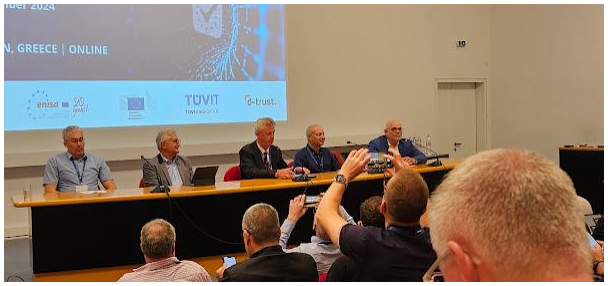
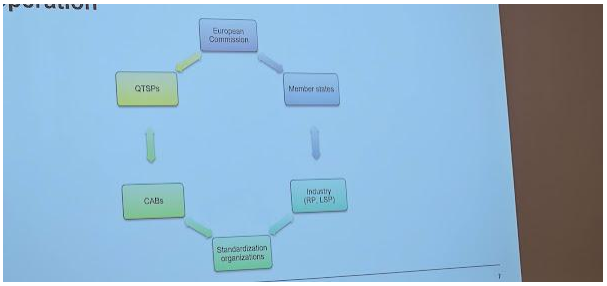
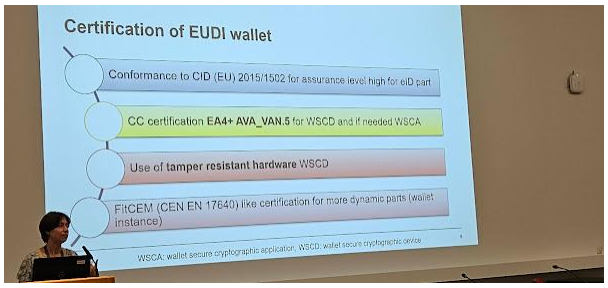
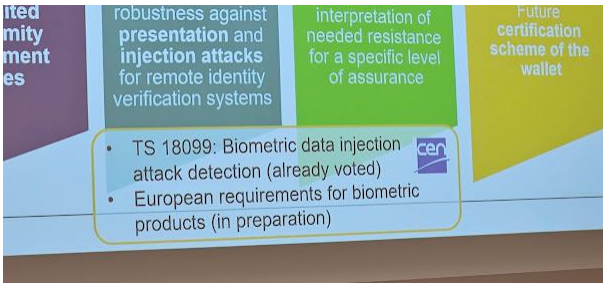
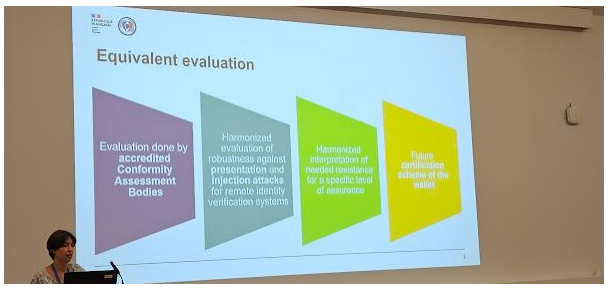

N, GREECE | ONLINE
enisa
TÜVIT
d-trust.

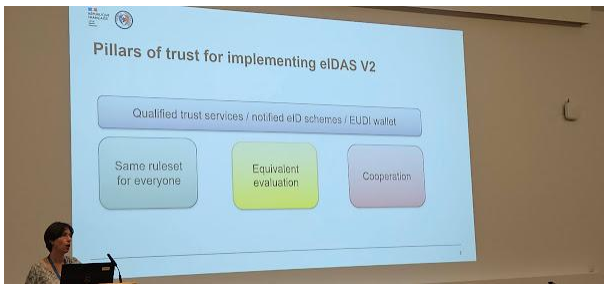

European Commission
QTSPs
Member states
CABs
Industry (WP, LSP)
Standardization organizations

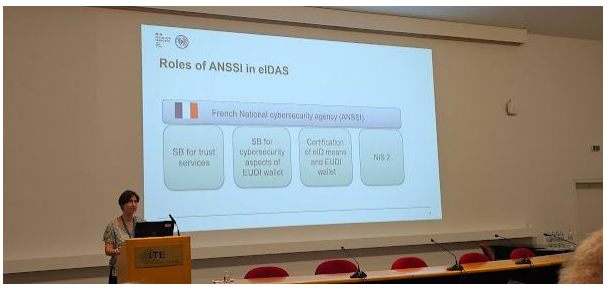

Certification of EUDI wallet
Conformance to CID (EU) 2015/1502 for assurance level high for eID part
CC certification EA4+ AVA_VAN.5 for WSCD and if needed WSCA
Use of tamper resistant hardware WSCD
FitCEM (CEN EN 17640) like certification for more dynamic parts (wallet instance)
WSCA: wallet secure cryptographic application, WSCD: wallet secure cryptographic device

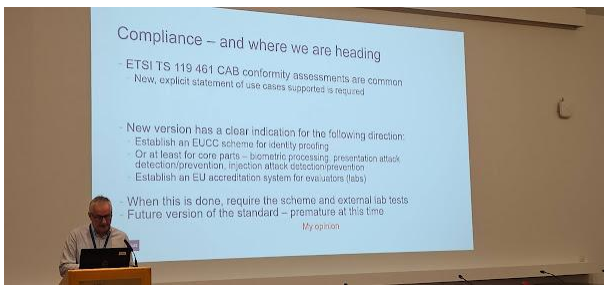

robustness against presentation and injection attacks for remote identity verification systems
interpretation of needed resistance for a specific level of assurance
Future certification scheme of the wallet
TS 18099: Biometric data injection attack detection (already voted)
European requirements for biometric products (in preparation)


Equivalent evaluation
Evaluation done by accredited Conformity Assessment Bodies
Harmonized evaluation of robustness against presentation and injection attacks for remote identity verification systems
Harmonized interpretation of needed resistance for a specific level of assurance
Future certification scheme of the wallet

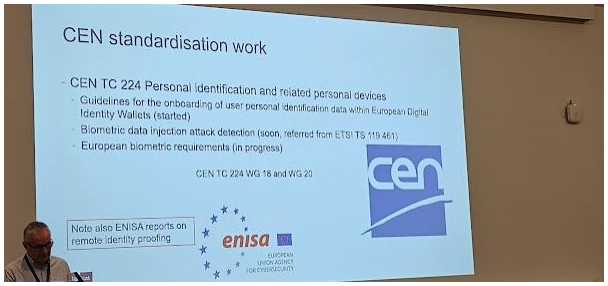

Same ruleset for everyone
Implementing acts
Providing more detailed rules on implementing eIDAS
European standards
Adapted to the singularities of European legislation
International standards / technical specifications
Many standards existing, others in work, some still missing

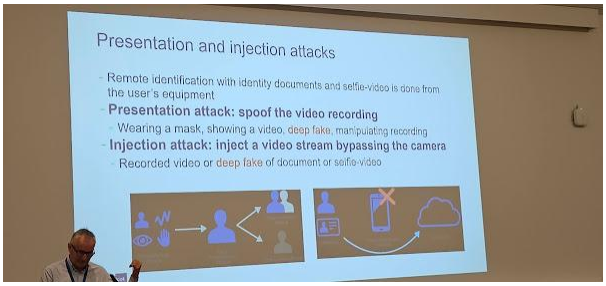

Pillars of trust for implementing eIDAS V2
Qualified trust services / notified eID schemes / EUDI wallet
Same ruleset for everyone
Equivalent evaluation
Cooperation

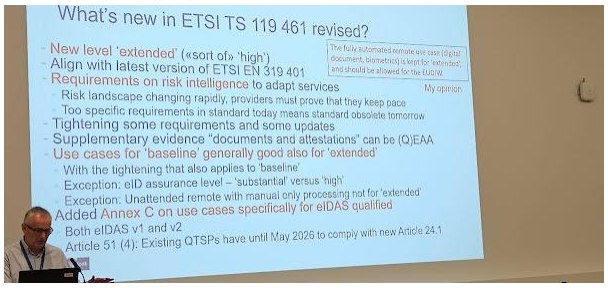

Roles of ANSSI in eIDAS
French National cybersecurity agency (ANSSI)
SB for trust services
SB for cybersecurity aspects of EUDI wallet
Certification of eID means and EUDI wallet
NIS 2

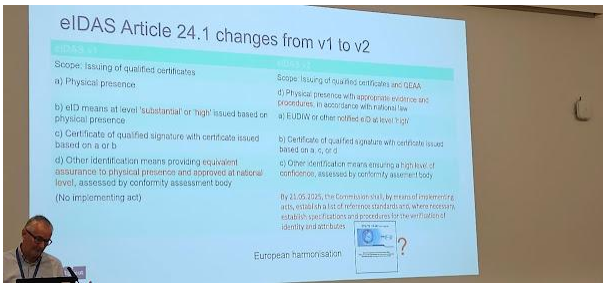

Compliance – and where we are heading
ETSI TS 119 461 CAB conformity assessments are common
New, explicit statement of use cases supported is required
New version has a clear indication for the following direction:
Establish an EUCC scheme for identity proofing
Or at least for core parts – biometric processing, presentation attack detection/prevention, injection attack detection/prevention
Establish an EU accreditation system for evaluators (labs)
When this is done, require the scheme and external lab tests
Future version of the standard – premature at this time
My opinion

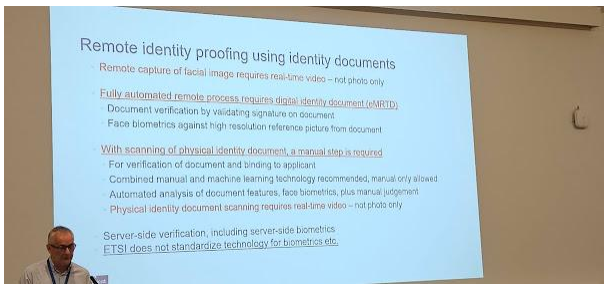

ISO standards
ISO

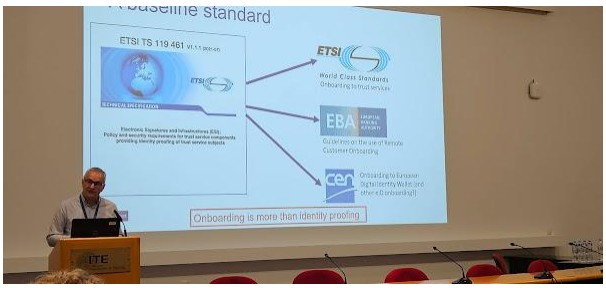

CEN standardisation work
- CEN TC 224 Personal identification and related personal devices
- Guidelines for the onboarding of user personal identification data within European Digital Identity Wallets (started)
- Biometric data injection attack detection (soon, referred from ETSI TS 119 461)
- European biometric requirements (in progress)
CEN TC 224 WG 18 and WG 20
Note also ENISA reports on remote identity proofing
enisa
cen

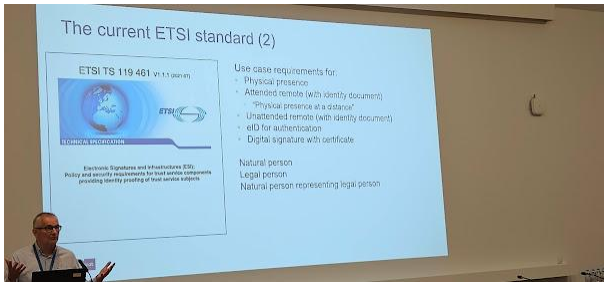

Presentation and injection attacks
- Remote identification with identity documents and selfie-video is done from the user's equipment
- Presentation attack: spoof the video recording
Wearing a mask, showing a video, deep fake, manipulating recording
- Injection attack: inject a video stream bypassing the camera
- Recorded video or deep fake of document or selfie-video

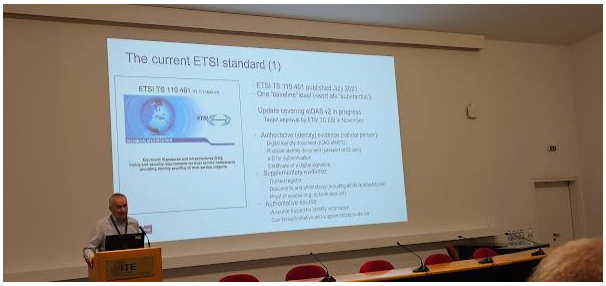

What's new in ETSI TS 119 461 revised?
- New level 'extended' («sort of» 'high')
- Align with latest version of ETSI EN 319 401
- Requirements on risk intelligence to adapt services
- Risk landscape changing rapidly, providers must prove that they keep pace
- Too specific requirements in standard today means standard obsolete tomorrow
- Tightening some requirements and some updates
- Supplementary evidence "documents and attestations" can be (Q)EAA
- Use cases for 'baseline' generally good also for 'extended'
- With the tightening that also applies to 'baseline'
- Exception: eID assurance level – 'substantial' versus 'high'
- Exception: Unattended remote with manual only processing not for 'extended'
Added Annex C on use cases specifically for eIDAS qualified
Both eIDAS v1 and v2
Article 51 (4): Existing QTSPs have until May 2026 to comply with new Article 24.1
The fully automated remote use case (digital document, biometrics) is kept for 'extended' and should be allowed for the EUDIW.
My opinion

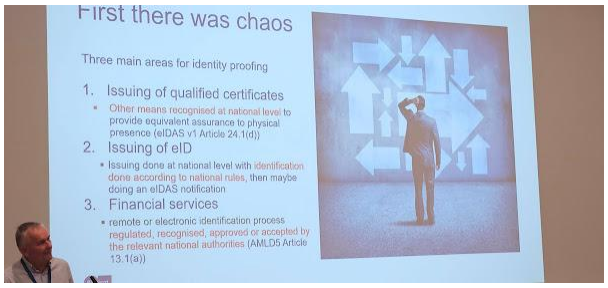

eIDAS Article 24.1 changes from v1 to v2
Scope: Issuing of qualified certificates
a) Physical presence
b) eID means at level 'substantial' or 'high' issued based on physical presence
c) Certificate of qualified signature with certificate issued based on a or b
d) Other identification means providing equivalent assurance to physical presence and approved at national level, assessed by conformity assessment body
(No implementing act)
Scope: Issuing of qualified certificates and QEAA
a) Physical presence with appropriate evidence and procedures, in accordance with national law
a) EUDIW or other notified eID at level high
b) Certificate of qualified signature with certificate issued based on a, c, or d
c) Other identification means ensuring a high level of confidence, assessed by conformity assement body
By 21.05.2025, the Commission shall, by means of implementing acts, establish a list of reference standards and, where necessary, establish specifications and procedures for the verification of identity and attributes
European harmonisation

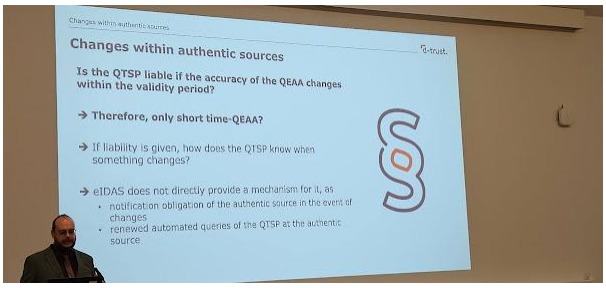

Remote identity proofing using identity documents
- Remote capture of facial image requires real-time video – not photo only
- Fully automated remote process requires digital identity document (eMRTD)
Document verification by validating signature on document
Face biometrics against high resolution reference picture from document
- With scanning of physical identity document, a manual step is required
For verification of document and binding to applicant
Combined manual and machine learning technology recommended, manual only allowed
Automated analysis of document features, face biometrics, plus manual judgement
Physical identity document scanning requires real-time video – not photo only
- Server-side verification, including server-side biometrics
- ETSI does not standardize technology for biometrics etc.

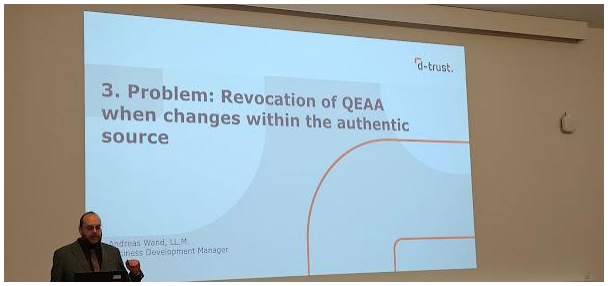

baseline standard
ETSI TS 119 461
ETSI
World Class Standards
EBA
cen
Onboarding is more than identity proofing
ITE

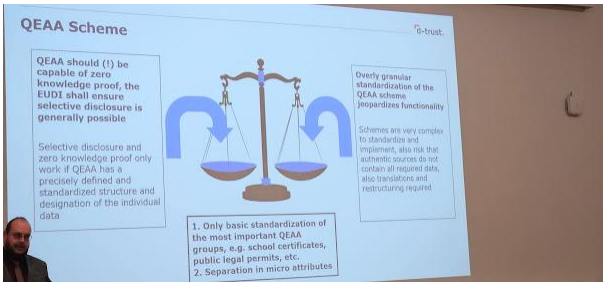

The current ETSI standard (2)
ETSI TS 119 461
Use case requirements for:
- Physical presence
- Attended remote (with identity document)
"Physical presence at a distance"
- Unattended remote (with identity document)
- eID for authentication
- Digital signature with certificate
Natural person
Legal person
Natural person representing legal person

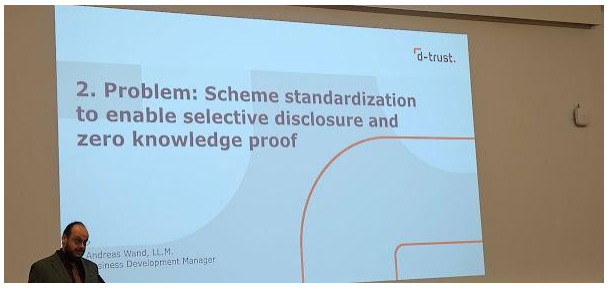

The current ETSI standard (1)
ETSI TS 119 461
ITE

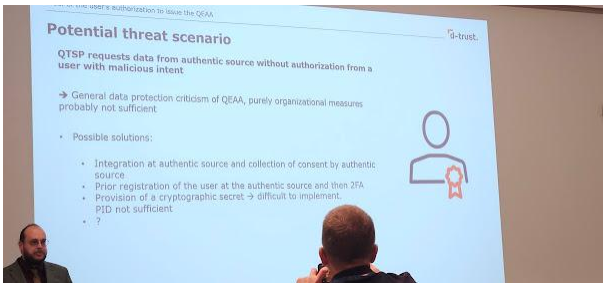

First there was chaos
Three main areas for identity proofing
1. Issuing of qualified certificates
Other means recognised at national level to provide equivalent assurance to physical presence (eIDAS v1 Article 24.1(d))
2. Issuing of eID
Issuing done at national level with identification done according to national rules, then maybe doing an eIDAS notification
3. Financial services
remote or electronic identification process regulated, recognised, approved or accepted by the relevant national authorities (AMLD5 Article 13.1(a))

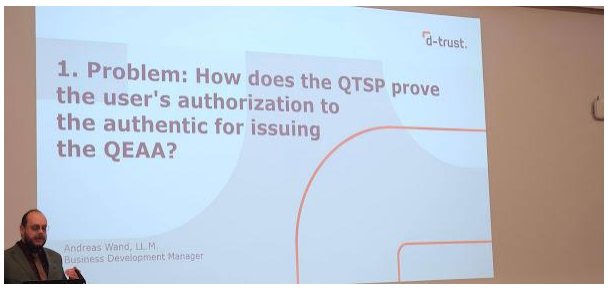

Changes within authentic sources
Changes within authentic sources
Is the QTSP liable if the accuracy of the QEAA changes within the validity period?
→ Therefore, only short time-QEAA?
→ If liability is given, how does the QTSP know when something changes?
→ eIDAS does not directly provide a mechanism for it, as
- notification obligation of the authentic source in the event of changes
- renewed automated queries of the QTSP at the authentic source

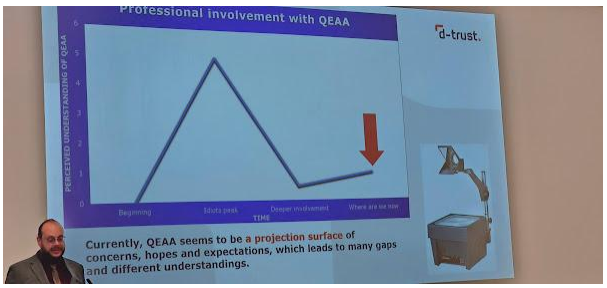

d-trust.
3. Problem: Revocation of QEAA when changes within the authentic source
Andreas Wand, LL.M.
Business Development Manager


QEAA Scheme
d-trust.
QEAA should (!) be capable of zero knowledge proof, the EUDI shall ensure selective disclosure is generally possible
Selective disclosure and zero knowledge proof only work if QEAA has a precisely defined and standardized structure and designation of the individual data
Overly granular standardization of the QEAA scheme jeopardizes functionality
Schemes are very complex to standardize and implement, also risk that authentic sources do not contain all required data, also translations and restructuring required
1. Only basic standardization of the most important QEAA groups, e.g. school certificates, public legal permits, etc.
2. Separation in micro attributes

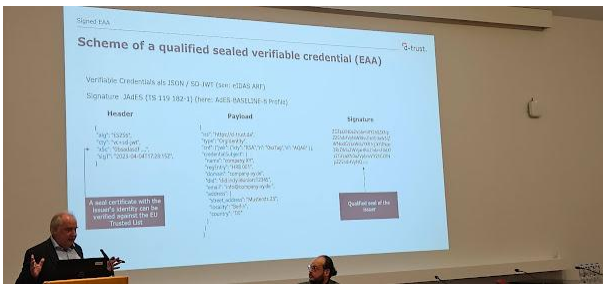

d-trust.
2. Problem: Scheme standardization to enable selective disclosure and zero knowledge proof
Andreas Wand, LL.M.
Business Development Manager

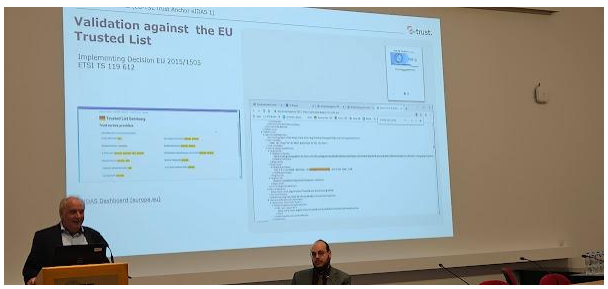

Potential threat scenario
d-trust.
QTSP requests data from authentic source without authorization from a user with malicious intent
→ General data protection criticism of QEAA, purely organizational measures probably not sufficient
Possible solutions:
Integration at authentic source and collection of consent by authentic source
Prior registration of the user at the authentic source and then 2FA
Provision of a cryptographic secret → difficult to implement.
PID not sufficient
?

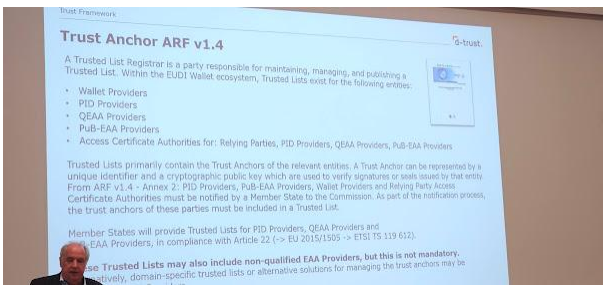

d-trust.
1. Problem: How does the QTSP prove the user's authorization to the authentic for issuing the QEAA?
Andreas Wand, LL.M.
Business Development Manager

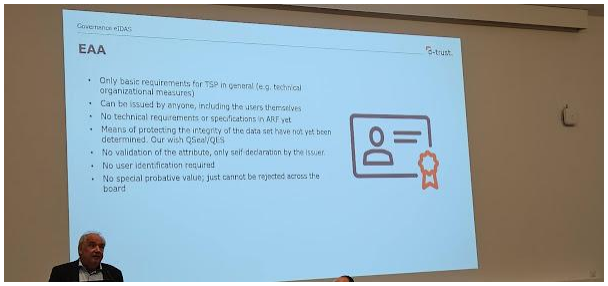

Professional involvement with QEAA
d-trust.
PERCEIVED UNDERSTANDING OF QEAA
TIME
Beginning
Idiots peak
Deeper involvement
Where are we now
Currently, QEAA seems to be a projection surface of concerns, hopes and expectations, which leads to many gaps and different understandings.

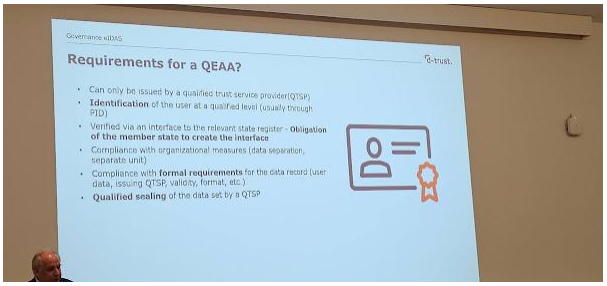

Legal Identity
d-trust.
European organisational company ID - ORG ID
Payload of a QEAA
Definition EUID
Directive EU 2017/1132
Commission Implementing Regulationd (EU) 2015/884 of 8 June 2015
Business Registers Interconnetion System (BRIS) Register
D-Trust GmbH - Germany
https://e-justice.europa.eu/content_find_a_company-489-en.do

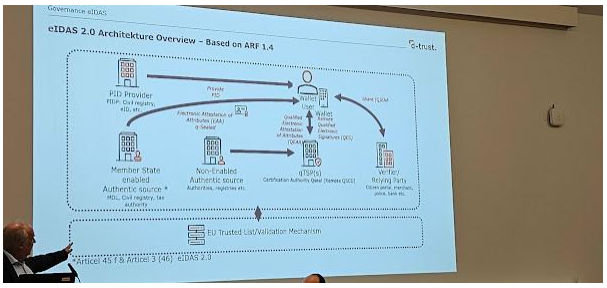

Signed EAA
d-trust.
Scheme of a qualified sealed verifiable credential (EAA)
Verifiable Credentials als JSON / SD-JWT (see: eIDAS ARF)
Signature JAdES (TS 119 182-1) (here: AdES-BASELINE-B Profile)
Header
Payload
Signature
A seal certificate with the issuer's identity can be verified against the EU Trusted List
Qualfied seal of the issuer


d-trust.
Validation against the EU Trusted List
Implementing Decision EU 2015/1505
ETSI TS 119 612


Trust Framework
d-trust.
Trust Anchor ARF v1.4
A Trusted List Registrar is a party responsible for maintaining, managing, and publishing a Trusted List. Within the EUDI Wallet ecosystem, Trusted Lists exist for the following entities:
Wallet Providers
PID Providers
QEAA Providers
PuB-EAA Providers
Access Certificate Authorities for: Relying Parties, PID Providers, QEAA Providers, PuB-EAA Providers
Trusted Lists primarily contain the Trust Anchors of the relevant entities. A Trust Anchor can be represented by a unique identifier and a cryptographic public key which are used to verify signatures or seals issued by that entity. From ARF v1.4 - Annex 2: PID Providers, PuB-EAA Providers, Wallet Providers and Relying Party Access Certificate Authorities must be notified by a Member State to the Commission. As part of the notification process, the trust anchors of these parties must be included in a Trusted List.
Member States will provide Trusted Lists for PID Providers, QEAA Providers and PuB-EAA Providers, in compliance with Article 22 (-> EU 2015/1505 -> ETSI TS 119 612).
These Trusted Lists may also include non-qualified EAA Providers, but this is not mandatory.







ENISA meeting - 6th session

Christian sergebarth d trust

Qtsp are authentic sources
They deliver things to the wallets
Things are signed and sealed
Pub eaa
What kind of databases and interfaces will be available
Eaa can be used by anyone
No validation of the attributes just seal them
Eaa jade's baseline b
RegEntry is the point to identify the issuer
For credentials there is this standard

Andreas wand
Idiot's peek.
3 open problems
How does qtsp prive user authorisation
Potential threats scenario
Integrate qeaa to the authentic source
Schem stabdarisatio versus zkp

No EU regulatio requirements on zkp
Over granular qeaa jeopardize functionality
Revocation problemas.of qeaa
Liability of qeaa when authentic source changes?
How to asses the attribute is still valid?
Automatic queries for eaa on issued attributes

Jon olnes
Identity proffing

Remote identity proffing does not exist in most countries
Update on the standards for eidas 2
Prove you id using at least one authoritative means
Supplementary evidence can be bank login
Standard brings good use case requirements
Onboarding for the wallet will use this standard
Remote need to do a video. Photos is not enough
ETSI does not standardise biometrics
A lot of changes from eidas1 to eidas2
Problem of video spoofing
Injection attack bypassing the camera
Deep fakes are a problem now

Andrea rock
Best practices for impelmentin eidas 2

Pilar's for implementing eidas2
Same ruleset for everyone, equivalent evaluation, cooperation
Wallet certification eea4+ wscd and wsca
Use tamper resistant hardware on the wallet

Panel
A lot of changes on eidas1
Remote signature are a big possibility
Eidas was successful in the cooperation between different bodies
The problem of diginitar was important for making some things happen
The best hopes tor QTSP are on QEAA
Creating new services is paramount for the future. Its is a plain field on that.
article 45 is very important for browsers
do you believe in qualified ledger?
it is possible f well certified
does it compete with time stamping?
the challenge is making qualified ledger operational
Auditing on qualified ledge and auditing for qualified archival
use of certificate transparency logs and transparency
Certificate transparency for public use require resources
ETSI and the browser are working to make CT workeablçe and inclusion of the TSL on browsers