TÜV
TRUST IT
TÜV AUSTRIA Group

TRUST SERVICE AUDITING

THE ART OF SIMULTANEOUSLY FOLLOWING MULTIPLE STANDARDS

Clemens Wanko - TÜV TRUST IT / TUV AUSTRIA CERT

STATUS QUO

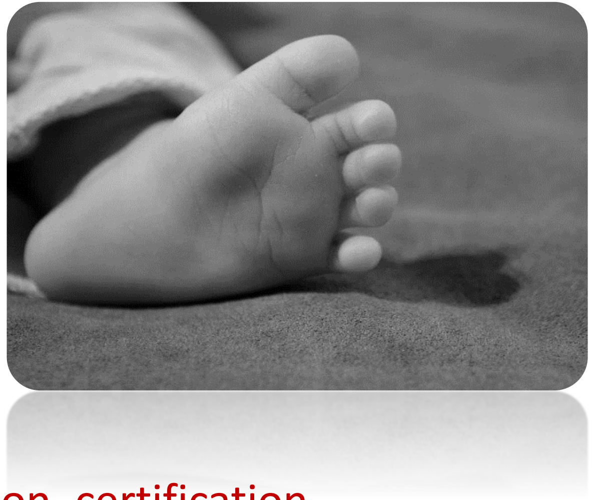
- Legal, technical, organizational rule sets

SITUATION FACING

- Challange of simoultaneously managing multiple standards

TSP SPECIFIC SOLUTION

- Get your bearings and find your way out



eIDAS started in 2016/17

By that time, we didn‘t have much…

- eIDAS legal requirements

…implementing acts?

- ETSI EN 319 401 V2.1.1 (2016-02)
- ETSI EN 319 411-1 V1.1.1 (2016-02)
- ETSI EN 319 411-2 V2.1.1 (2016-02)
- ETSI EN 319 421 V1.1.1 (2016-03)

Accreditation, certification, audit schemes?

based upon ETSI TS 102 042, ETSI TS 101 456 and ETSI TS 102 023 covering issuance of public key certificates qualified certificates and time stamps

Today we have improved…

Commission Implementing Decision (EU)
on Trust Services

- 2015/806
  EU Trust Mark for Qualified Trust Services
- 2015/1505
  Technical specifications and formats relating to trusted lists
- 2015/1506
  Specifications relating to formats of advanced electronic signatures and advanced seals to be recognised by public sector bodies
- 2016/650
  Standards for the security assessment of qualified signature and seal creation devices

…and we have…

A national legal implementation supporting eIDAS in several EU memberstates!

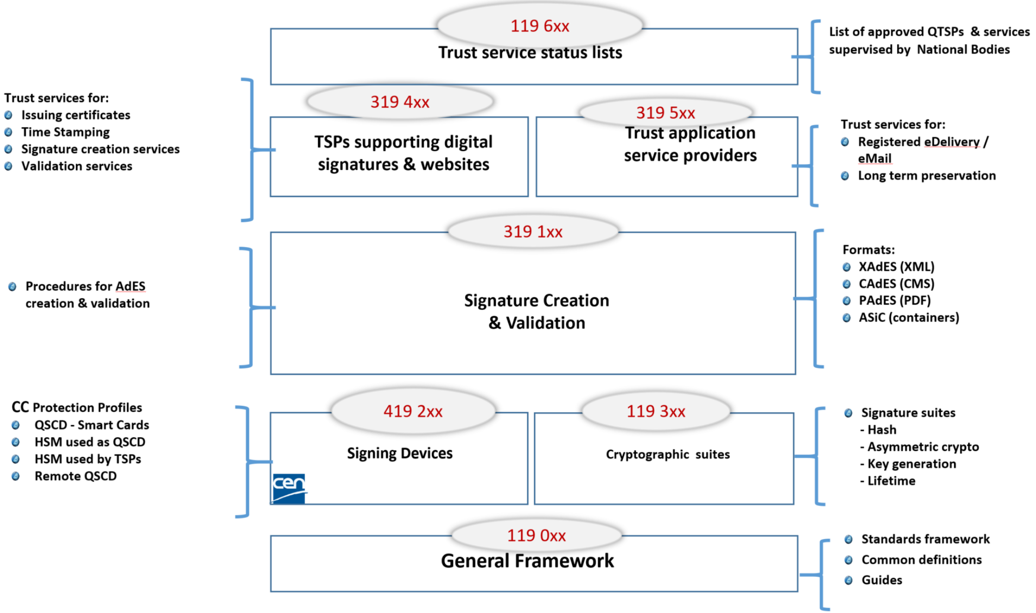
e.g. Germany:

- Vertrauensdienstegesetz
- Verordnung zum Vertrauensdienstegesetz

…we have supporting ETSI / CEN Standards for Trust Services in almost all areas…

- **TSL**
- **TSP supporting digital signatures & websites**
  (Issuing certificates, Time Stamping, Signature creation services, Validation services)
- **Trust application service provider**
  (Trust services for: Registered eDelivery/eMail, Long term preservation)
- **Signature Creation & Validation**
  (Procedures & Formats)
- **Signing devices**
  (CC protection profiles)
- **Cryptographic suites**
  (Signature suites)
- **General Framework**

…we have supporting ETSI/ CEN Standards for Trust Service in almost all areas …



119 6xx
Trust service status lists

List of approved QTSPs & services supervised by National Bodies

Trust services for:
- Issuing certificates
- Time Stamping
- Signature creation services
- Validation services

319 4xx
TSPs supporting digital signatures & websites

319 5xx
Trust application service providers

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

319 1xx
Signature Creation & Validation

- Procedures for AdES creation & validation

Formats:
- XAdES (XML)
- CAdES (CMS)
- PAdES (PDF)
- ASiC (containers)

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

419 2xx
Signing Devices

119 3xx
Cryptographic suites

- Signature suites
  - Hash
  - Asymmetric crypto
  - Key generation
  - Lifetime

119 0xx
General Framework

- Standards framework
- Common definitions
- Guides

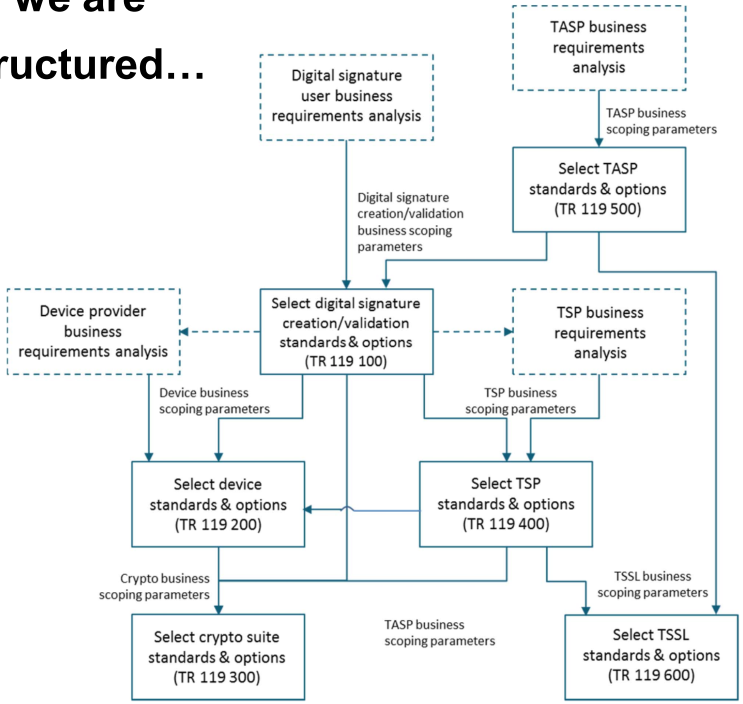
Trust Service Auditing

The art of auditing multiple standards

…and hey, we are

well structured…

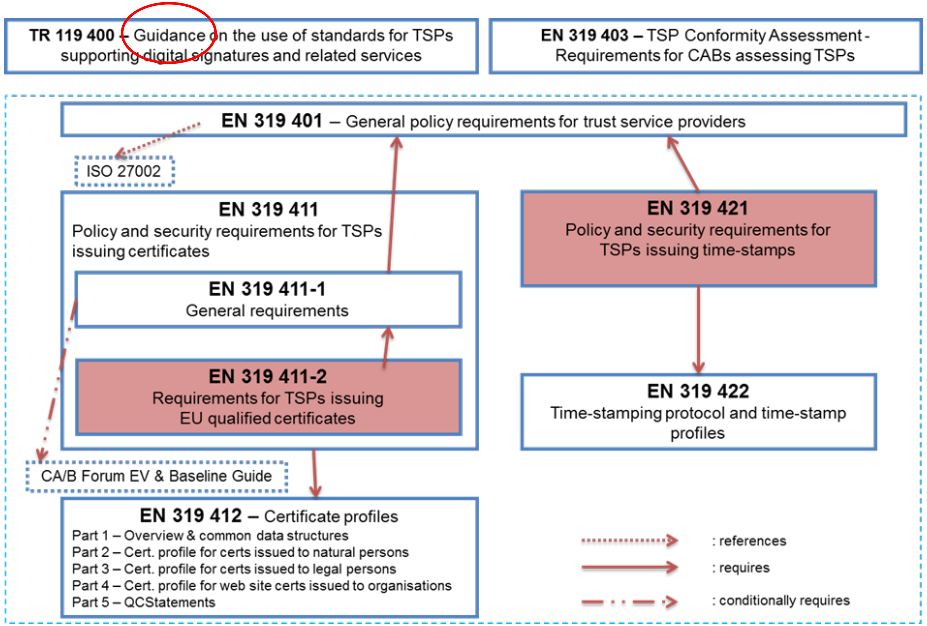
14 ETSI TR 119 000 V1.2.1 (2016-04)



TASP business requirements analysis
Digital signature user business requirements analysis
TASP business scoping parameters
Select TASP standards & options (TR 119 500)
Digital signature creation/validation business scoping parameters
Device provider business requirements analysis
Select digital signature creation/validation standards & options (TR 119 100)
TSP business requirements analysis
Device business scoping parameters
TSP business scoping parameters
Select device standards & options (TR 119 200)
Select TSP standards & options (TR 119 400)
Crypto business scoping parameters
TSSL business scoping parameters
TASP business scoping parameters
Select crypto suite standards & options (TR 119 300)
Select TSSL standards & options (TR 119 600)

Figure 3: Dependencies of the business scoping parameters among the functional areas

…and luckily enough, we do have support and crystal clear guidance!



TR 119 400 – Guidance on the use of standards for TSPs supporting digital signatures and related services

EN 319 403 – TSP Conformity Assessment - Requirements for CABs assessing TSPs

EN 319 401 – General policy requirements for trust service providers

ISO 27002

EN 319 411
Policy and security requirements for TSPs issuing certificates

EN 319 411-1
General requirements

EN 319 411-2
Requirements for TSPs issuing EU qualified certificates

EN 319 421
Policy and security requirements for TSPs issuing time-stamps

EN 319 422
Time-stamping protocol and time-stamp profiles

CA/B Forum EV & Baseline Guide

EN 319 412 – Certificate profiles
Part 1 – Overview & common data structures
Part 2 – Cert. profile for certs issued to natural persons
Part 3 – Cert. profile for certs issued to legal persons
Part 4 – Cert. profile for web site certs issued to organisations
Part 5 – QCStatements

: references
: requires
: conditionally requires

But hold on…

that‘s only been the
eIDAS / ETSI / CEN requirements part!

There is more to come!

Other TSP related requirements…

- **CA/Browser Forum Requirements**
  (Baseline Requirements, EV Guidelines, Network security requirements)
- **Browser Root Store Programs**

AICPA (American Institute of Certified Public Accountants)

- **WebTrust**
  (if not replaced by ETSI EN 319 411)
- **SOC2**
  (Service Organization Control – SOC
  Security, Availability, Processes, Integrity, Confidentility, Secrecy, Data protection)
  - Type 1 (design)
  - Type 2 (design and effectiveness)

Trust Service Auditing

The art of auditing multiple standards

…and toppings up to your individual flavour:

- **ISO 27001**
  Information Security Management Systems
- **GDPR**
  General Data Protection Regulation requirements
- **ISO 14001**
  Environmental Management Systems
- **ISO 50001**
  Energy Management Systems
- …

Let‘s stop considering standards then…
…let‘s talk about their implementation:

Audit schemes focusing at

- full scale past-present-future (eIDAS/ETSI)
- past period (public accountants)

Audit frequency, requiring

- yearly full audit (CA/B Forum)
- bi-yearly audit (eIDAS/ETSI)
- three-yearly audit (ISO27xxx)

+ supervision

Certificate maintenance

- scheme to be agreed between CAB and TSP (ETSI EN 319 403)
- none, others

LOST
FOUND

No universal solution!

TSP approach to overcome the confusion:

Make sure you know…

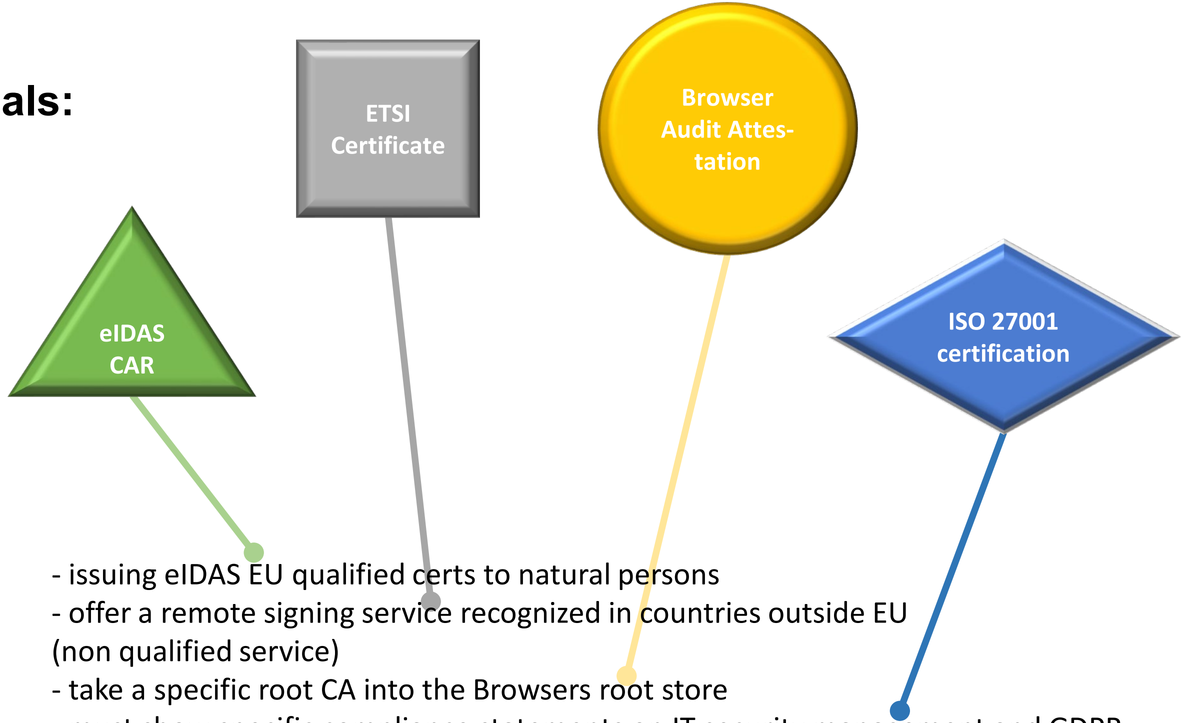
- **where you are today**

  - experienced EU based PKI operator
  - issuing non qualified electronic certificates for natural persons

- **your goals**

  - issuing eIDAS EU qualified certs to natural persons
  - offer a remote signing service recognized in countries outside EU
  (non qualified service)
  - take a specific root CA into the Browsers root store
  - must show specific compliance statements on IT security management and GDPR

Transfer into focussed goals:



- **your goals**

- issuing eIDAS EU qualified certs to natural persons
- offer a remote signing service recognized in countries outside EU (non qualified service)
- take a specific root CA into the Browsers root store
- must show specific compliance statements on IT security management and GDPR

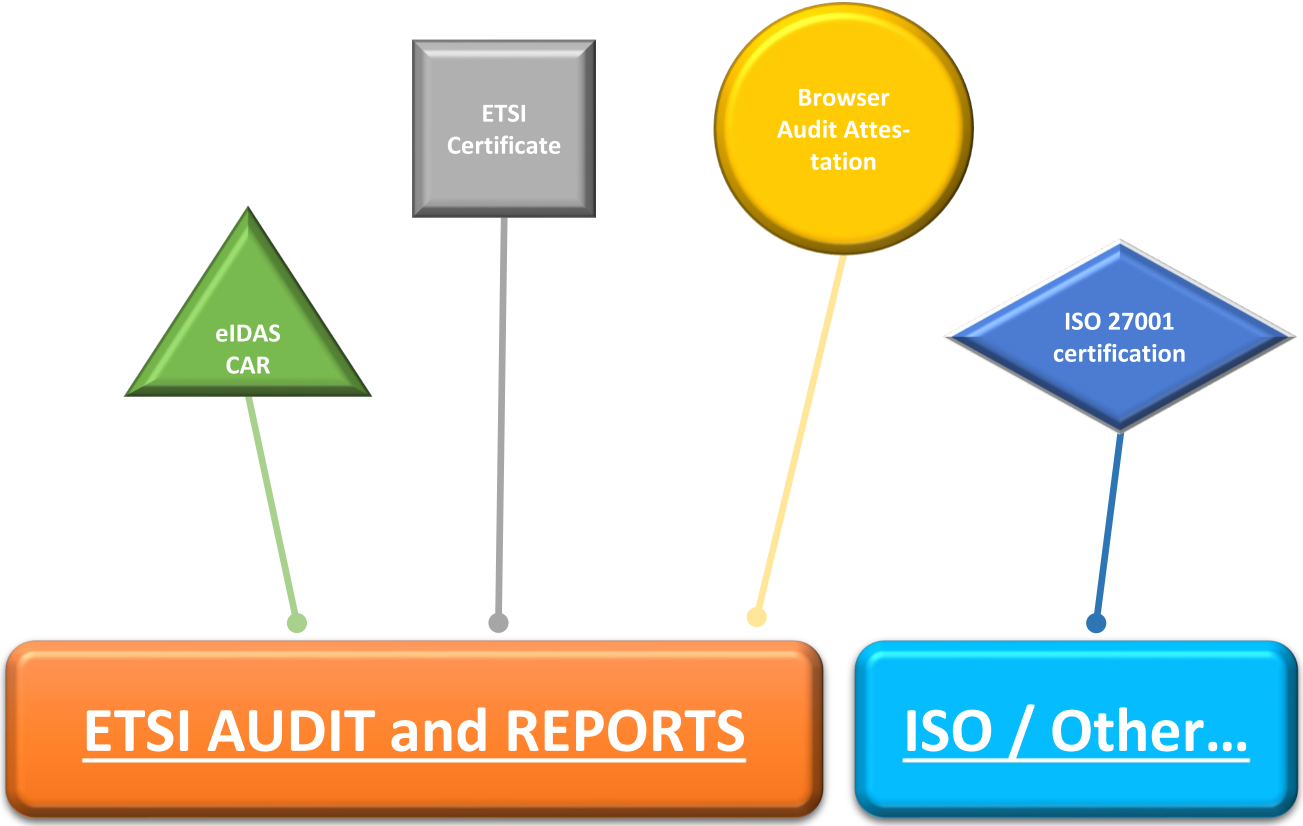
Trust Service Auditing

The art of auditing multiple standards

Focussed goals:

- Use case

- Audit base



Ask for joint & integrated auditing

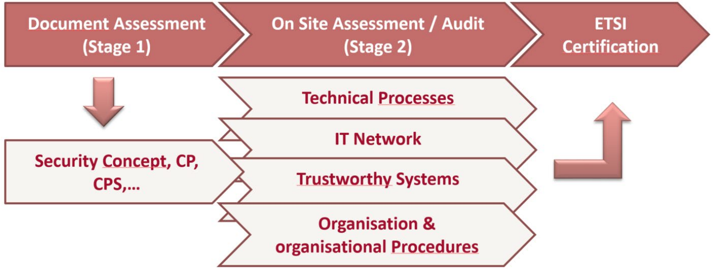
Makes perfectly sense for

- all standards with overlapping requirements

Even a synchronization of

- schemes
- audit frequency
- maintenance

is possible!


Document Assessment (Stage 1)
On Site Assessment / Audit (Stage 2)
ETSI Certification
Security Concept, CP, CPS,…
Technical Processes
IT Network
Trustworthy Systems
Organisation & organisational Procedures

- **Audit base**

ETSI AUDIT and REPORTS

ISO / Other…

Goal:

save time for your staff members to work on the real stuff!

Definition of „real stuff“ is up to U! ☺

Use the support of your Conformity Assessment Body for that.

We shall be happy to assist you!

Accredited Conformity Assessment Body

for Trust Service Provider under eIDAS

TÜV TRUST IT
TÜV AUSTRIA Group

Clemens Wanko

TÜV TRUST IT
Waltherstr. 49-51
51069 Köln

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

www.it-tuv.com