSI ESI Activities and PSD2 Status	Nick Pope	Security & Standards Associates	**Remote**
10:00	ACABc Requirements for Audit reports eIDAS and PTC	Matthias Wiedenhorst	TUVIT	Anwesend
10:20	Trust Zones -The Gordian knot between QWAC and Browser: Proposal for a solution	Enrico Entschew	D-TRUST	Anwesend
10:40	Q+A and Coffee Break			
11:00	Artificial intelligence based user identification under eIDAS	Clemens Wanko	TÜV Austria	Anwesend
11:20	CA/B-Forum: Status and future activities	Dimitris Zacharopoulos	Harica, CA/B-Chair	Anwesend
11:40	Audits used by Mozilla's CA Program	Ben Wilson	Mozilla	**Remote**
12:00	Identity Proofing for Trust Service Subjects	Sylvie Lacroix	Sealed	Anwesend
12:20	How to improve identities in browsers	Chris Bailey	ENTRUST Datacard	**Remote**
12:40	Helping Qualified Trust Services become a global standard	Andrea Vale	Adobe	**Remote**
13:00	Wrap up and Q+A			

European Digital Identity

CA Day

23 September 2020

Speech of President von der Leyen *(16 September 2020)*

“Every time an App or website asks us to create a new digital identity or to easily log on via a big platform, we have no idea what happens to our data in reality. That is why the Commission will soon propose a secure European e-identity. One that we trust and that any citizen can use anywhere in Europe to do anything from paying your taxes to renting a bicycle. A technology where we can control ourselves what data and how data is used.”

The Issue at Stake

Identification has become fundamental to the Digital World:

- **Users** expect speed, security, convenience and protection of personal data
- **Markets** require versatile, secure and trustworthy identification
- **Technology** creates opportunities and challenges: mobile identification, distributed ID systems, 5G, cybersecurity (e.g. secure elements / SE).

eID – Limiting Factors

- **Limited Offer -** 14 of 27 Member States have notified eID scheme (including 7 mobile schemes)
- **Limited Access -** 55% of EU population has access to a notified scheme in their MS)
- **eID is limited to interactions with the public sector**
- **Low Public Sector Digitalisation** (only 14% of public providers offer eIDAS authentication)

Vision for a European Digital Identity

- **Universally Available** – all EU citizens and businesses may use it on a voluntary basis
- **Universally Useable** – recognised by private and public service providers for all transactions that require authentication (« EU single-sign-on »)
- **Protecting Personal Data** – users must be able to take control of their identity and consent to the disclosure of personal data

Technical Implementation *– Basic Characteristics*

- **Mobile Application** - hardware-based Secure Element (local or remote) or software-based Secure Element
- **Common Standards** - Specific Standardisation Framework to be developed by ETSI for EUeID / privacy by design architecture

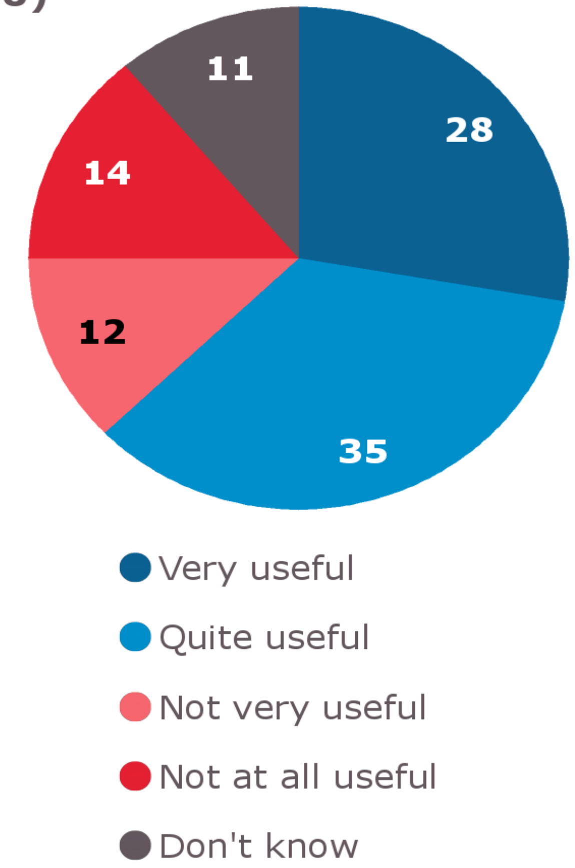
Support for a European Digital ID – *Eurobarometer*

March 2020

A large majority (63%) think it would be useful to have a secure single digital ID for all online services and give them control over the use of their data

Support ranges from 52% (LT) to 80% (DK)

QC15 How useful would it be for you to have a secure single digital ID that could serve for all online services (both public and private) and give you control over the use of your data?
(% - EU)



Support for User Control of Data *– Eurobarometer March 2020*

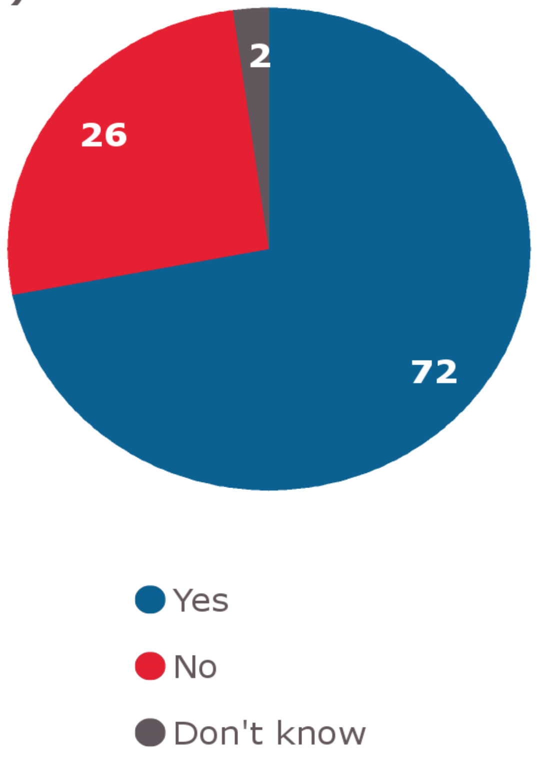
An overwhelming majority (72%) want to know how their data are used when they use social media accounts to access websites

Authentication:

29% authenticate through social media accounts (DK-46%)

70% authenticate via user-name / password (NL-96%, FR/DE-78%..)

QC14 Do you want to know how your data are used when you use your social media account to access other websites?
(% - EU)



Thank you

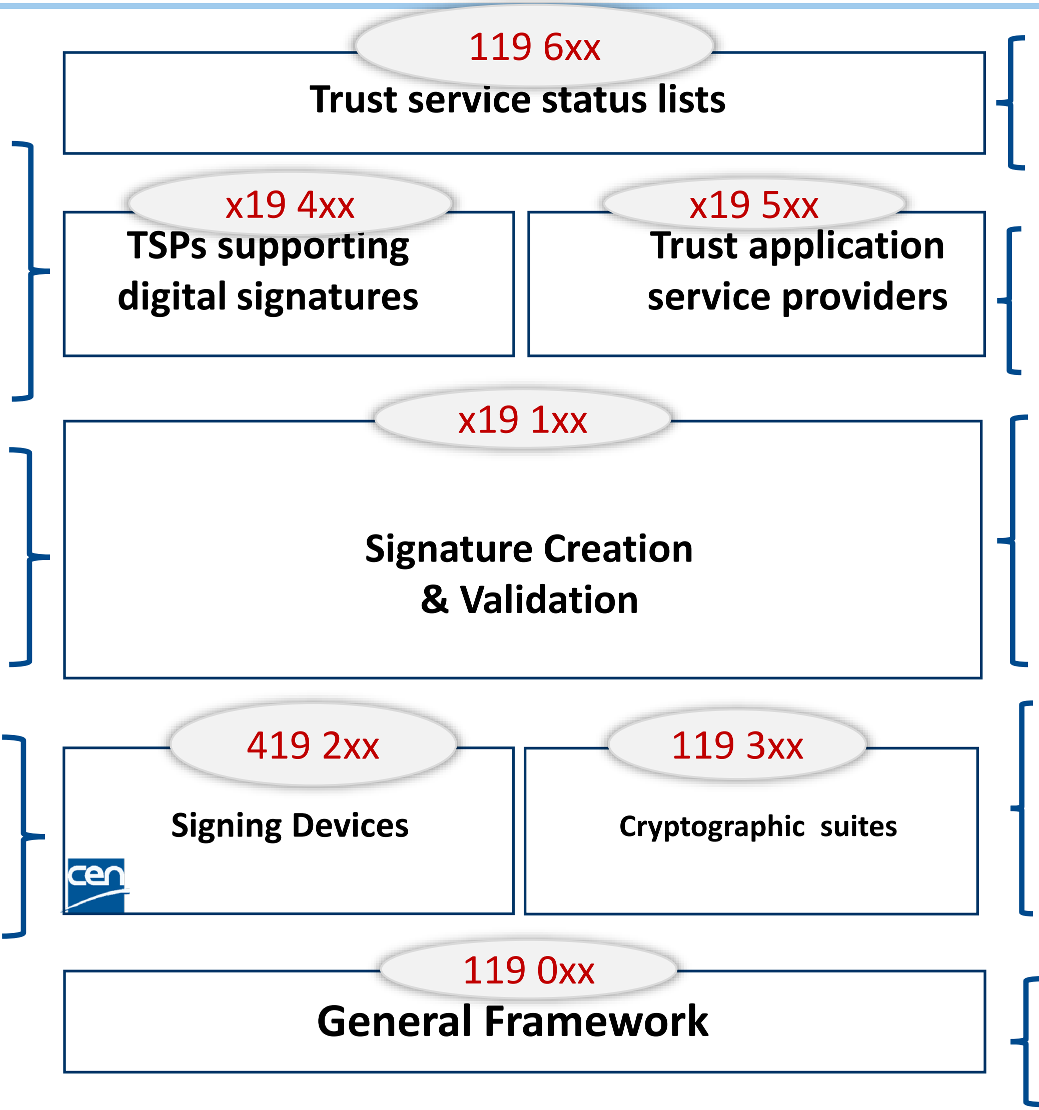
The Standards People

ETSI ESI Activities Update

CA Day 2020

Presented by: **Nick Pope – Vice Chair ETSI ESI**

ETSI & CEN Standards supporting eIDAS – the overall picture



119 6xx
Trust service status lists

- Trusted list ✓
- Using & interpreting trusted list (new)
- Validation policy using trusted list (new)

Trust services for:
- Issuing certificates ✓ *
- Time Stamping ✓
- Signature creation services ✓ *
- Signature validation services ✓ *
- Identity proofing (new)

x19 4xx
TSPs supporting digital signatures

x19 5xx
Trust application service providers

Trust services for:
- Registered eDelivery / eMail ✓
- Long term preservation ✓

x19 1xx
Signature Creation & Validation

- AdES creation & validation
  - Part 1: procedures ✓
  - Part 2: signature validation report ✓ *
  - Part 3: extended signature validation (new)

Formats:
- XAdES (XML) ✓ *
- CAdES (CMS) ✓ *
- PAdES (PDF) ✓
- ASiC (containers) ✓
- JAdES (new)

419 2xx
Signing Devices

119 3xx
Cryptographic suites

CC Protection Profiles
- QSCD - Smart Cards ✓
- HSM used as QSCD ✓
- HSM used by TSPs ✓
- Remote QSCD ✓

- Signature suites ✓
  - Hash
  - Asymmetric crypto
  - Key generation
  - Lifetime
- Schema for algorithm catalogues (new)

119 0xx
General Framework

- Standards framework ✓
- Common definitions ✓
- Guides ✓

✓ Completed
* Update
(new) New

Trust services issuing certificates – Updates
EN 319 401, EN 319 411-1 & EN 319 411-2 – Policy requirements

Multiple detailed changes to clarify requirements including:

- Trust service components (subcontracted components e.g. RA, server signing ….)
- Alignment with Short term certificates, and opening RFC 5280 size limits in EN 319 412-x
- Re-wording existing requirements, clarifying terminology
- Alignment of 411-1 requirements with 411-2, some general requirements moved from 411-2 to 411-1
- Use of EU Trusted List by relying parties

EN 319 401: 14 Changes, EN 319 411-1: 25 Changes, EN 319 411-2: 4 Changes

Draft EN October / November

Trust services issuing certificates – Updates EN319 412-1,-2,-3,-5 Certificate profiles

TS/EN 319 412-1: General

- Placement of eID information to Certificate Profile,
- Indicator of “short term” certificates
- Use of ‘EL’ as alternative to country code ‘GR’

EN 319 412-2: Natural persons & 412-3 Legal persons

- Clarification Key Usage indicator
- Clarification Authority information access
- Removal on RFC 5280 64 character limit on naming fields

EN 319 412-5: Qualified Certificate Statements

- Facilitate QC Statements by non-EU Qualified certificates

Published

Trusted List
TS 119 612 – Use and interpretation

Draft TS 119 615: Procedures for using and interpreting European Union Member States national trusted lists

- on the use of information within an EU Trusted List by relying parties,
- how to process a trusted list in order to obtain information about a QTSP and QTS(s) it provides
- Publication depends on clarification of EU Official Journal announcement regarding use of “compiled list” / pivot List of Trusted Lists.

Draft TS 119 172-4: Signature Validation Policy for European Qualified Electronic Signatures / Seals Using Trusted Lists

Awaiting EU Official Journal publication regarding EU list of trusted lists.

Extended Signature Validation

TS 119 102-3 Extended signature validation procedures aim to avoid the risks in accepting documents whose signature validates but the data format can lead to misinterpretation of the content (e.g. change in appearance due to macros within the document without changing the signed bytes)

Sub part 1: General

Sub part 2: Signed PDF (PAdES)

Sub part 3: Signed XML (XAdES)

Sub part 4: ASiC packages

Publication Q4 2021

TS 119 152 JAdES digital signatures

- Based on JSON Web Signatures RFC 7515
- Separate Profile of JAdES for open banking being developed jointly with Open Banking Europe
- Publication due end 2020

ETSI

The Standards People

Ongoing Standards issues
1) Web browser and QWACs
2) PSD2 & Brexit

CA Day 2020

Nick Pope – Director Security & Standards

Note: These are my own opinions not those of ETSI nor Open Banking Europe, and I reserve the right to change my views following further events. Consult you own lawyers to get a legal opinion.

Web browser and QWACs
- EU Informal Working Group on QWACs meetings

- Set up by EU Commission

- Membership
  - Web browser suppliers: Apple, Google, Microsoft, Mozilla, Opera, and Vivaldi
  - EU: Commission, ENISA, ETSI
- Aim
  - Discuss the use of Qualified Website Authentication Certificates in Web Browsers

Web browser and QWACs
- The dialogue

Proposal from Google and Mozilla:

- Remove Specific Requirements to link QWAC to Transport Layer Security (TLS/SSL) protocol & Split QWAC into DV Certificate and ntQWAC (non TLS QWAC)

ETSI Response (see ESI(20)000_16r3):

- “Making it possible to authenticate the website” is an essential element of QWACs
- ETSI Proposals using attribute certificate or single certificate based on CABF Baseline

Proposal from Browsers

- Offers alternative approach of using QWAC to sign set of certificates

EU Response

- Need clarify on how browser proposal makes it possible to authenticate the website

Proposal from Browsers

- Yet another solution (nt-ac-QWAC) which still did not say how website authentication is provided using a QWAC

2 October deadline for contribution to eIDAS review

Web browser and QWACs
- The conclusion

- ➢ Browser vendors are concerned primarily with supporting website authentication at the domain level.

- ➢ Browser vendors have not yet come forth with a solution which meets the EU requirements.

- ➢ The absence of an acceptable solution can be taken into account in the eiDAS review and may result in additional regulatory measures:
  e.g. to clarify that a QWAC needs to make it possible to authenticate a website.

Web browser and QWACs
- Need to promote advantages

- EU QWACs provide independent trust

- EU QWACs protect consumers by assuring that there is a genuine and legitimate entity standing behind the website.

PSD2 and Brexit
- use of PSD2 eIDAS certificates in the UK

- UK Open Banking is the largest community of "Third party payment service providers" (TPPs) currently applying PSD2 using eIDAS certificates
    - UK 178 TPPs of total around 400

- EBA (European Banking Authority) has issued statement which states that UK PSD2 eIDAS certificates will be revoked

  https://eba.europa.eu/eba-calls-financial-institutions-finalise-preparations-end-transitional-arrangements-between-eu-and

- UK Open Banking :
    - Assumes that existing UK eIDAS certificates will be revoked,
    - Alternative certificates are being issued by UK Open Banking Implementation Entity
    - Use of eIDAS certificates will continue to be supported

  https://www.fca.org.uk/publication/consultation/cp2018-quarterly-consultation-paper-no-29.pdf

PSD2 & Brexit
ETSI TS 119 495 for PSD2 and open banking

- Currently, TS 119 495 is specifically aimed at for PSD2 for Europe

- ETSI proposing to "internationalise" of TS 119 495 to be applicable to PSD2 and other similar national regulations for open banking

- UK alternative "OBSeals" and "OBWACs" are adopting TS 119 495 specific attributes

PSD2 and Brexit
- The big questions

Will existing eIDAS certificates be revoked?

☺ EBA will have no jurisdiction in the UK post Brexit

☺ As yet there is no official route for eIDAS certificates to be revoked except by request by the National Competent Authority for Open Banking

☺ UK open banking will continue to support eIDAS certificates

☹ Current certificates issued under TS 119 495 are specifically for the purpose of EU PSD2

Will EU QTSPs still be able to sell to UK?

☺ UK will continue to recognise eIDAS certificates

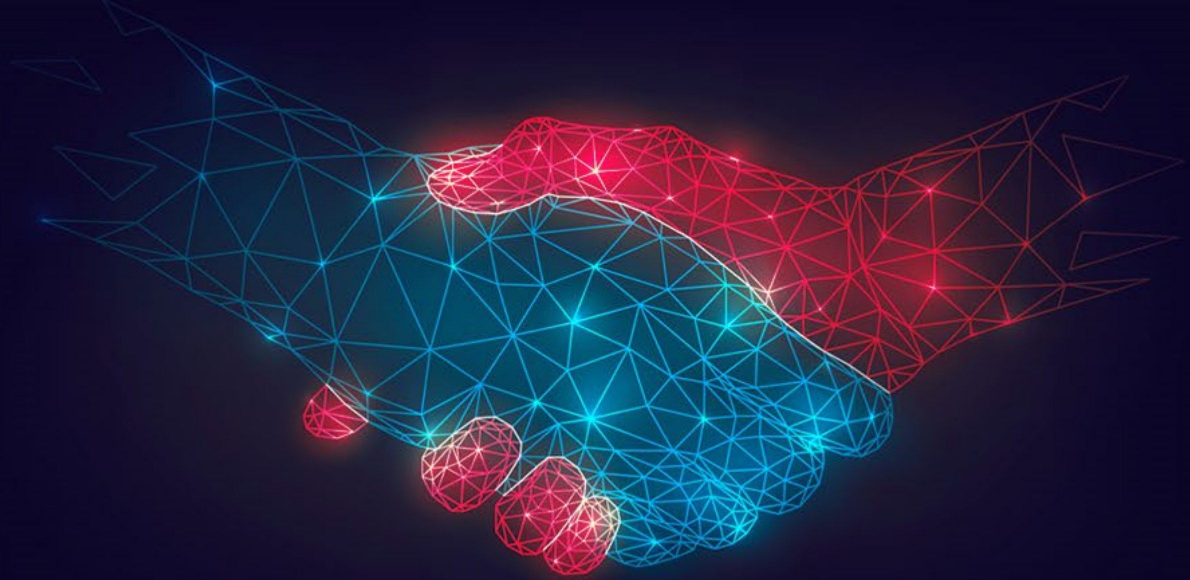
☺ Number of TPPs operate both in UK and Europe

☺ In the future TS 119 495 can continue to be basis of Open Banking around the world

☹ UK TPPs are encouraged to use UK alternative OBWACs and OBSeals

- Information on available standards and current activities: https://portal.etsi.org/TBSiteMap/ESI/ESIActivities.aspx
- ETSI standards: available for free download http://www.etsi.org/standards-search

nick.pope@secstanassoc.com



Harmonized Audit Reports for PTC and eIDAS audits

Matthias Wiedenhorst

Requirements for audit reports

-

PTC -Audits

Requirements for audit reports

PTC - Audits

- Requirements on PTC audits and PTC audit reporting can be found in various different sources
  - Browser Root Store Policies
  - CCADB Policy
  - CABF documents BR & EVCG

- ETSI TS 119 403-2 aims to consolidate the requirements into a single document

- Most audit attestation letter refusals are due to formal reasons

ETSI TS 119 403-2 V1.2.1 (2019-04)

ETSI
TECHNICAL SPECIFICATION

**Electronic Signatures and Infrastructures (ESI);
Trust Service Provider Conformity Assessment;
Part 2: Additional requirements for
Conformity Assessment Bodies auditing Trust Service
Providers that issue Publicly-Trusted Certificates**

Requirements for audit reports

PTC - Audits

- ACAB‘c members agreed on a common template as basis for PTC audit reporting
  - Fulfils the relevant requirements
  - Facilitates the formal correctness of issued audit attestations
  - Has been cross-checked by Root Store Operators
  - Can be adapted to changed or new requirements quicker as the ETSI TS

- ACAB‘c will publish a public version of that template in the near future
  - Can be used by non-ACAB‘c members as basis for their audit reporting

ACAB'c

Accredited Conformity Assessment Bodies Council (ACAB'c)

www.acab-c.com

ACAB'C

ACAB’C in short

- Association of Conformity Assessment Bodies together with other relevant stakeholders such as TSP’s, Supervisory Bodies, Standardisation Bodies
- It’s main goal is to harmonize amongst CABs a comparable/standardized application of the conformity assessment requirements by different CABs in respect with the REGULATION (EU) No 910/2014 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC (eIDAS).
- Trusted CAB’s by accreditation based on ISO standards (ISO/IEC 17065, ETSI EN 319403)
- Free of charge membership available

Requirements for audit reports

PTC - Audits

- Typical errors seen in audit statements, causing problems with the mostly automated processing of audit statements
  - CCADB format requirements are not adhered to
  - Audit statements with a different target audience are provided (e.g. eIDAS conformity assessment reports)
  - Audit standards are not properly stated or out-dated versions have been used
  - CA certificates in the scope of the audit are missing or not properly referenced

Requirements for audit reports
-
eIDAS

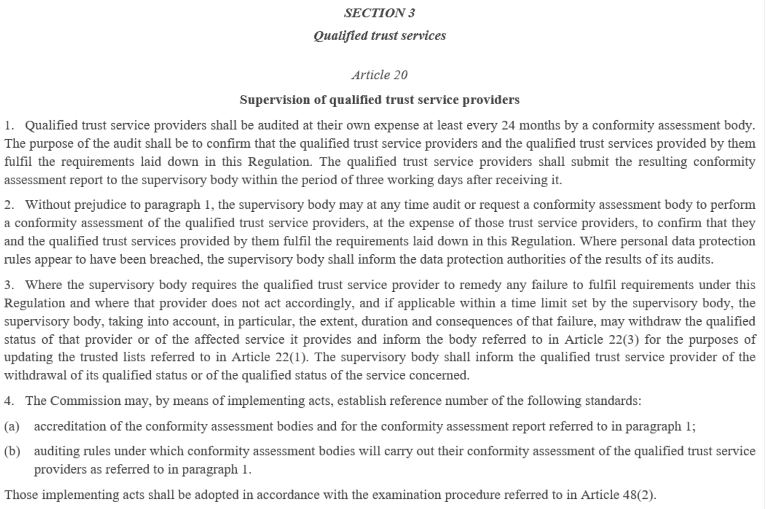
Requirements for audit reports

PTC - Audits

- eIDAS does not mandate certain content or format for conformity assessment reports

- Article 20 (4) of eIDAS allows for an implementing act about conformity assessment reports, but no such IA has been adopted yet

- As result, conformity assessment reports may vary between different CAB's



SECTION 3

Qualified trust services

Article 20

Supervision of qualified trust service providers

1. Qualified trust service providers shall be audited at their own expense at least every 24 months by a conformity assessment body. The purpose of the audit shall be to confirm that the qualified trust service providers and the qualified trust services provided by them fulfil the requirements laid down in this Regulation. The qualified trust service providers shall submit the resulting conformity assessment report to the supervisory body within the period of three working days after receiving it.

2. Without prejudice to paragraph 1, the supervisory body may at any time audit or request a conformity assessment body to perform a conformity assessment of the qualified trust service providers, at the expense of those trust service providers, to confirm that they and the qualified trust services provided by them fulfil the requirements laid down in this Regulation. Where personal data protection rules appear to have been breached, the supervisory body shall inform the data protection authorities of the results of its audits.

3. Where the supervisory body requires the qualified trust service provider to remedy any failure to fulfil requirements under this Regulation and where that provider does not act accordingly, and if applicable within a time limit set by the supervisory body, the supervisory body, taking into account, in particular, the extent, duration and consequences of that failure, may withdraw the qualified status of that provider or of the affected service it provides and inform the body referred to in Article 22(3) for the purposes of updating the trusted lists referred to in Article 22(1). The supervisory body shall inform the qualified trust service provider of the withdrawal of its qualified status or of the qualified status of the service concerned.

4. The Commission may, by means of implementing acts, establish reference number of the following standards:

(a) accreditation of the conformity assessment bodies and for the conformity assessment report referred to in paragraph 1;

(b) auditing rules under which conformity assessment bodies will carry out their conformity assessment of the qualified trust service providers as referred to in paragraph 1.

Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 48(2).

Requirements for audit reports

PTC - Audits

- ETSI TS 119 403-3 defines content requirements for conformity assessment reports
- Supervisory bodies should require the conformity assessment reports to fulfil this specification
- No additional ACAB’c template available, as requirements are relatively stable and hence no such demand has been expressed so far

ETSI TS 119 403-3 V1.1.1 (2019-03)

TECHNICAL SPECIFICATION

**Electronic Signatures and Infrastructures (ESI);
Trust Service Provider Conformity Assessment;
Part 3: Additional requirements for conformity assessment bodies assessing EU qualified trust service providers**

Contact

Matthias Wiedenhorst
Head of Certification
Division TSP

IT Infrastructure
+49 201 8999-536
m.wiedenhorst@tuvit.de

www.tuvit.de

Trust Spaces

The Gordian knot between QWAC and browser – Proposal for a solution

Datum: 23.09.2020
Ort: Berlin
Verfasser: Enrico Entschew

What distinguishes a trust space?

- Regulation
- Technical implementation
- Responsibility
- Monitoring

Trust spaces exist according to the same scheme in both the analog and digital world.

Examples for trust spaces

The browser trust space

- Regulation: Root Store Policy, Baseline Requirements, EV-Guidelines
- Technical implementation: Root Store
- Responsibility: Browser
- Monitoring: Qualified auditors and CCADB

The European Digital Single Market

- Regulation: EU regulation eIDAS, referenced implementing acts and technical standards
- Technical implementation: EU Trusted List and national eIDAS Trusted Lists
- Responsibility: EU Commission
- Monitoring: Supervisory Bodies and Conformity Assessment Bodies

The qualified certificate for website authentication (QWAC)

- Trust service of eIDAS
- Classic TLS certificate according to RFC 5280
- Check against eIDAS Trusted List
- According to eIDAS Recital 67 "Website authentication services provide a means by which a visitor to a website can be assured that there is a genuine and legitimate entity standing behind the website"
- QWAC is to be used in accordance with the rules of the EU

At the CA/Browser Forum, D-TRUST has worked with other European CAs to get the browsers to consider QWAC.

The Status Quo of the QWAC in the Browser

- Rarely used in connection with the browser
- Use only if EV guidelines are followed
- Root CA must be included in the root store of the browser
- Some specific fields are not allowed or supported for QWAC by the browsers, for example European Payment Service Directive 2 (PSD2) extensions

Discussions between the EU Commission and browsers on the recognition of QWAC are ongoing.

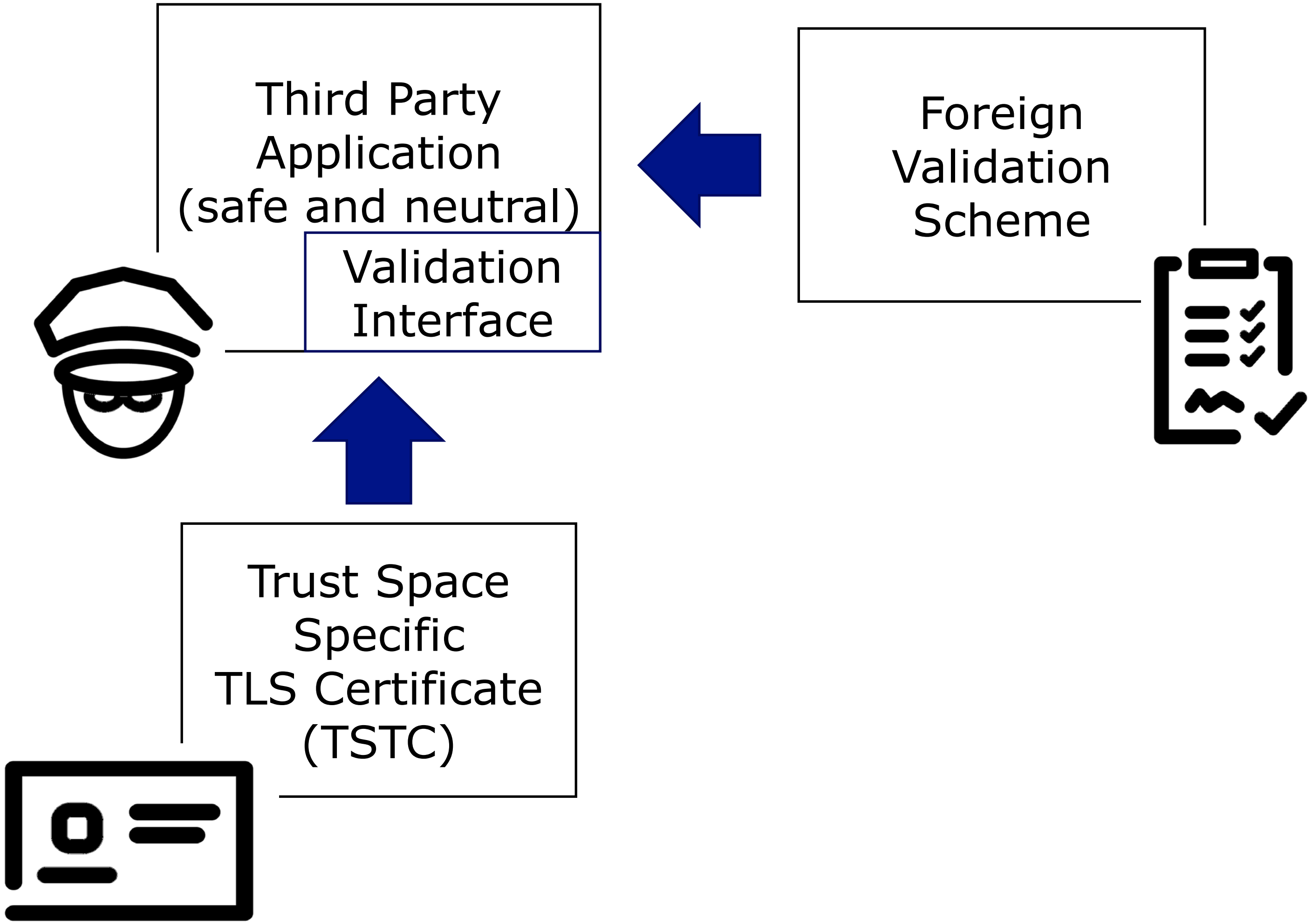
We need a bridge between trust spaces!

In all applications, it must always be visible in which trust space the user is located.

How to build that bridge in real life ...

How do we validate elements of a foreign trust scheme?

What do we have to do to build that bridge?



Third Party Application (safe and neutral)

Validation Interface

Foreign Validation Scheme

Trust Space Specific TLS Certificate (TSTC)

The browser trust space

- Regulation: Root Store Policy, Baseline Requirements, EV-Guidelines
- Technical implementation: Root Store
- Responsibility: Browser
- Monitoring: Qualified auditors and CCADB

The European Digital Single Market

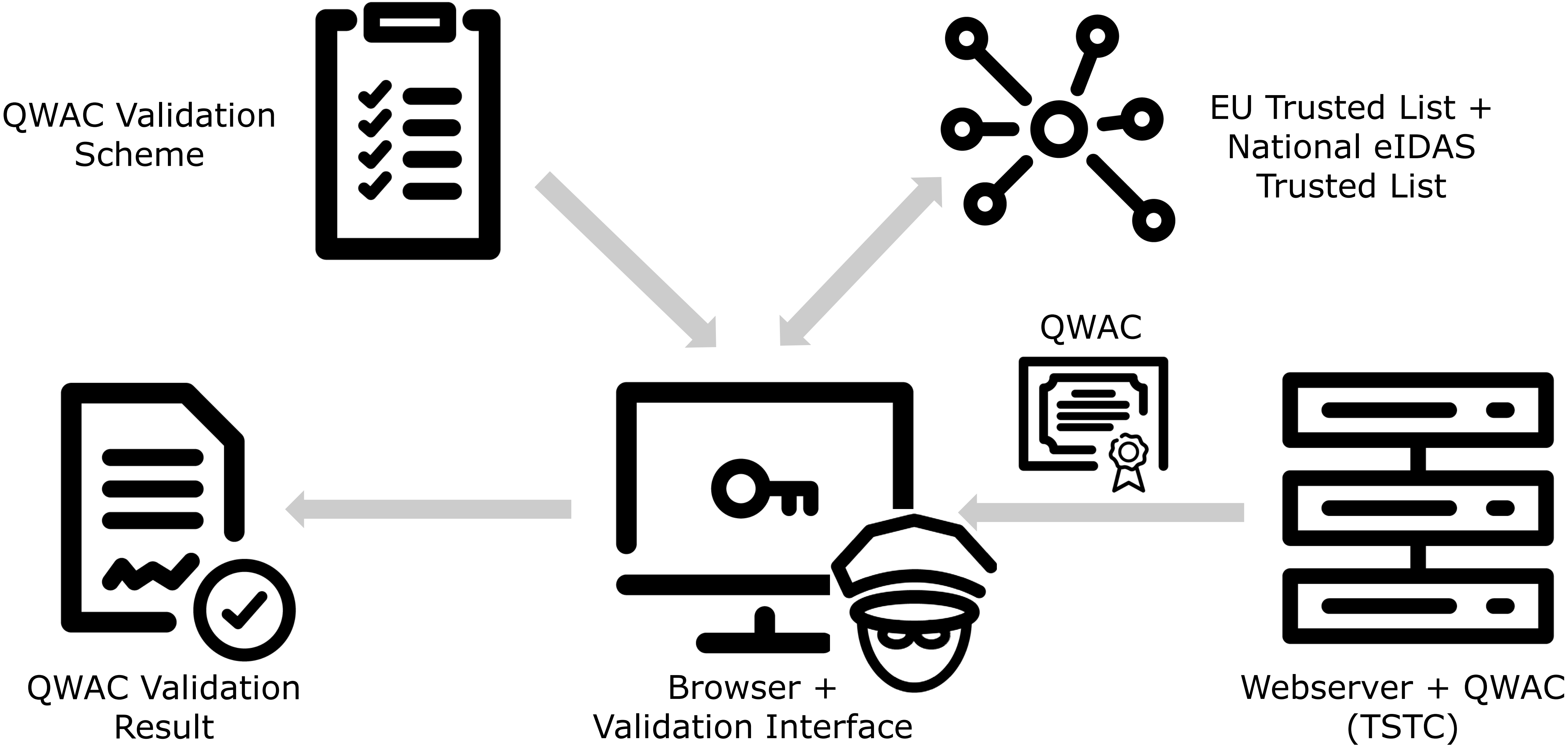
- Regulation: EU regulation eIDAS, referenced implementing acts and technical standards
- Technical implementation: EU Trusted List and national eIDAS Trusted Lists
- Responsibility: EU Commission
- Monitoring: Supervisory Bodies and Conformity Assessment Bodies

Target

- Users and certificate holders can use QWAC in the browser
- Browser is not responsible for QWAC verification results
- Browser runs its own trust space
- EU retains sovereignty over the QWAC

Thus a QWAC can be used in the browser without any risk for both parties. Each party keeps its own responsibility.

Integration of QWAC in the browsers


QWAC Validation Scheme
EU Trusted List + National eIDAS Trusted List
QWAC
QWAC Validation Result
Browser + Validation Interface
Webserver + QWAC (TSTC)

Goals for QWAC

- ✓ Users and certificate holders can use QWAC in the browser
- ✓ Browser is not responsible for QWAC verification results
- ✓ Browser runs its own trust space
- ✓ EU retains sovereignty over the QWAC

✓ **Thus a QWAC can be used in the browser without any risk for both parties.**

Take away

- The concept could solve the Gordian knot problem with browsers and the usage of QWAC.
- The concept is not limited to TLS but can also be used for other certificate types and applications other than browsers.
- The concept allows applications to integrate trust spaces without being held responsible for them.
- This gives applications a high degree of flexibility and extends their range of use.

We need an open validation interface for applications because …

Using trust spaces should be as easy as traveling by car.

… there will always be different trust spaces in the world and there is always a need for applications to be able to use standardized trust spaces.

Enrico Entschew
E-Mail: e.entschew@d-trust.net or enrico.entschew@bdr.de
Telefon: +49 (30) 2598-3070

Thank you!

Hinweis: Diese Präsentation ist Eigentum der D-TRUST GmbH.
Sämtliche Inhalte – auch auszugsweise – dürfen nicht ohne die Genehmigung der D-TRUST GmbH vervielfältigt, weitergegeben oder veröffentlicht werden.

TÜV
TRUST IT
TÜV AUSTRIA Group

TRUST SERVICE AUDITING

ENISA CA- DAY 2020

ARTIFICIAL INTELLIGENCE BASED USER IDENTIFICATION UNDER EIDAS

Clemens Wanko - TÜV TRUST IT / TÜV AUSTRIA CERT

What is the goal, actually?

- a person (subject or user) which was properly identified?
- the issuance of a certificate?
- the issuance of a qualified certificate?
- to sign a document?

Yes, yes, yes, yes..!

But…

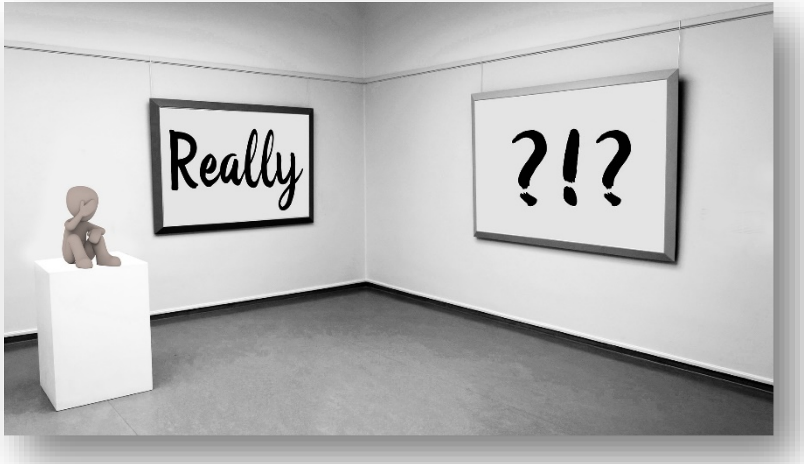


Illustration PixaBay

Biometric subject identification for eIDAS Trust Services

…isn‘t the goal rather the following:

If a person want‘s to express their opinion or wish for something, legally binding, right now…

…they just should be able to do so in an electronic format - right now!

- In the B2B context

  …sign a tender or contract legaly binding right now.

- In the B2C context

  …buy your car and finance it right now from your sofa at home.

- In the B2A context

  …hand in your business related declarations without company representatives showing up, no appointments, no waiting.

Illustration PixaBay

So, what is the demand actually in all areas of relationships B2B, B2C, B2A?

A fully integrated

electronic process

taking you to your goal of having a specific opinion or wish expressed and

legally binding documented

right now!

Illustration PixaBay

Biometric subject identification for eIDAS Trust Services

What do we need to reach the goal?

…at best including

- a validation protocol,
- being shipped using electronic registered delivery services and
- preserved over time making use of a preservation service.

Process:

- **input:**
  opinion or wish on electronic document
- **output:**
  electronically signed document

All this shall be legally binding.
That‘s why it happens on the eIDAS **qualified level** and it happens **right now!**

That‘s it!

Illustration PixaBay

Subject identification:
a significant part of the solution!

What exactly is required?

Subject remote identification means, which

- can be seamlessly fully integrated
- operate frictionless and
- are available 24x7

at best…

- all year long and with no human intervention required.

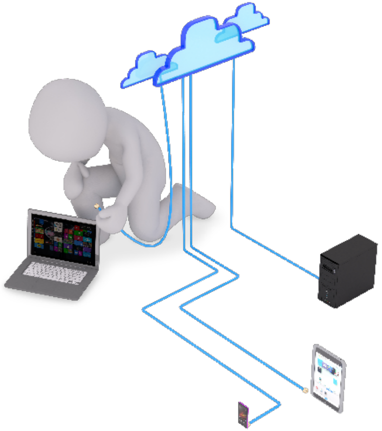


Illustration PixaBay

Biometric subject identification for eIDAS Trust Services

What does the eIDAS regulation regard to be sufficient for remote identification?

- Art 24 1 (b)
  making use of eID means based upon a physical identification at LoA substancial or high as set out in eIDAS Art 8

- Art 24 1 (d)
  making use of a process *using other identification methods […] which provide* ***equivalent assurance in terms of reliability to physical presence.*** *The equivalent assurance shall be confirmed by a conformity assessment body.*

Illustration PixaBay

Biometric subject identification:
a significant part of the solution!

…or just another big problem?

- Art 24 1 (d)
  methods which provide equivalent assurance
  in terms of reliability to physical presence

Illustration PixaBay

Biometric subject identification for eIDAS Trust Services

Illustration PixaBay

How do we evaluate biometric ident processes for their equivalence, if

- there are no further legal criteria provided by eIDAS?
- there are no normative guidelines available mapping to eIDAS?

(Available Standards like ISO/IEC 30107-3:2017 on “Biometric presentation attack detection” need to be regarded as “uncomplete” today as they don’t cover state of the art attack scenarios anymore.)

How can equivalence be evaluated?

Approach:

Evaluation of biometric security **relative** to the typical F2F process through

- step by step comparison of security elements along the identification process between typical F2F and biometric process steps and
- consideration of specific bio approach inherent weaknesses

Identification process core:

- ID document validation
- Face matching & liveness detection (AI / biometrics / deep learning algorithms)
- Attack prevention measures
- Supporting security elements along process flow

plus examination of

- algorithm development and management,
- attack research, detection and loop back and
- general process management and operations.

Cross sectional measures over time and general management

Illustration PixaBay

Biometric subject identification for eIDAS Trust Services

Adopted algorithm parametrization

FAR, FRR, EER/CER **(false acceptance rate, false rejection rate, equal error rate/cross over error rate)**

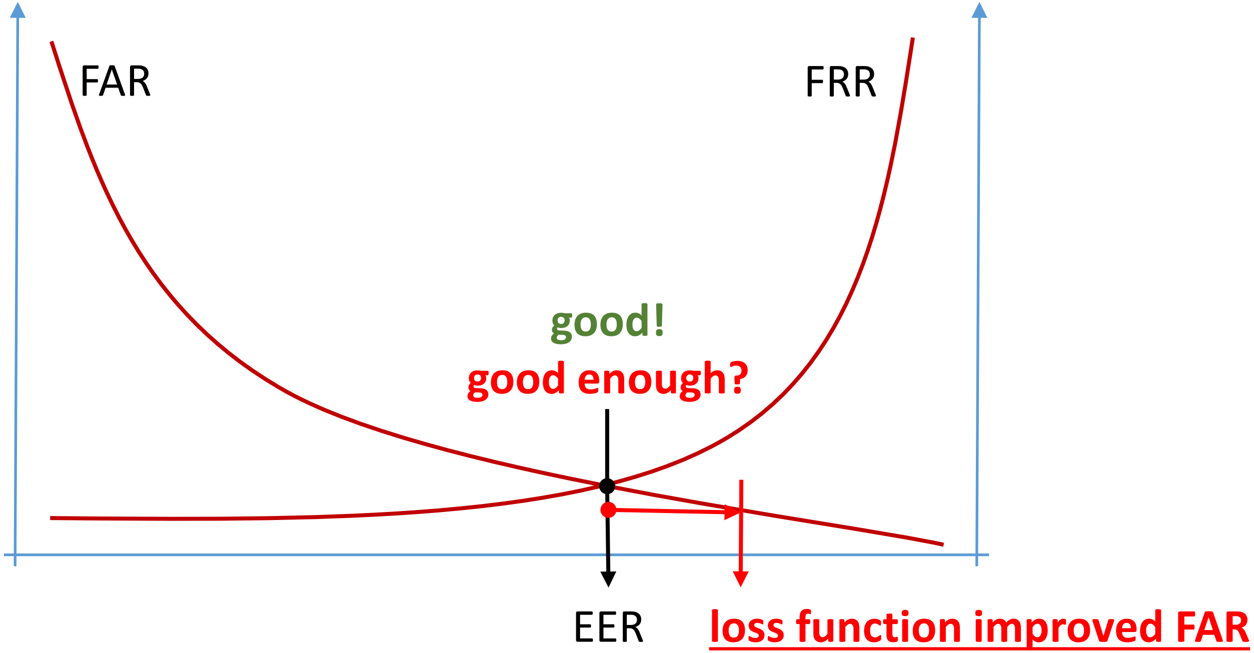


Illustration PixaBay

Crucial for overall security:

Cross sectional measures over time!

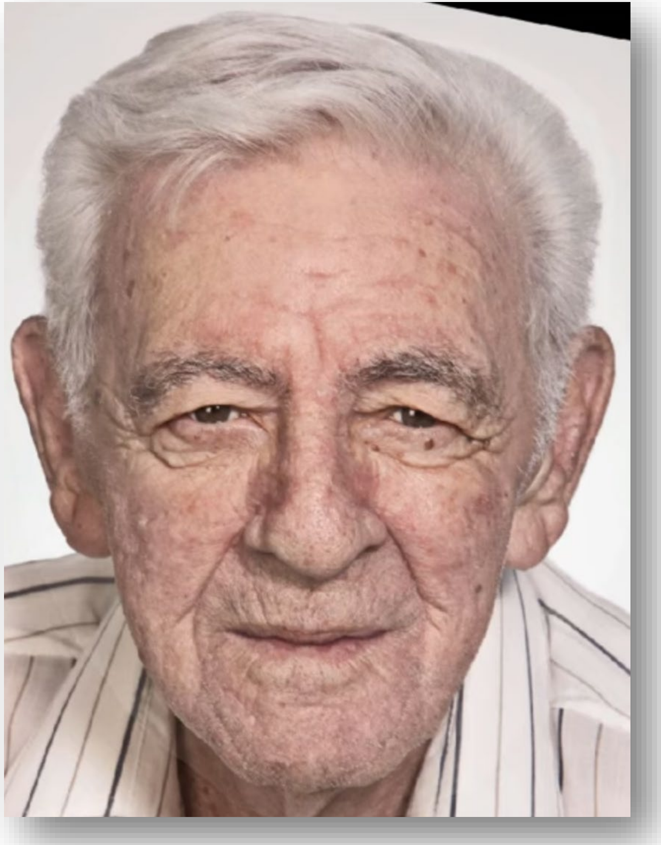
Active attack resistance monitoring and evaluation

- algorithm quality control and management
- attack research and review
  - known attack fields
  - upcoming new attacks (research)
  - spoof bounty programs
  - etc.

Deep fake puppets from photos or videos
a matter of seconds:
See deepfake tutorials on youtube.com
Tools are available: DeepFaceLab, Reallusions Character Creator,…

Illustration PixaBay

Biometric subject identification for eIDAS Trust Services



Deep fake puppets:

Mike Sharewood/ 3Dtest

https://www.youtube.com/watch?v=tnviGWO0wbU

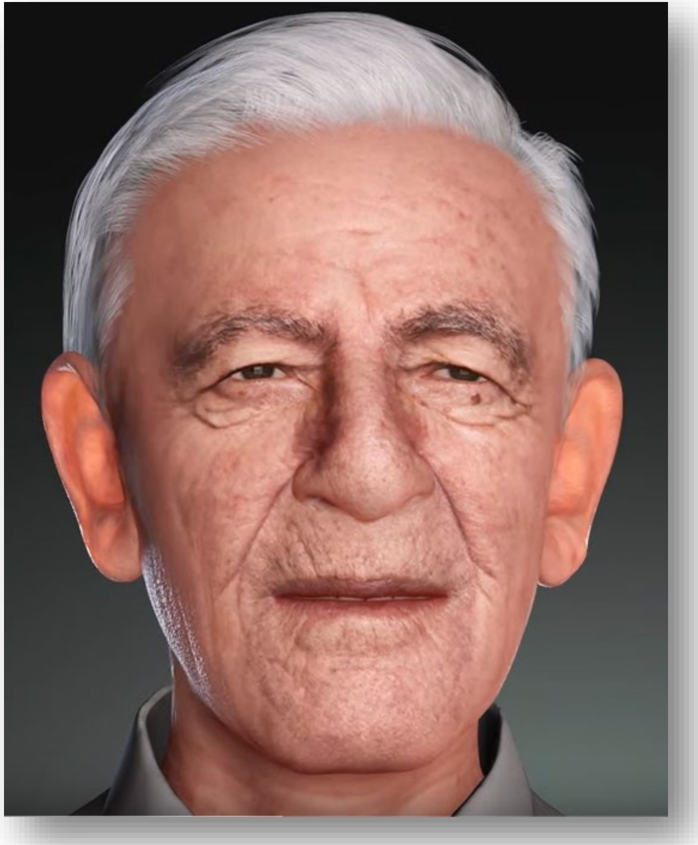


Illustration PixaBay

Biometric subject identification for eIDAS Trust Services

Biometrics demonstrated solid equivalent assurance, finally!

- step by step comparison showed: biometric process was significantly ahead F2F

provided and (only) as long as

- proper process and biometric algorithm quality control and management over time is guaranteed!

New biometric approaches for subject identification are possible!

eIDAS conformance can be attested!

Bio process specific
security management must be guaranteed!

Illustration PixaBay

Accredited Conformity Assessment Body

eIDAS eID schemes and Trust Services

TÜV TRUST IT
TÜV AUSTRIA Group

Clemens Wanko

TÜV TRUST IT
Waltherstr. 49-51
51069 Köln

Phone +49 170 80 20 20 7
clemens.wanko@tuv-austria.com

www.it-tuv.com

HARICA

CAB CA/BROWSER FORUM

CA/Browser Forum

Status and future activities

Dimitris Zacharopoulos

CA/Browser Forum Chair

What is the CA/Browser Forum?

- Global “Standards Defining Organization (SDO)” but not an incorporated entity
- Competing Organizations get together to agree on mutual policies/practices for the provisioning/issuance/governance of Publicly-Trusted SSL/TLS, Code Signing,…. Certificates
- Produces “Guidelines” which are incorporated into:
  - WebTrust for CAs Standards by WebTrust Task Force
  - ETSI Standards by ESI
  - … other Standards/national policies
- Guidelines are licensed under Creative Commons Attribution 4.0

Sampling of CA/B Forum members

48 CAs, 8 Browsers

kpn
izenpe
digicert
WebTrust
GlobalSign
ICANN
ETSI
HARICA
network solutions
buypass
digidentity
D-TRUST
SKAITMENINIO SERTIFIKAVIMO CENTRAS
E-tugra
KEYNECTIS
SECTIGO
TURKTRUST
中華電信
Chunghwa Telecom
Let's Encrypt
kamu SM
SecureTrust
Entrust
Go Daddy.com
swisscom
QuoVadis
Certum

Current Governance

- CA/B Forum Plenary → https://cabforum.org/
    - Server Certificate Working Group
        - Validation Subcommittee
        - Network Security Subcommittee
    - Code Signing Certificate Working Group
    - S/MIME Certificate Working Group
- Each WG has some level of independence (via charter)
- More Working Groups can be created depending on Industry interest

Expectations to comply with Guidelines

- CA/B Forum Maintenance Guidelines are voted and become effective usually 30 days after initial vote
- WebTrust and ETSI take more time to update their respective standards
- Certificate Consumers expect Certificate Issuers to **comply to the latest Guidelines <u>when they become effective</u>!**
- Some Maintenance Guidelines contain **<u>fixed</u> effective dates!**

Latest News in Server Certificate WG

- Update Domain Validation Methods
  - SC25: Define New HTTP Domain Validation Methods v2 (2020-03-03)
  - SC27: Version 3 Onion Certificates (2020-03-27)
  - SC33 - TLS Using ALPN Method (to be published)
- Other topics
  - SC23: Precertificates (2019-12-19)
  - SC24: Fall cleanup v2 (2019-12-19)
  - SC26 - Pandoc-Friendly Markdown Formatting Changes (2020-05-04)
  - SC28 - Logging and Log Retention (in IPR Review Period)
  - SC29 - Configuration Management (2020-06-08)
  - SC30 - Disclosure of Registration/Incorporating Agency (2020-08-20)
  - SC31 - Browser Alignment (2020-08-20)
  - SC35 - Cleanups and Clarifications (in IPR Review Period)
- Ballots under consideration
  - NCSSRs Zones
  - SC34 - Account Management
  - Minimum expectations regarding weak keys
  - Security Requirements for Air-Gapped CA Systems

Latest News in Code Signing WG

- “Baseline Requirements for Code-Signing Certificate” v2.0 (2020-09-02)
  - Combines EV Guidelines for Code-Signing
- Convert to RFC 3647 structure
- EV vs. Non-EV items will be reviewed
- **Move deadline for transition of RSA-3072 to end of Q2 2021**
- Discussions about how to handle “high-risk” certificates

Latest News in S/MIME Certificate WG

- Collecting various existing international/national standards (ETSI, RFC 5280, government documents) related to S/MIME Certificates
- Define a basic Certificate Profile
- Describe major use cases and solicit feedback from other WGs and/or the public
- Individual S/MIME certs versus those used on gateways

Other resources

- Meeting minutes (including F2F) https://cabforum.org/category/minutes/
- Mailing-list archives
  - 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/
    - NetSec Subcommittee public list https://cabforum.org/pipermail/netsec/
  - Code Signing Certificate WG public list https://cabforum.org/pipermail/cscwg-public/
  - S/MIME Certificate WG public list https://lists.cabforum.org/pipermail/smcwg-public/
- How to join the CA/B Forum
  - https://cabforum.org/information-for-potential-members/

HARICA

CA/BROWSER FORUM

Thank you

Dimitris Zacharopoulos

dzacharo@harica.gr

CA Day 2020

Audits used by Mozilla’s CA Program

Ben Wilson, Mozilla

Overview

- Why does Mozilla run a root program?
- Auditor Qualifications
- Audit Attestation Content and Format Requirements
- Delivering Audit Statements and Delays
- Mozilla Audit Processing Flow
- Audit Full Key Lifecycle
- Other Important Developments

https://wiki.mozilla.org/CA/Audit_Statements#ETSI_Audits

Why does Mozilla review audits, auditors, and audit statements?

Principle 4: Individuals' security and privacy on the internet are fundamental and must not be treated as optional.

- To keep our users safe.
- Partnership with auditors to ensure that TSPs are performing required tasks.
- https://wiki.mozilla.org/CA/Audit_Statements: To ensure that TSPs are "operating securely and in compliance with our policies."
- Auditors are not equally qualified and the quality of their work varies.
- Who do we trust? Who can we rely on? Is our reliance reasonable?

Auditor Qualifications

https://wiki.mozilla.org/CA/Audit_Statements#Standard_Check

- The NAB must be a full EA member listed here: https://european-accreditation.org/ea-members/directory-of-ea-members-and-mla-signatories/
- The CAB’s accreditation documentation must be issued by that NAB and be hosted on the NAB's website
- The CAB's accreditation documentation must explicitly refer to at least:
  - ETSI EN 319 403 as the relevant standard for the CAB to perform ETSI audits, allocated under ISO/IEC 17065 as the framing standard
  - ETSI EN 319 401 and ETSI EN 319 411-1, as standards to audit publicly trusted Trust Service Providers

Audit Attestation Basic Contents (1 of 2)

Scope: Name and SHA256 of every CA certificate in scope of audit Based on the technical capability of the CA - trust bit, EKUs, and policy OIDs (not based on TSP intent)

Enforcement is based on certificate content and audit statements

Identify:

- Trust Service Provider / CA Operator
- Conformity Assessment Body (including principal assessor), and
- National Accreditation Body (*including URL to NAB site with PDF showing Accreditation of CAB by NAB*)

Audit Attestation Basic Contents (2 of 2)

Dates:

- One-year Period of Operation Covered by Audit (continuous consecutive audits needed) with a Start Date and an End Date
- Date of Statement Issuance (must be within 90 days of audit period End Date)

Standards, Criteria, and Policies (incl. versions):

- ETSI EN 319-411-1 v.1.2.2 (LCP and (DVCP or OVCP)) or (NCP and EVCP)

  EVCP must be clearly stated (not just QCP-w)
- CABF Baseline Requirements v.1.7.1
- Applicable CPs/CPSes

Bugzilla Incidents, Findings, Qualifications, and Non-Conformities

Formatting the Audit Attestation for Audit Letter Validation (ALV)

- Selectable text
- SHA2 HASH of all Certificates in scope of the audit: formatted with all Uppercase letters, No colons, spaces, or line feeds
- Date Formats (in English):

  Month DD, YYYY example: May 7, 2016

  DD Month YYYY example: 7 May 2016

  YYYY-MM-DD example: 2016-05-07

  (No extra text within the date, such as “7th” or “the”)

https://www.ccadb.org/policy#51-audit-statement-content

Delivering the Audit Attestation Letter (AAL)

- AAL dated/issued within 90 days of end of the Audit Period
- AAL downloadable from an accredited CAB’s Website (used for ALV)

A Bugzilla attachment can be used (1) for testing ALV (see Test Preliminary Audit Statements) or (2), according to Section 5.1 of the CCADB Policy:

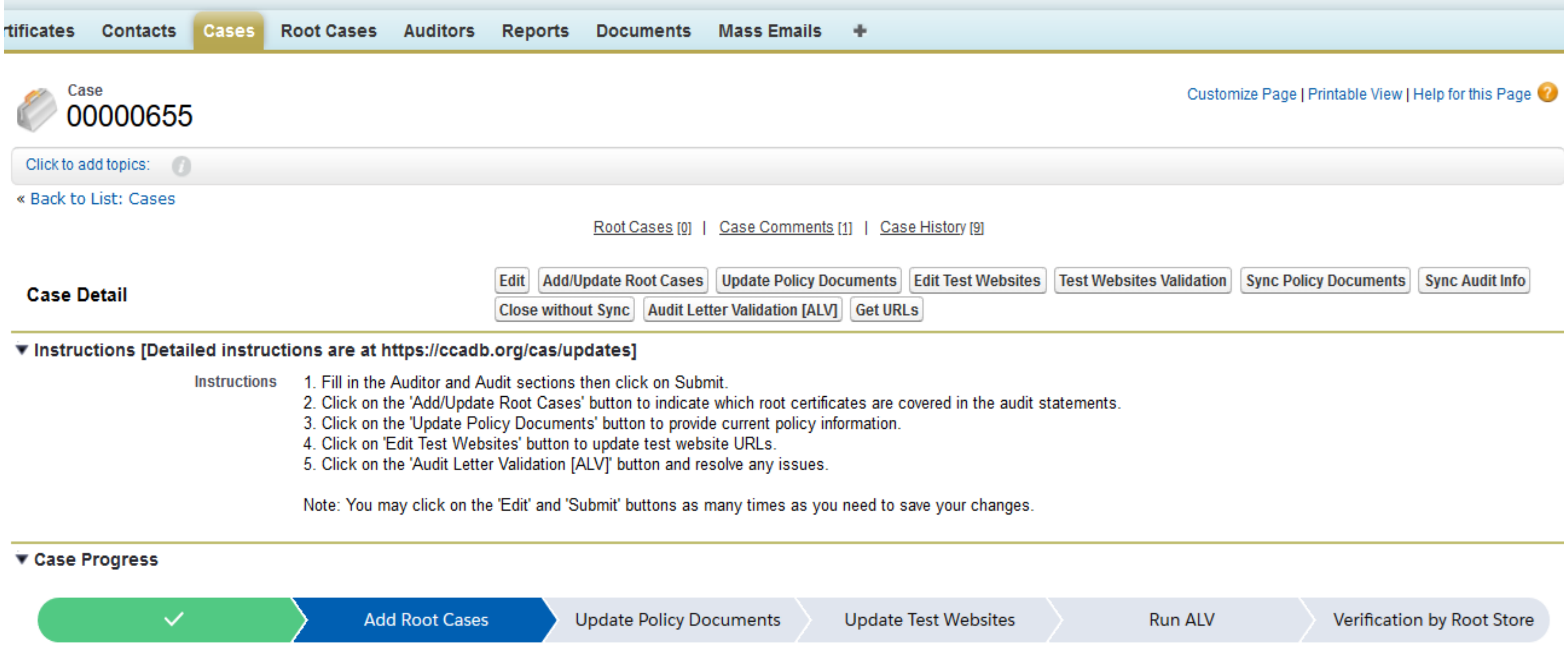
“When an ETSI Certificate cannot be issued, the CA must still provide an AAL such that there are no gaps between audit periods for consecutive audits. The CA may post the AAL on their own website or attach the attestation report to a Bugzilla Bug and provide that URL. Additionally, the CA needs to provide an explanation about the problems and time frame for resolution of the problems.”

Audit Delay due to COVID19/other reasons

- An Audit Delay is when one or more of the following requirements cannot be met:
  - "Full-surveillance period-of-time audits MUST be conducted and updated audit information provided no less frequently than annually."
  - "... MUST be provided to Mozilla via the CCADB within three months of the point-in-time date or the end date of the period."

- As soon as the TSP realizes that the audit will be delayed, a Bugzilla bug must be filed. https://wiki.mozilla.org/CA/Audit_Statements#Audit_Delay The TSP is expected to provide status updates in Bugzilla. The TSP should work with its assessor to provide a publicly available audit attestation detailing the procedures that were or were not yet performed.

Creating an Audit Case in the CCADB



Case
00000655

Case Detail

▼ Instructions [Detailed instructions are at https://ccadb.org/cas/updates]

Instructions

1. Fill in the Auditor and Audit sections then click on Submit.
2. Click on the 'Add/Update Root Cases' button to indicate which root certificates are covered in the audit statements.
3. Click on the 'Update Policy Documents' button to provide current policy information.
4. Click on 'Edit Test Websites' button to update test website URLs.
5. Click on the 'Audit Letter Validation [ALV]' button and resolve any issues.

Note: You may click on the 'Edit' and 'Submit' buttons as many times as you need to save your changes.

▼ Case Progress

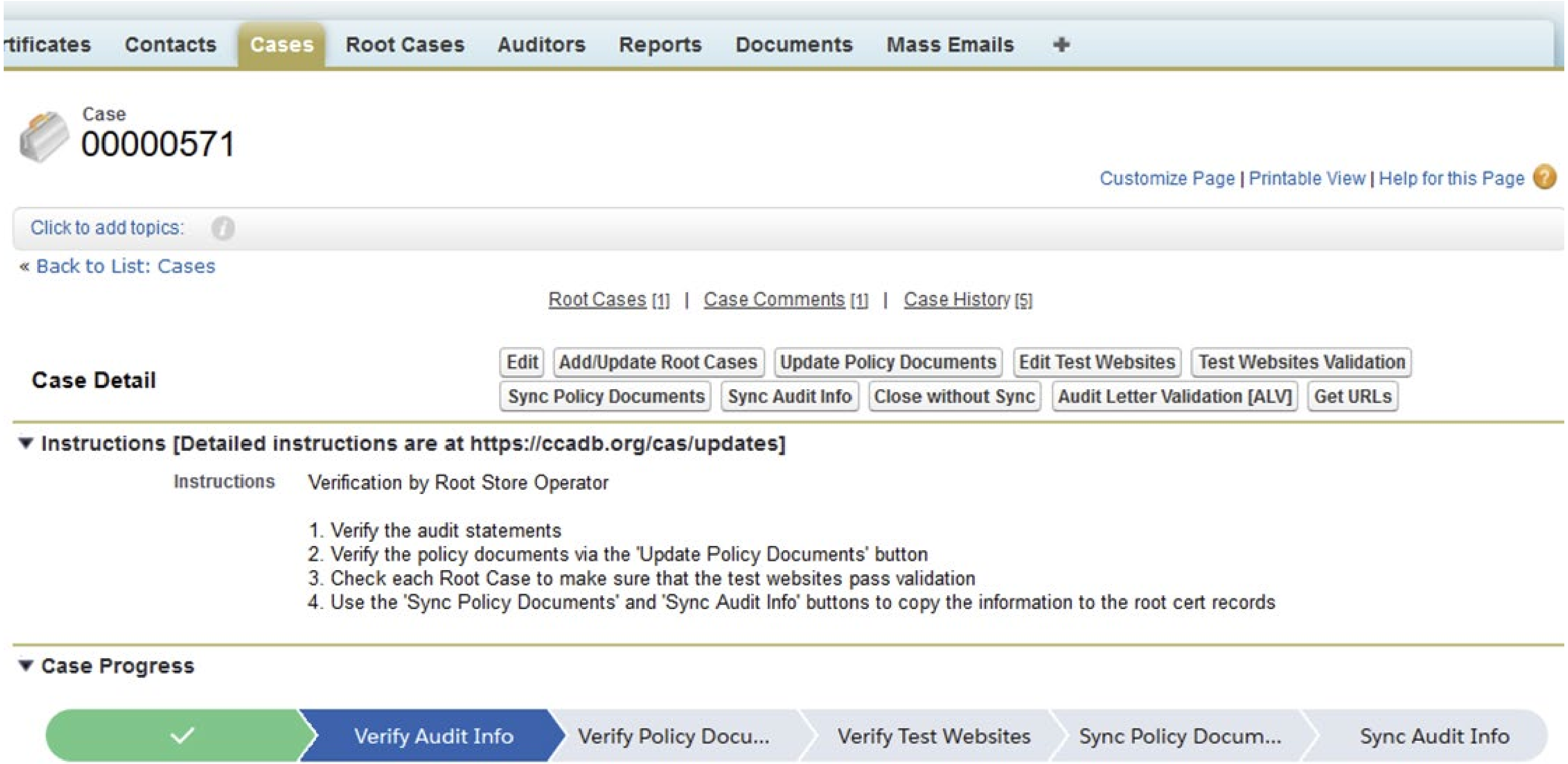
Instructions & Video: https://www.ccadb.org/cas/updates#instructions

ALV Errors

Error(s)	Recommended Actions
[StandardAudit] Auditor is not found in the Audit Letter	Ensure the correct Auditor is selected in the CCADB record and that it matches the auditor name recorded in your standard audit statement.
[StandardAudit] Audit letter not found in certified location.	Audit letter will be manually reviewed. Audit letter should be hosted by an approved certifying authority.
[StandardAudit] StartDate and EndDate missing in request and system is unable to extract suitable audit period from letter.	Please ensure that your audit statement clearly specifies the Audit Period Start and End dates. Validate the Audit Period dates in the CCADB record.
[StandardAudit] Validation of StatementDate '05/06/2020' skipped due to the failure of validating Audit Period.	Auditor must provide an audit statement that clearly specifies the Audit Period Start and End dates. If the dates are correct in the audit letter, please update the dates in the CCADB record to match the dates in the letter.

https://wiki.mozilla.org/CA/Audit_Statements#Common_ALV_Findings

Steps Taken by Mozilla



Case

00000571

Case Detail

▼ **Instructions [Detailed instructions are at https://ccadb.org/cas/updates]**

Instructions: Verification by Root Store Operator

1. Verify the audit statements
2. Verify the policy documents via the 'Update Policy Documents' button
3. Check each Root Case to make sure that the test websites pass validation
4. Use the 'Sync Policy Documents' and 'Sync Audit Info' buttons to copy the information to the root cert records

▼ **Case Progress**

Audit Full Key Lifecycle - Cradle-to-Grave

- Some TSPs pre-generate keys in batches and “park” them for later use.
- Other TSPs claim that the CA is “no longer issuing any certificates”
- Issues 139, 153 and 173 in the Mozilla Policy’s GitHub Repository
- Root and Subordinate CA Key Pairs and Certificates audited continuously from Key Pair Generation until the Root CA is no longer in the Mozilla Root Store.
- Continuous: period-of-time audits must be sequential, contiguous audit periods--each not exceeding one year in duration, for the full lifetime of all CA private keys--from generation to destruction.
- Key Generation audit reports and Key Destruction audit reports

Other Matters

- Clarify that EV audit scope must include all certificates ***capable*** of issuing EV certificates

- Github Issue 187: Require audit reports to list all incidents that occurred during the audit period (or clearly state that the auditor is unaware of any)

- Github Issue 203: Require information about auditor qualifications in the audit report (in addition to current section 8.2 of Baseline Requirements)

  (**Require Curriculum Vitae for Auditors who Conduct Audit**)

- Github Issue 207: Audit statements should provide information about which CA Locations were and were not audited, and the extent to which they were (or were not) audited

Thank You!

Ben Wilson

bwilson@mozilla.com

The Standards People

Identity Proofing for Trust Service Subjects

CA DAY 2020

23/09/2020

Presented by: **Sylvie Lacroix - ETSI/ESI STF 588**

STF 588 - rationales

- The current European standards published by ETSI on trust services specify identity proofing only by generic requirements like “physical presence” or “means which provide equivalent assurance as physical presence”.
  - Physical presence as a benchmark is not well-defined as no requirements are posed neither for the quality of physical identity documents nor for the competence or procedures to be carried out by the person performing the check.
  - What constitutes equivalent assurance as physical presence is up to subjective judgement.
  - Guidelines for remote identity proofing are needed to avoid cumbersome and expensive physical presence procedures when possible.
- These initial rationales becomes even more pertinent under the options to review the eIDAS Regulation

STF 588 deliverables

- Detail on team & project on web page: https://portal.etsi.org/STF/STFs/STF-HomePages/STF588

- **ETSI TR 119 460 Electronic Signature and Infrastructures (ESI); Survey of technologies and regulatory requirements for identity proofing for trust service subjects. (18/12/2020)**

This document will survey the technologies, legislations, specifications, guidelines and standards related to or used for identity proofing. Information will then be gathered from stakeholders such as national agencies developing requirements, product and service vendors, research and academic environments, and relevant existing specifications.

- ETSI TS 119 461 Electronic Signatures and Infrastructures (ESI); Policy and security requirements for trust service components providing identity proofing of trust service subjects. (31/07/2021)

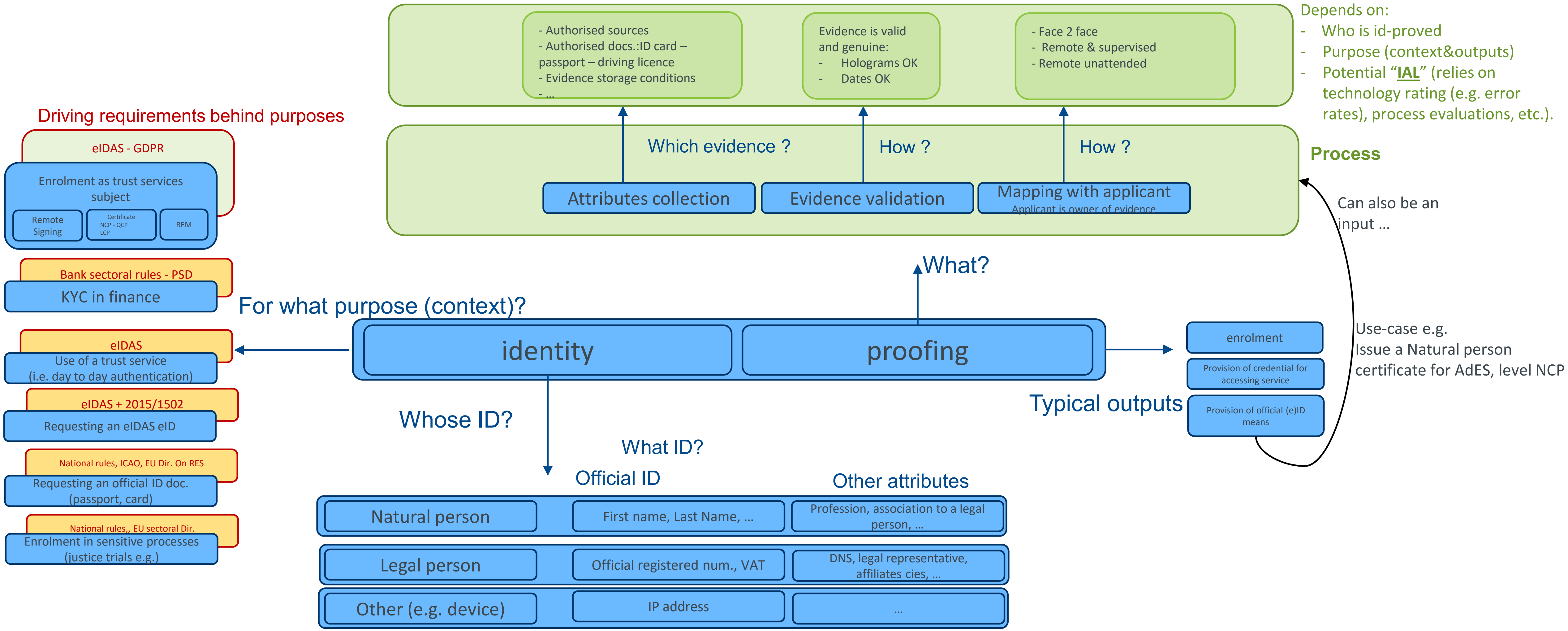
This document specifies policy and security requirements for a trust service component providing identity proofing of trust service subjects. This can be used for conformity assessment of a trust service provider which includes this service component as part of its service or can be used for conformity assessment of a specialized provider of identity proofing supporting other trust service providers. The document specifies best practices for security supporting different technological approaches, and possibly for different assurance levels.

The Technical Specification

- **ETSI TS 119 461 Electronic Signatures and Infrastructures (ESI); Policy and security requirements for trust service components providing identity proofing of trust service subjects. (31/07/2021)**
  - ID proofing is NOT a trust service by itself (up to now), but a trust service component
  - An identity proofing service may be used by many different trust services
    - One audit that can be reused for different purposes -> ETSI EN 319 403-1 auditable
  - Security and policy requirements
    - Based on ETSI EN 319 401 – common requirements for all trust services
    - Specific requirements for identity proofing (relation with EN 319 411-1 / -2 clauses 6.2) - Possibly 2 IALs
    - Specific requirements to support qualified trust services (! does not mean the ID Proofing is a QTS)

- Out of scope:
  - risk assessment (but security requirements are provided to cover risks)
  - technologies rating (but rated technologies are considered for achieving a certain security level)
  - Interface from / toward other component (but considered secure as assumption)

Scope : identity proofing is part of the broader identity management lifecycle



POLICY REQUIREMENTS

Depends on:

- Who is id-proved
- Purpose (context&outputs)
- Potential "**IAL**" (relies on technology rating (e.g. error rates), process evaluations, etc.).

- Authorised sources
- Authorised docs.:ID card – passport – driving licence
- Evidence storage conditions
- …

Evidence is valid and genuine:

- Holograms OK
- Dates OK

- Face 2 face
- Remote & supervised
- Remote unattended

Process

Which evidence ? – Attributes collection

How ? – Evidence validation

How ? – Mapping with applicant (Applicant is owner of evidence)

Can also be an input …

Driving requirements behind purposes

Driving requirements	Purpose
eIDAS - GDPR	Enrolment as trust services subject: Remote Signing; Certificate NCP - QCP LCP; REM
Bank sectoral rules - PSD	KYC in finance
eIDAS	Use of a trust service (i.e. day to day authentication)
eIDAS + 2015/1502	Requesting an eIDAS eID
National rules, ICAO, EU Dir. On RES	Requesting an official ID doc. (passport, card)
National rules,, EU sectoral Dir.	Enrolment in sensitive processes (justice trials e.g.)

For what purpose (context)?

identity proofing

What?

Whose ID?

What ID?

	Official ID	Other attributes
Natural person	First name, Last Name, …	Profession, association to a legal person, …
Legal person	Official registered num., VAT	DNS, legal representative, affiliates cies, …
Other (e.g. device)	IP address	…

Typical outputs

- enrolment
- Provision of credential for accessing service
- Provision of official (e)ID means

Use-case e.g.
Issue a Natural person certificate for AdES, level NCP

Information collection

- Initial collection of relevant documents by ESI

(i.e. technologies, legislations, specifications, guidelines and standards related to or used for identity proofing)

- Further eMails to ESI and eSignature News mailing list (i.e. outside ETSI)
- Elements found by STF experts while analysing received info
- Direct contacts with stakeholders – spontaneous inputs
- Questionnaire to TSP and vendors
- eIDAS up-date consultation

Methodology for analyse: Reading Sheets based on ID proofing process components

The reading sheets offers **a common window to look at the information,** to compare heterogenous and numerous information **and derive trends for each component**:

- Short description (purpose, context, type of ID, …)
- Attribute & evidence collection
- Attribute & evidence validation
- Mapping ID attributes with applicant (binding)
- Requirements of the process (incl. security requirements)

This is to be completed and “confronted” with the feedback from the questionnaires to vendors and TSPs.

The conclusions will identify relevant information for the TS.

Attribute and evidence collection

- Identity attributes collected (individuals, legal entities, individuals acting on behalf of legal entities)
- Type of evidence to be / that can be presented:
  - Type of document or evidence (e.g. a passport)
  - Regulatory constraints if any
  - Trusted/authoritative sources for the ID attributes (presentation of eligible issuers or trusted data sources of ID attributes)

  "*determination that the evidence is genuine - issued by recognised independent/authoritative sources*" is addressed in next step.
- Type of presentation of the attributes:
  - Collected as digital representation of an identity document (e.g. scan or photo of identity card or passport)
    - Captured remotely
    - Captured on site
  - Digitally extracted from an ID document (e.g. through (remote) access to the identity document chip)
  - Transmitted in purely digital form as an eID (or SSI);
- Communication channels:
  - In the event of remote collection, e.g.:
    - Protocol and APIs used for the transfer of ID attributes (e.g. SAML or OpenID Connect);
    - Security measures deployed to protect the integrity of the attribute transmission (e.g. end-to-end encryption);
    - ID attributes remotely presented by the applicant or obtained from a third party independent of the applicant (a "trust " service)
  - Constraints to be observed in case of on-site presentation (e.g. on the personnel)

Attribute and evidence validation

- Determination that the evidence is genuine (issued by recognised independent/authoritative sources)

- Determination that the ID attributes are valid (not expired, not revoked)

The following aspects are analysed:

  - Description of customary security checks implemented, and security features verified in relation to attributes collected as digital representation of an ID document;

  - Description of customary security checks implemented in relation to ‘purely digital’ attributes (digitally extracted from ID documents or obtained via an eID or SSI);

  - Description of other checks implemented if any (e.g. matching with other data, verification of expiry date, etc);

  - Description of external (governmental) sources queries if any;

  - Applicable technical standards if any.

Mapping (or binding) with applicant (1)

- Mapping ID attributes with applicant or the attribute binding process can be defined as the steps taken to confirm, with a given degree of confidence, that the claimed identity credentials (for example those shown in a passport or ID card) which have been obtained and confirmed as valid are indeed those of the applicant and not of someone else
- 3 main scenarios are recognised : 'Face-to-face'; 'Supervised remote' and 'Full-remote'

Mapping (or binding) with applicant (2)

- *On premise 'physical presence'* is generally viewed as a benchmark for binding purposes but is rarely specified
  - This generates uncertainty as to the meaning of '*equivalent assurances in terms of reliability to physical presence*' for binding processes performed remotely
- 'Supervised remote' mode implies video interviews and human interactions at both ends but is not universally recognised
- Full-remote binding relies on using one or more knowledge-based, possession-based or inherence-based authentication factors, with the latter required to achieve a high level of assurance (in line with UE 2015/1502)
  - Specifications for Full-remote binding requirements are slowly emerging, and yet to come to achieve a High LoA

Elements common to the process

- How the process is done – best practice
- Possible security levels associated to one step or the whole process
- Process-specific compliance measures, documentation, records management, equipment security, personnel training and competence, attack vectors and protection (e.g. biometrics)
- Base technical standards applied if any
- Other process specific requirements, e.g. auditing
- Security requirements

Analyse work - figures

- 44 documents (or series of documents) analysed in depth through reading sheets
- A couple of documents analysed but considered out of scope
- In-depth responses to questionnaires: 5 from QTSPs and 9 from vendors

Initial results from ETSI questionnaires: TSPs

Note: Analysis of answers still ongoing

- 5 QTSPs provided answers – good input but not statistically significant
- All use physical appearance, video interview, existing eIDs, and existing e-signature
- 2 use NFC reading of ID documents, 1 use optical scanning of ID documents
- Main challenges user friendliness and regulations; then scaling, trust/security, state of standardization
- Standards sought for level of assurance requirements and security and policy requirements (and more)
- Legal person and natural person representing legal person in scope for all
- ISO/IEC 27001 and ETSI standards are used by all (and ISO/IEC 9001)

Initial results from ETSI questionnaires: vendors

Note: Analysis of answers still ongoing

- 9 vendors of identity proofing services or products provided answers – good input on best practices
- Some of these are also (Q)TSPs, most operate also outside of the EU
- 7 use NFC reading of ID documents with biometrics
- Main challenges trust/security, user friendliness and regulations, state of standardization; then scaling
- Standards sought for level of assurance requirements and security and policy requirements (and more)
- Legal person and natural person representing legal person in scope for a few only
- ISO/IEC 27001 and ETSI EN 319 401 are in widespread use

ETSI

The Standards People

HOW TO IMPROVE IDENTITIES IN BROWSERS

CHRIS BAILEY, ENTRUST

CA DAY - 23 SEPTEMBER 2020

ENTRUST

SECURING A WORLD IN MOTION

Executive overview

- What does the eIDAS and GDPR want for QWACs?
- How do we fix browser UI to meet eIDAS, GDPR expectations?

  Add positive and negative indicators:
  - “Straw person” proposal #1 for a new common UI – Positive Indicator
  - “Straw person” proposal #2 for a new common UI – Negative Indicators

WHAT DO eIDAS AND GDPR WANT FOR QWACS?

What does eIDAS want for QWACs?

An authentication mechanism to confirm identity to relying parties:

> *“[The EU shall set]* minimum technical specifications, standards and procedures [for] the reliability and quality of the following elements: *** (c) the authentication mechanism, through which the natural or legal person uses the electronic identification means to confirm its identity to a relying party” Art. 8(3)(c)

eIDAS also has a reference to an eIDAS “EU trust mark” to “differentiate” Qualified certificates from other certificates

GDPR applies too

GDPR Article 5 mandates:

***Article 5* - Principles relating to processing of personal data**

1. Personal data shall be: (a) processed lawfully, fairly and in a transparent manner in relation to the data subject (‘lawfulness, fairness and transparency’);

2. The controller [of a data collecting site] shall be responsible for, and be able to demonstrate compliance with, paragraph 1 (‘accountability’)

Unidentified websites (no identity in certificate) make it hard to confirm GDPR compliance when they collect personal data from browser users.

Solution: QWACs and improved browser UI can help!

What is GDPR transparency?

> “Transparency is fundamentally linked to fairness. Transparent processing is about being clear, open and honest with people from the start **about who you are**, and how and why you use their personal data.
>
> “Transparency is always important, but especially in situations where individuals *have a* ***choice*** *about whether they wish to enter into a relationship with you.”*

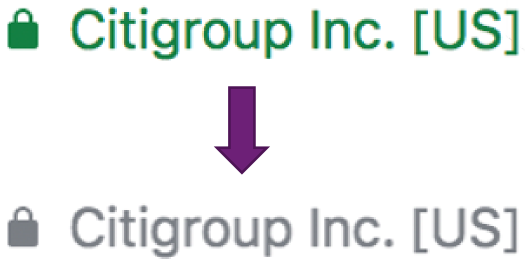
Without identity data about the website, users have no *informed* “choice” on doing business with the site, and no recourse for violations

UK Information Commissioner’s Office “Guide to the GDPR”
https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/principles/

How can users find out if a site has identity information now?

QWAC / EV UI after Chrome 69 (Sep 2018)

– EV UI moved from distinct **Green** to less distinct **Grey** in the Browser URL



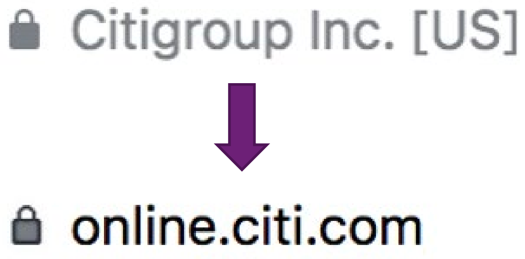
Citigroup Inc. [US]

Citigroup Inc. [US]

QWAC / EV UI after Chrome 77 (Sep 2019)

– EV UI removed.

– Now same as DV - URL only



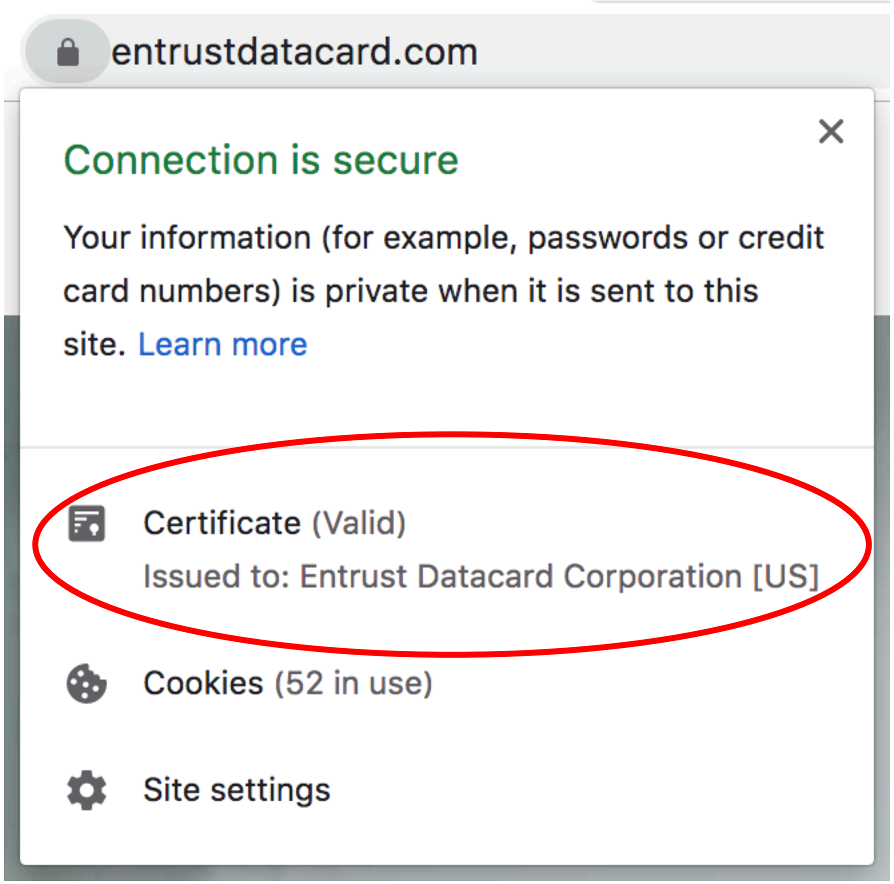
Citigroup Inc. [US]

online.citi.com

Websites identity is available in some browsers, but only if the lock symbol is clicked

Some identity data found only on the ***second*** page after user *clicks the lock symbol*

All browsers need multiple clicks to find full identity data



entrustdatacard.com

Connection is secure

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

Certificate (Valid)
Issued to: Entrust Datacard Corporation [US]

Cookies (52 in use)

Site settings

Browser reasons given for removing EV UI

Why did the browsers remove the EV distinct UI on the home page?

Browser reasons for removing EV UI:

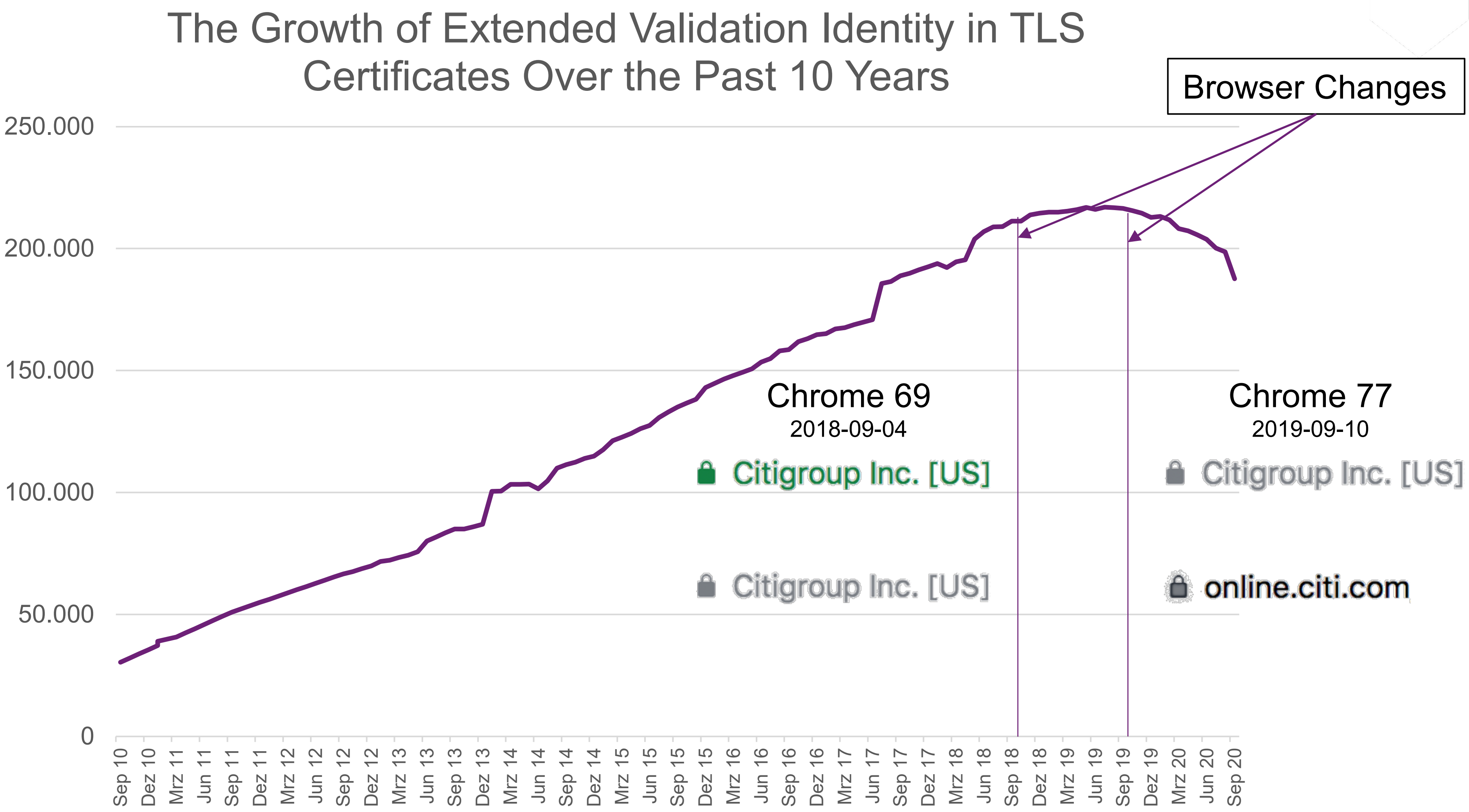
1. Users don't look at or use it
2. Browsers need the space in the URL bar

So EV UI disappeared. Now we are seeing the results…

Without a QWAC / EV UI

1. No QWAC / EV indicator in the URL Bar and no standardized way to display QWAC / EV information in the URL Bar. **All websites (DV, OV, EV, QWAC) look the same**.
2. No intuitive or standard way to look up EV identity data inside certificate
3. Current browser UI does not comply with the spirit of eIDAS and GDPR
4. The number of certificates with identity (QWAC, EV) are rapidly declining since browsers removed special EV UI

Proactive Browser UIs are Critical to Promoting Identity


The Growth of Extended Validation Identity in TLS Certificates Over the Past 10 Years

Browser Changes

Chrome 69
2018-09-04

🔒 Citigroup Inc. [US]

🔒 Citigroup Inc. [US]

Chrome 77
2019-09-10

🔒 Citigroup Inc. [US]

🔒 online.citi.com

Source: Netcraft.com

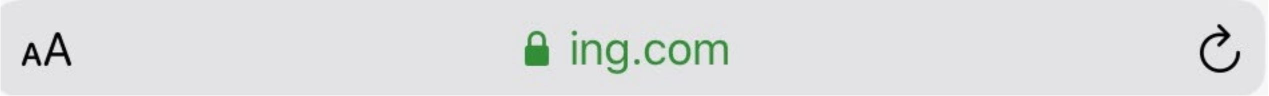
A Potential Solution

How can we address the two browser concerns in a new UI that complies with eIDAS and GDPR?

“STRAW PERSON” PROPOSAL #1 FOR A NEW COMMON UI – POSITIVE INDICATORS

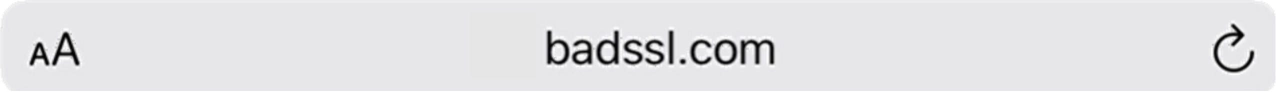
“Straw person” Proposal #1 – three changes to UI

Differentiate QWAC / EV in address bar with lock symbol and **green text**



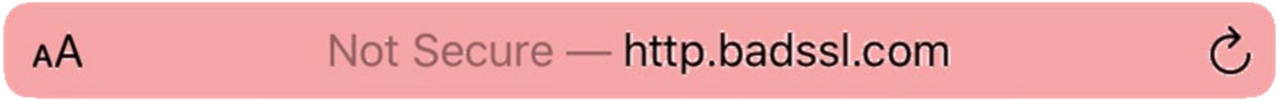
AA 🔒 ing.com

Remove the lock symbol for DV and OV websites, only URL displays



AA badssl.com

HTTP gets **warning**

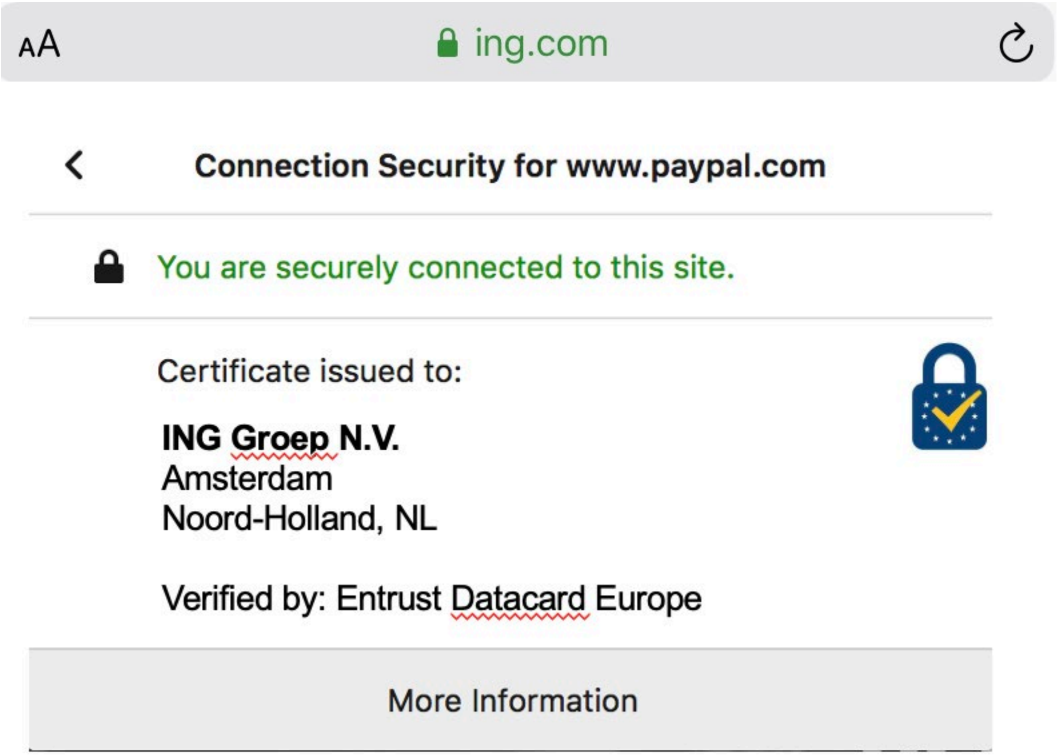


AA Not Secure — http.badssl.com

What happens if the lock symbol is clicked on QWAC / EV address bar?

"Straw person" Proposal #1

1. Single *click* on lock shows identity information in server certificate
2. New, improved presentation of data to user – understandable format
3. Can also show EU Mark, plus "More Information" with click
4. Promote common UI among all browsers to help user education



Connection Security for www.paypal.com

You are securely connected to this site.

Certificate issued to:

ING Groep N.V.
Amsterdam
Noord-Holland, NL

Verified by: Entrust Datacard Europe

More Information

This Straw Person Proposal #1 addresses browser concerns

This new design moves the conversation forward on addressing the two browser concerns.

“Users don’t look at it”

– Shows users on *home page* which sites have *identity*

– Standardizes UI, much easier for users to learn

“Browsers need the space in the URL bar”

– Uses the *same amount of space* in the current URL bar – identity data pops-up only if clicked

Also helps meet spirit of eIDAS, GDPR

“STRAW PERSON” PROPOSAL #2 FOR A NEW COMMON UI – NEGATIVE INDICATORS

Straw Person Proposal #2 – Leverage current warnings

Google research says users don't often use positive UI indicators to make security decisions but are affected by negative UI warnings.

Google used this research in its successful plan[1] to transition websites from *http* to *https*, employing a progressive combination of positive ("**Secure**") and negative ("**Not Secure**") indicators.

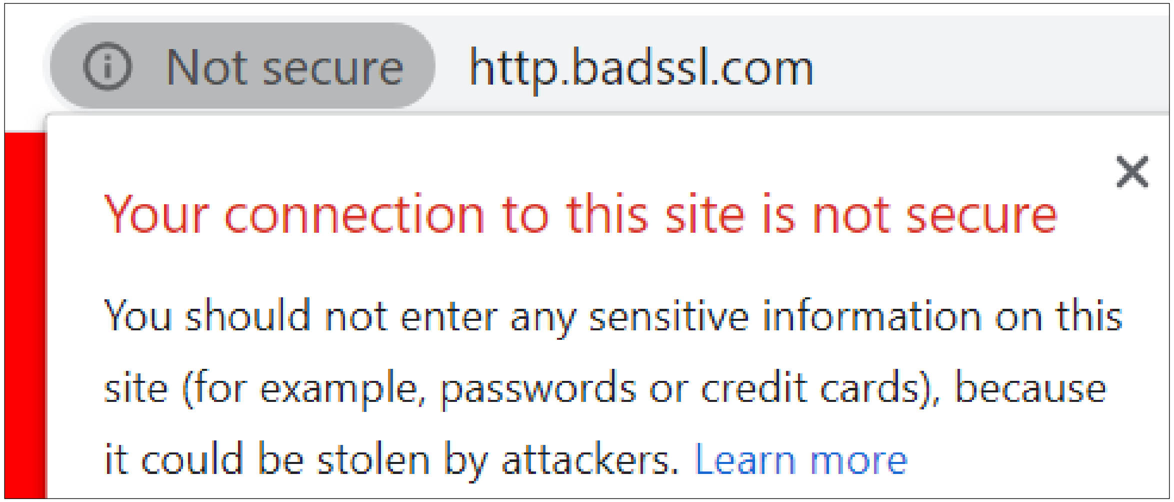
Past UI changes influenced both website owners (the positive indicators) and users (the negative warnings).

How can we learn from Google and leverage this experience?

[1] https://www.usenix.org/conference/usenixsecurity19/presentation/Thompson
https://www.chromium.org/Home/chromium-security/marking-http-as-non-secure
https://blog.chromium.org/2018/05/evolving-chromes-security-indicators.html

Leverage browser warnings for unencrypted sites

Leverage Google’s http (non-TLS) page warning pop-up message *for unidentified websites that have user data input field*

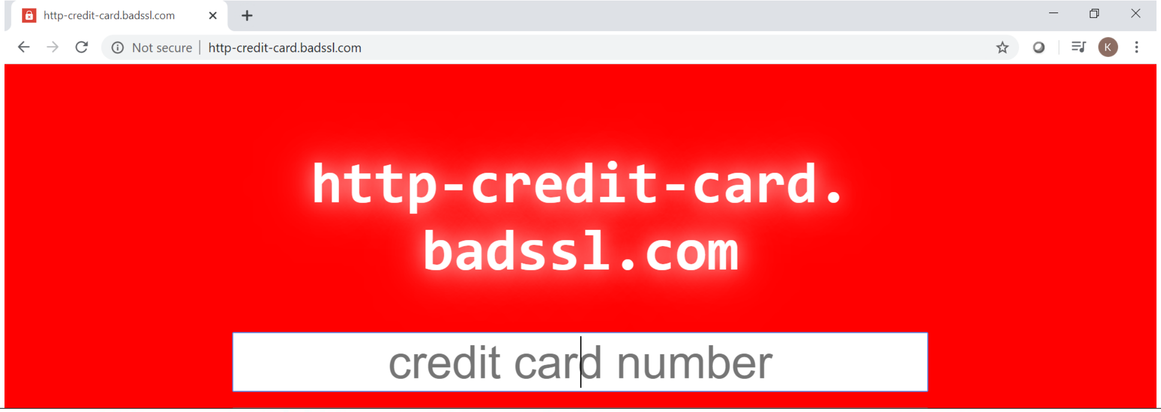


Your connection to this site is not secure

You should not enter any sensitive information on this site (for example, passwords or credit cards), because it could be stolen by attackers. Learn more

Leverage existing browser warning for user data fields

Leverage Google’s http (non-TLS) page warning pop-up message *when user attempts to enter data into a user input field*



http-credit-card.badssl.com

Not secure | http-credit-card.badssl.com

http-credit-card.badssl.com

credit card number

Automatic credit card filling is disabled because this form does not use a secure connection.

What about certificates with hundreds of SANs?

- A QWAC / EV identity certificate should only be used to represent the website owner’s content
- *Problem*: But some hosting providers / CDNs include hundreds of unrelated SANs in a certificate that contains the hosting provider’s identity, not the website owner’s identity.
- *Solution*: We should prohibit aggregating multiple SANs in a single QWAC / EV certificate that do match the certificate’s organization information and the website owner’s identity

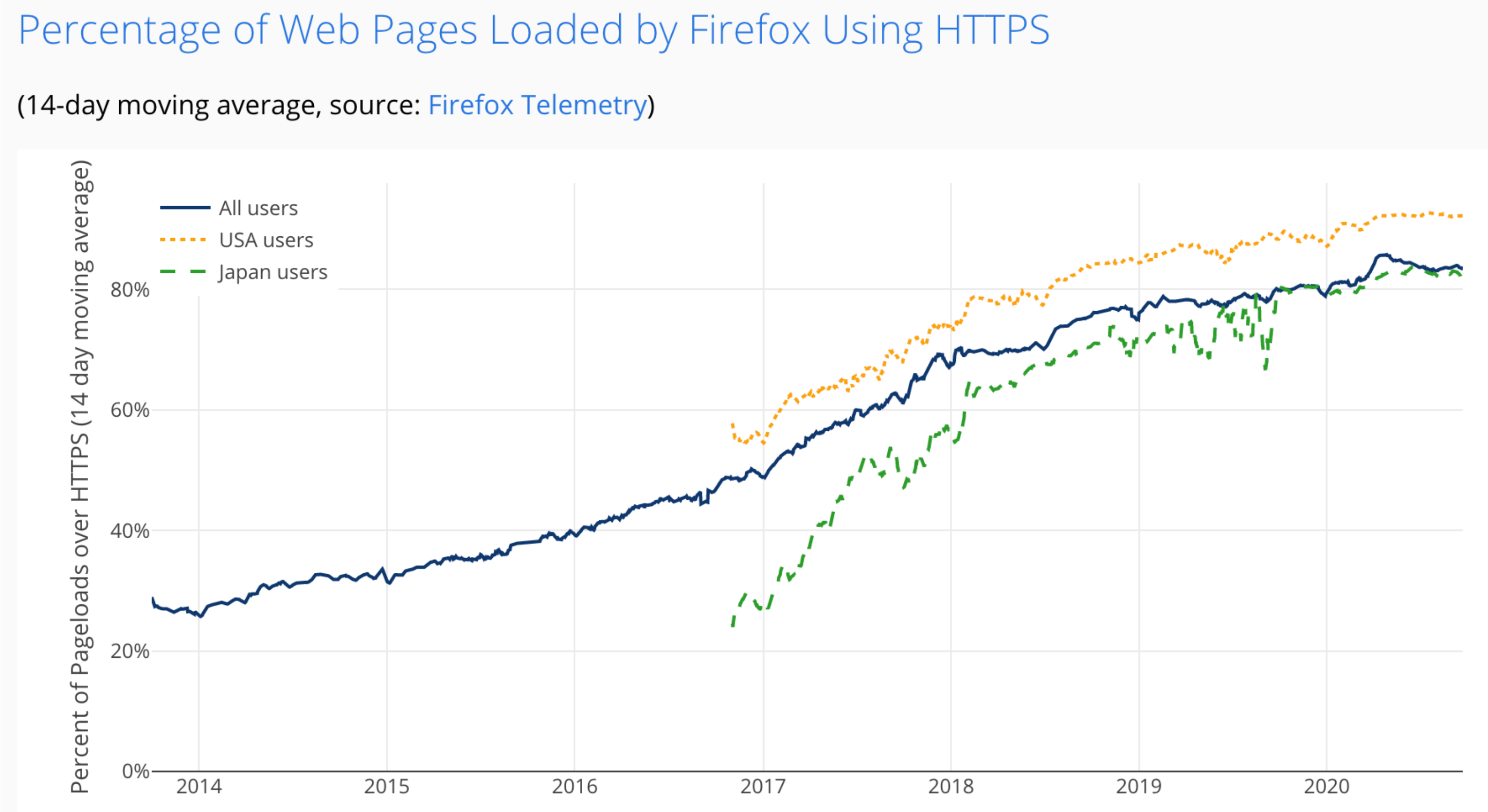
Summary of Straw Person Proposals #1 and #2

- Positive address bar UI for *QWAC / EV* websites - display **green lock symbol with Green DN / FQDN**
- Additional Identity information if lock symbol clicked
- Negative pop-ups if unidentified websites ask for personal information

- Impose positive UI immediately, negative UI gradually, over time

Past success with progressive warnings

Progressive warnings, positive indicators in the browsers moved the internet from 30% to 80% encryption over 6 years



Percentage of Web Pages Loaded by Firefox Using HTTPS

(14-day moving average, source: Firefox Telemetry)

https://letsencrypt.org/stats/

THANK YOU!
COMMENTS / QUESTIONS?

Chris Bailey

VP Trust Services

Entrust

chris.bailey@entrust.com

+1.678.595.7999