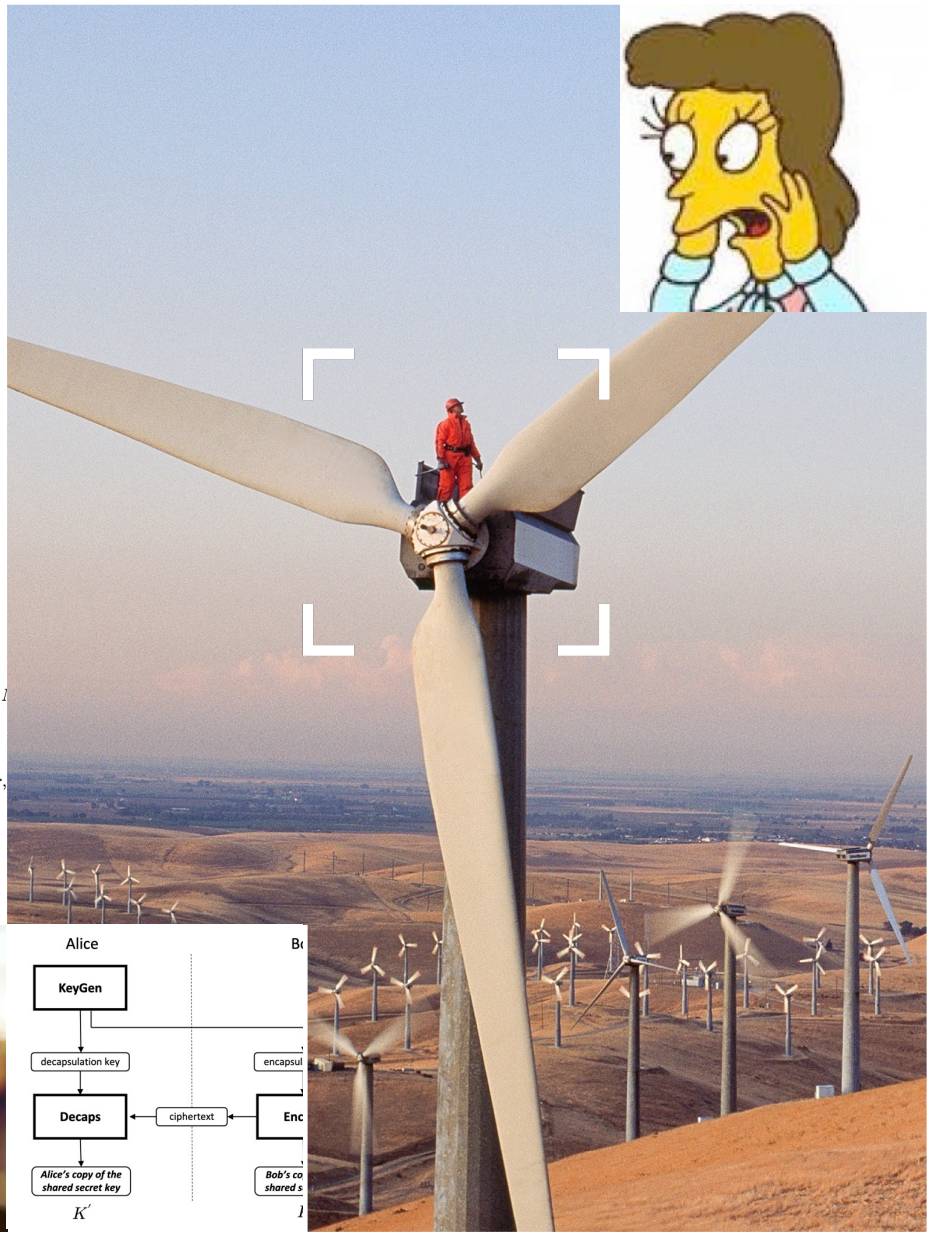
DNV
CYBER

Oh! Won't Someone Think of the Identification Infrastructure!

Jussipekka Leiwo, Ph.D.
Product Cyber Security Strategy Consultant



Why This Presentation?

Lot of talk of SNDL

And of Grover's Algorithm

And of Shor's Algorithm

And of the Q-Day

Maybe we should also talk a bit more of the identification infrastructure and PQC

DNV CYBER

Assets Guarded by SSCDs

prEN 14169-2:2012
Protection profiles for secure signature creation device — Part 2: Device with key generation

6.1 Assets, users and threat agents

The Common Criteria define assets as entities that the owner of the TOE presumably places value upon. The term “asset” is used to describe the threats in the operational environment of the TOE.

Assets and objects:

1. SCD: private key used to perform an electronic signature operation. The confidentiality, integrity and signatory’s sole control over the use of the SCD must be maintained.
2. SVD: public key linked to the SCD and used to perform electronic signature verification. The integrity of the SVD when it is exported must be maintained.
3. DTBS and DTBS/R: set of data, or its representation, which the signatory intends to sign. Their integrity and the unforgeability of the link to the signatory provided by the electronic signature must be maintained.

DNV CYBER

Assuming Conventional Crypto

QES is only legitimate when computed for the exact DTBS the signatory intended to sign

Adversary with a QC capable of cryptoanalysis can forge signatures, i.e. violate the unforgeability of the link between a QES and the DTBS

Increasing SCD/SVD size will not help

Harder-to-guess authentication data shall not help

DNV CYBER

It's About Non-Repudiation

prEN 14169-2:2012
Protection profiles for secure signature creation device — Part 2: Device with key generation

6.3 Organisational security policies

6.3.1 **P.CSP_QCert** *Qualified certificate*

The CSP uses a trustworthy CGA to generate a qualified certificate or non-qualified certificate (cf. **the directive**, article 2, clause 9, and Annex I) for the SVD generated by the SSCD. The certificates contain at least the name of the signatory and the SVD matching the SCD implemented in the TOE under sole control of the signatory. The CSP ensures that the use of the TOE as SSCD is evident with signatures through the certificate or other publicly available information.

6.3.2 **P.QSign** *Qualified electronic signatures*

The signatory uses a signature creation system to sign data with an advanced electronic signature (cf. **the directive**, article 1, clause 2), which is a qualified electronic signature if it is based on a valid qualified certificate (according to **the directive** Annex I)[9]. The DTBS are presented to the signatory and sent by the SCA as DTBS/R to the SSCD. The SSCD creates the electronic signature created with a SCD implemented in the SSCD that the signatory maintain under their sole control and is linked to the DTBS/R in such a manner that any subsequent change of the data is detectable.

6.3.3 **P.Sigy_SSCD** *TOE as secure signature creation device*

The TOE meets the requirements for an SSCD laid down in Annex III of **the directive** [1]. This implies the SCD is used for digital signature creation under sole control of the signatory and the SCD can practically occur only once.

6.3.4 **P.Sig_Non-Repud** *Non-repudiation of signatures*

The lifecycle of the SSCD, the SCD and the SVD shall be implemented in a way that the signatory is not able to deny having signed data if the signature is successfully verified with the SVD contained in their unrevoked certificate.

DNV CYBER

Failure to fulfill P.Sig_Non-Repud
=> failure of the SSCD to fulfill any security objectives

Table 1 Mapping of security problem definition to security objectives

	OT.Lifecycle_Security	OT.SCD/SVD_Auth_Gen	OT.SCD_Unique	OT.SCD_SVD_Corresp	OT.SCD_Secrecy	OT.Sig_Secure	OT.Sigy_SigF	OT.DTBS_Integrity_TOE	OT.EMSEC_Design	OT.Tamper_ID	OT.Tamper_Resistance	OE.CGA_QCert	OE.SVD_Auth	OE.SSCD_Prov_Service	OE.HID_VAD	OE.DTBS_Intend	OE.DTBS_Protect	OE.Signatory
T.SCD_Divulg					X													
T.SCD_Derive		X				X												
T.Hack_Phys					X				X	X	X							
T.SVD_Forgery				X									X					
T.SigF_Misuse	X						X	X							X	X	X	X
T.DTBS_Forgery								X								X	X	
T.Sig_Forgery			X			X						X						
P.CSP_QCert	X			X								X						
P.QSign						X	X					X				X		
P.Sigy_SSCD	X	X	X		X	X	X	X	X		X			X				
P.Sig_Non-Repud	X		X	X	X	X	X	X	X	X	X	X	X	X		X	X	X
A.CGA												X	X					
A.SCA																X		

- Plausible deniability of a digital signature shall trigger failure of practically every security objective of a SSCD
- A single forged signature or a credible possibility of it shall invalidate the entire digital signature infrastructure

DNV CYBER

Wait! There is more

DIRECTIVE 1999/93/EC OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 13 December 1999 on a Community framework for electronic signatures (OJ L 013, 19.1.2000, p.12)

Amended by: REGULATION (EC) No 1137/2008 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 22 October 2008

Article 5

Legal effects of electronic signatures

1. Member States shall ensure that advanced electronic signatures which are based on a qualified certificate and which are created by a secure-signature-creation device:

(a) satisfy the legal requirements of a signature in relation to data in electronic form in the same manner as a handwritten signature satisfies those requirements in relation to paper-based data; and

(b) are admissible as evidence in legal proceedings.

2. Member States shall ensure that an electronic signature is not denied legal effectiveness and admissibility as evidence in legal proceedings solely on the grounds that it is:

— in electronic form, or

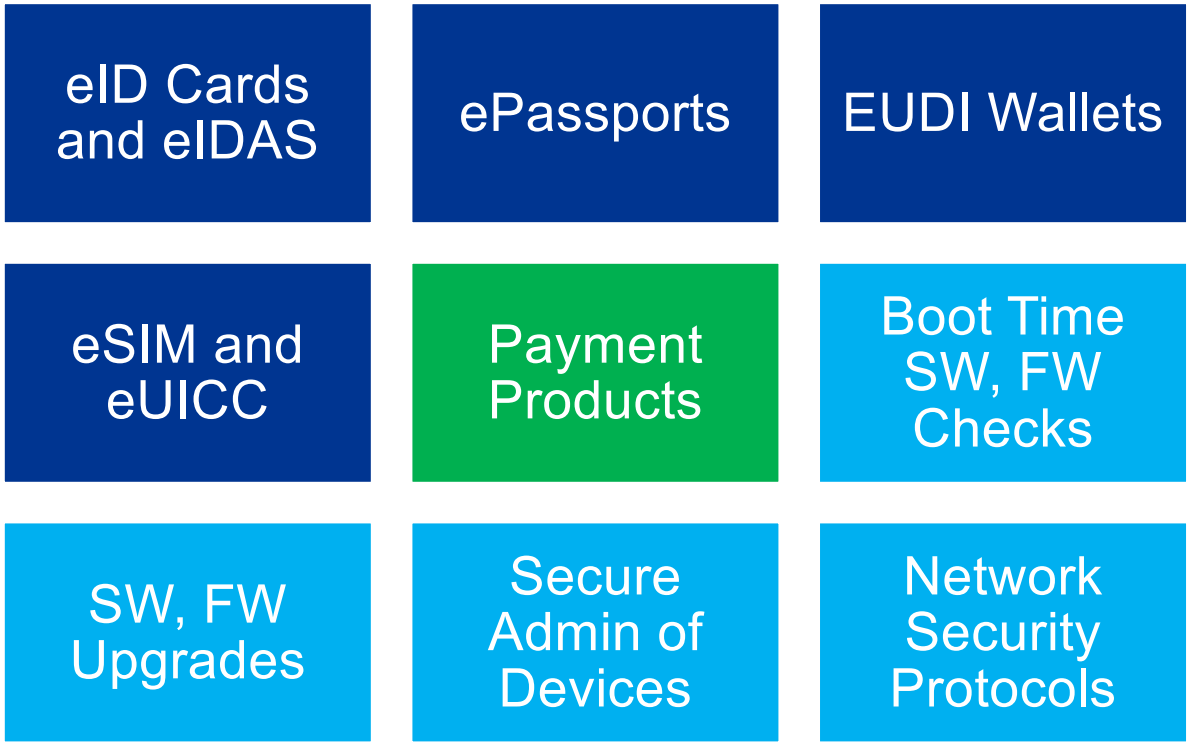
— not based upon a qualified certificate, or

— not based upon a qualified certificate issued by an accredited certification-service-provider, or

— not created by a secure signature-creation device.

DNV CYBER

Identification Infrastructure is at the Core of Everything



DNV CYBER

Common Characteristics of Identification Devices

- Based on Dedicated, High Assurance IC Chips
- Embedded Devices with Complex Life-Cycle Models
- Difficult to Upgrade, Patch Once Issued
- Require Considerable Back End Support for Operation
- Require Complex Personalization and Issuance Processes and Infrastructure
- Long Lead Times in the Development, Production
- Long Lead Times in Formal Evaluations, Certifications
- At Least Five, Preferably Ten Years of Validity – Longer for OT Components
- 2030/2035 is Approaching Fast

DNV CYBER

Why 2030 and 2035?

Source: A Coordinated Implementation Roadmap for the Transition to Post-Quantum Cryptography

https://digital-strategy.ec.europa.eu/en/library/coordinated-implementation-roadmap-transition-post-quantum-cryptography

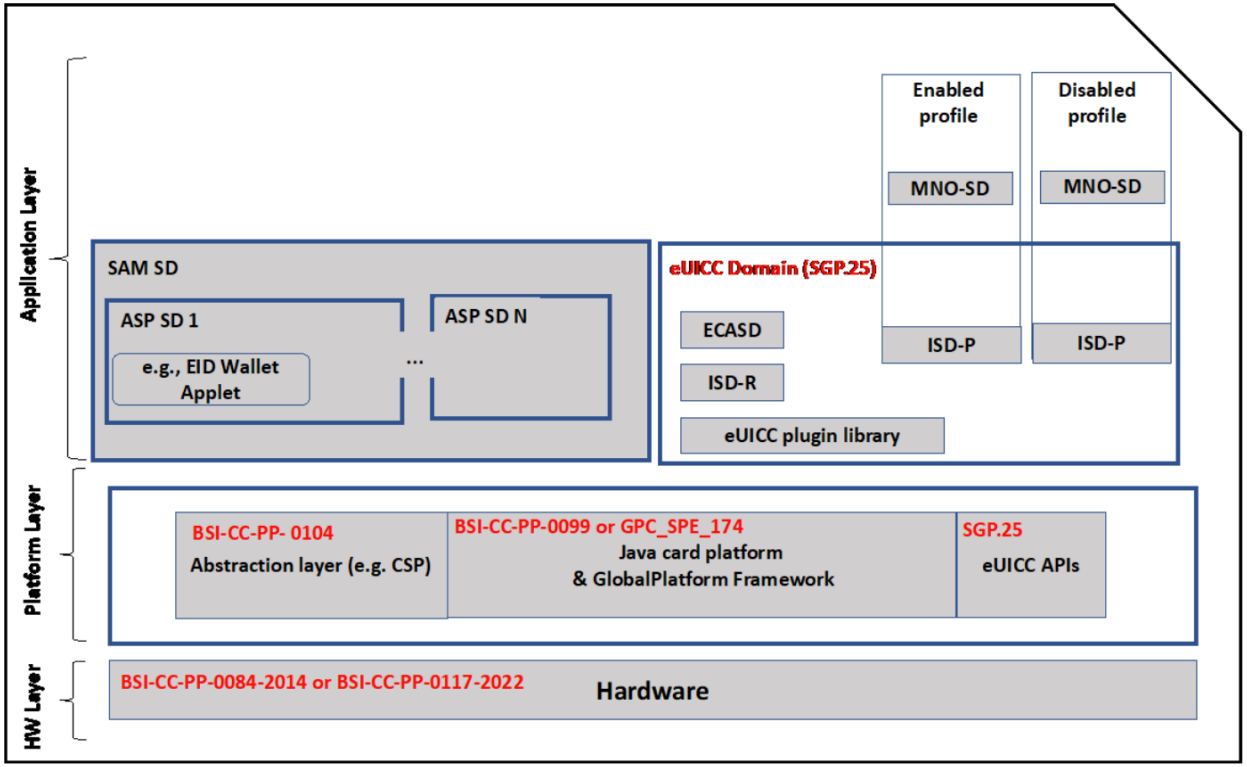
Timeline for the transition to PQC

1. By **31.12.2026**:
   - At least the *First Steps* have been implemented by all Member States.
   - Initial national PQC transition roadmaps have been established by all Member States.
   - PQC transition planning and pilots for high- and medium-risk use cases have been initiated.
2. By **31.12.2030**:
   - The *Next Steps* have been implemented by all Member States.
   - The PQC transition for high-risk use cases has been completed.
   - PQC transition planning and pilots for medium-risk use cases have been completed.
   - Quantum-safe software and firmware upgrades are enabled by default.
3. By **31.12.2035**:
   - The PQC transition for medium-risk use cases has been completed.
   - The PQC transition for low-risk use cases has been completed as much as feasible.

2030/2035 is Approaching Fast

DNV CYBER

Example: eUICC Chip (Consumer Device)



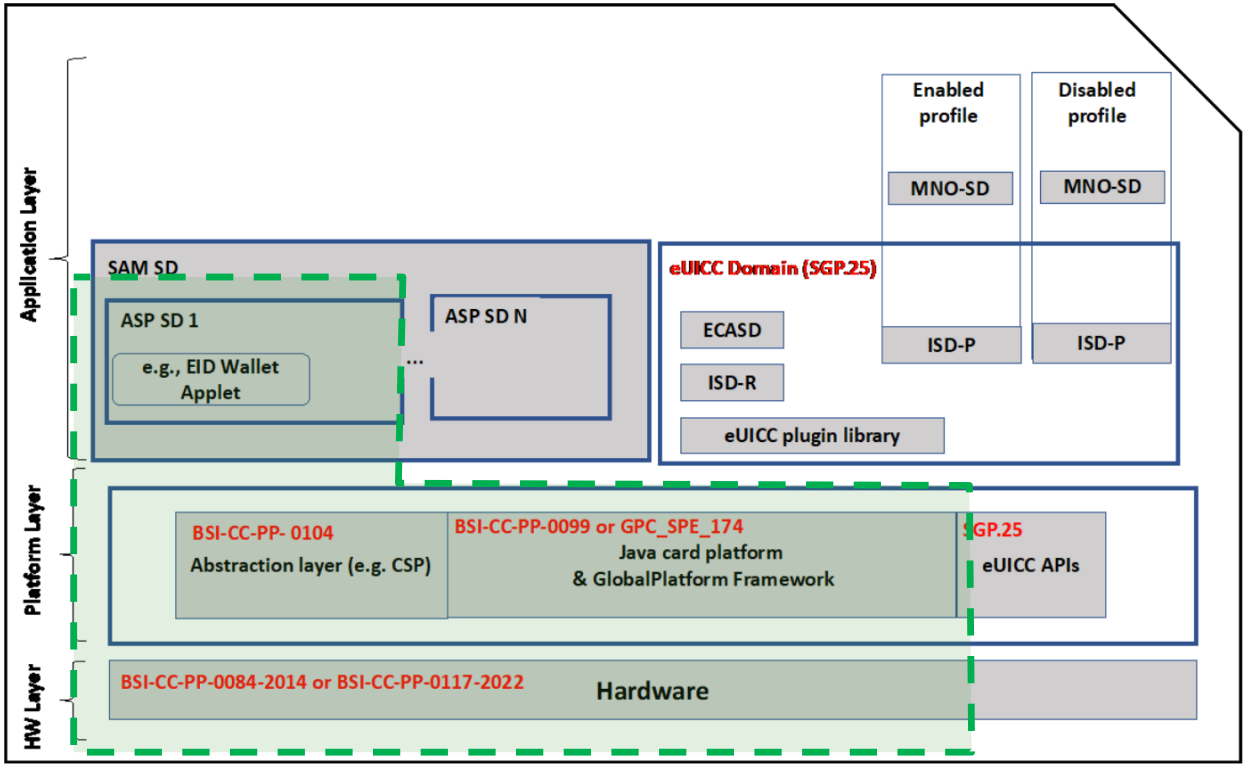
Source: SPECIFICATIONS FOR EUICC CERTIFICATION UNDER THE EUCC SCHEME, Version 1.0 for public consultation
https://certification.enisa.europa.eu/document/download/23686749-bb1a-46d1-bd7d-bee64f3e69ea_en?filename=EU5G-eUICC%20consultation-240626_0.pdf

DNV CYBER

Technology vs. Application Security Requirements

Protection Profiles for Applications (e.g. SSCD)

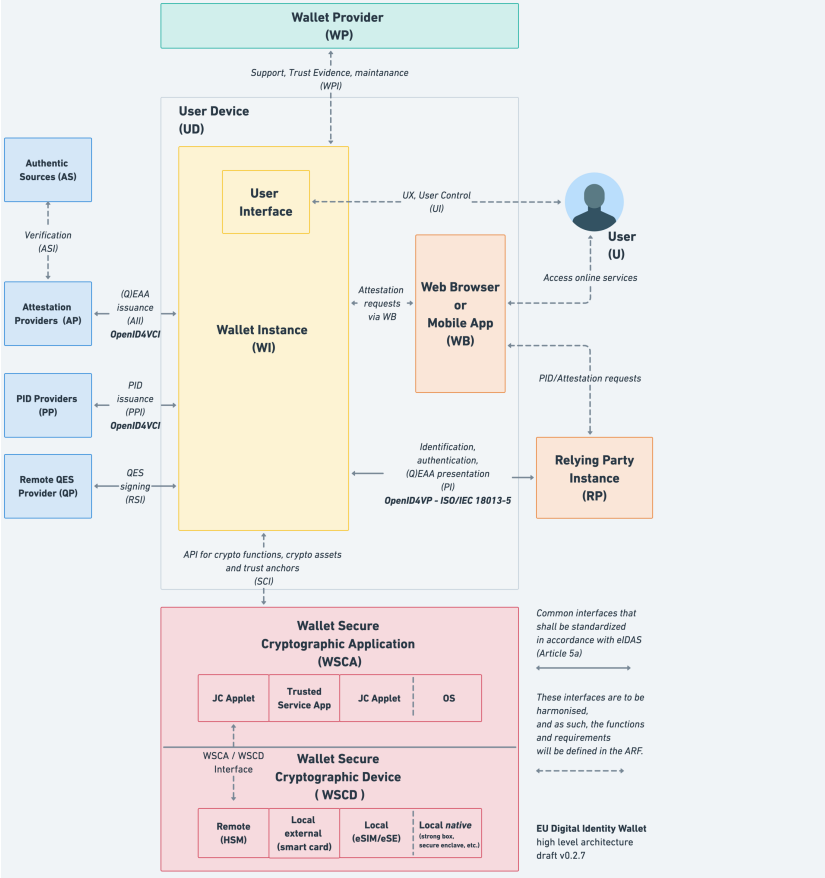
Protection Profiles for Technologies (e.g. Smart Card IC)



Source: SPECIFICATIONS FOR EUICC CERTIFICATION UNDER THE EUCC SCHEME, Version 1.0 for public consultation
https://certification.enisa.europa.eu/document/download/23686749-bb1a-46d1-bd7d-bee64f3e69ea_en?filename=EU5G-eUICC%20consultation-240626_0.pdf

DNV CYBER

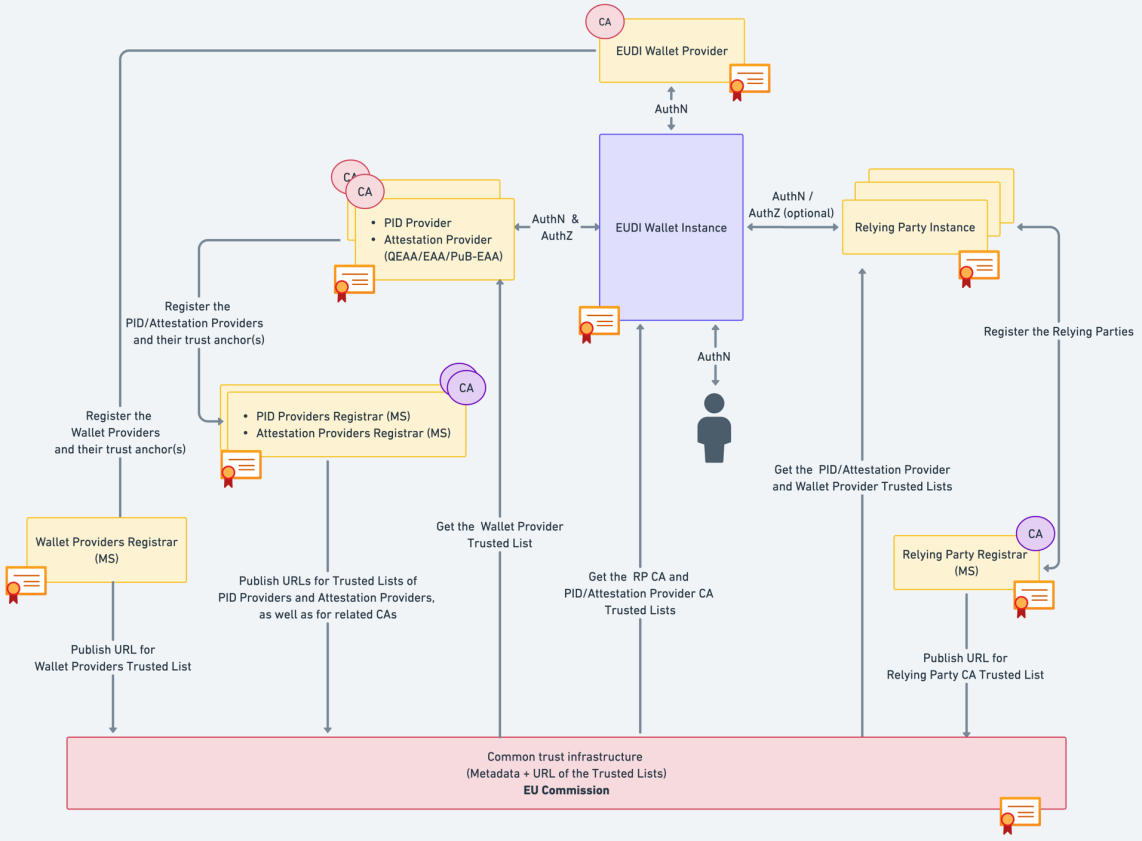
Example: EUDI Wallet Reference Architecture



Source: European Digital Identity Wallet Architecture and Reference Framework
https://eu-digital-identity-wallet.github.io/eudi-doc-architecture-and-reference-framework/1.4.0/arf/

DNV
CYBER

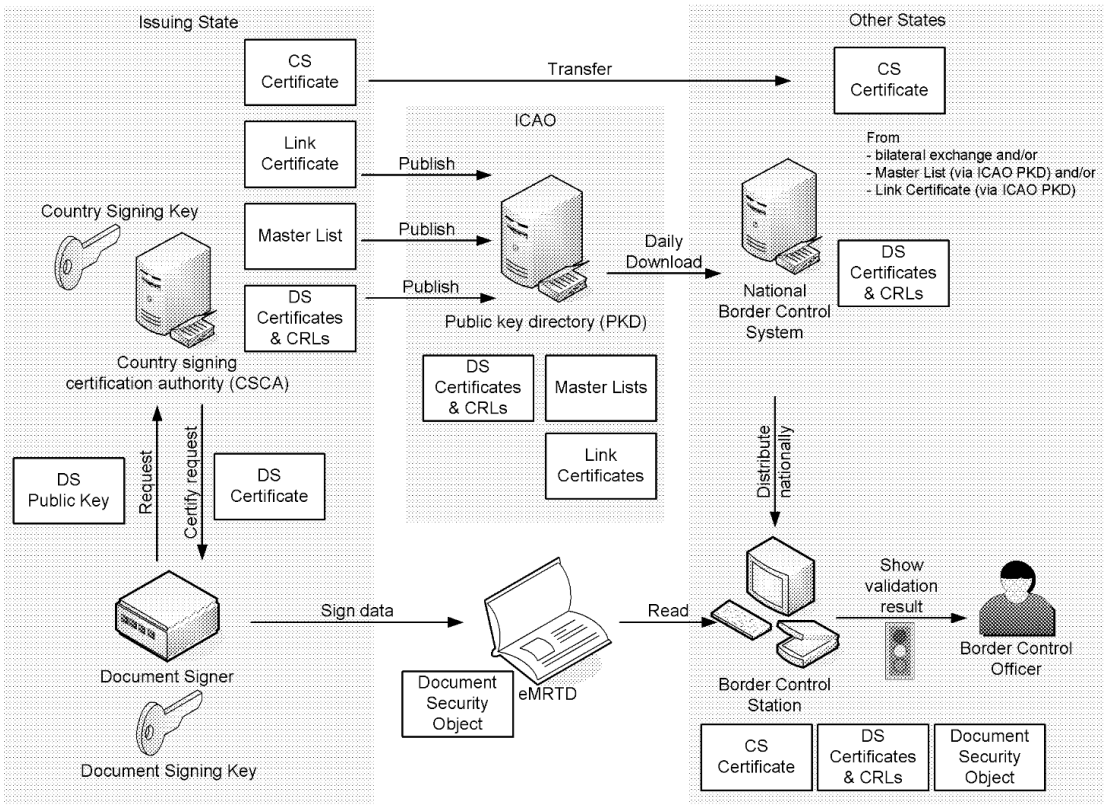
Example: EUDI Wallet Trust Infrastructure



Source: European Digital Identity Wallet Architecture and Reference Framework
https://eu-digital-identity-wallet.github.io/eudi-doc-architecture-and-reference-framework/1.4.0/arf/

DNV CYBER

Example: ICAO Public Key Directory



105

participants at the end of July, 2025

Source: https://www.icao.int/sites/default/files/2025-06/APrimeronthePublicKeyDirectory.pdf

DNV CYBER

Cyber Security of the Critical Sectors

Highly critical sectors in scope are:

- Digital infrastructures (electronic communications, trust services, domain name services, top level domain registries, cloud services, data centers, internet exchange points, content delivery networks);
- Energy (electricity, district heating, oil, gas and hydrogen);
- Transport (air, rail, water, road);
- Banking and Financial market infrastructures;
- Health (healthcare providers, EU reference labs, research and manufacturing of pharmaceuticals and medical devices);
- Drinking water and waste water;
- Public administrations;
- Space.

Other critical sectors in scope are:

- Postal and courier services;
- Waste management;
- Manufacture, production and distribution of chemicals;
- Manufacturing;
- Digital providers;
- Research.

Alongside the provisions of the NIS2, new requirements have been introduced from other key horizontal and sector-specific legislations, such as the Cyber Resilience Act (CRA) and the Digital Operational Resilience Act (DORA).
ENISA developed a NIS2 awareness campaign the effort to further support organisations and authorities in adhering with the provisions of the NIS 2 Directive. The purpose of this informative material and resources is to educate businesses and competent authorities by providing a comprehensive overview of the Directive's requirements, illustrating how it affects them.

NIS2 is for the trustworthiness of Entities. CRA is for the trustworthiness of Products

Source: https://enisa.europa.eu/topics/cybersecurity-of-critical-sectors

DNV CYBER

What Does NIS2 Have to Do with PQC?

Highly critical sectors in scope are:

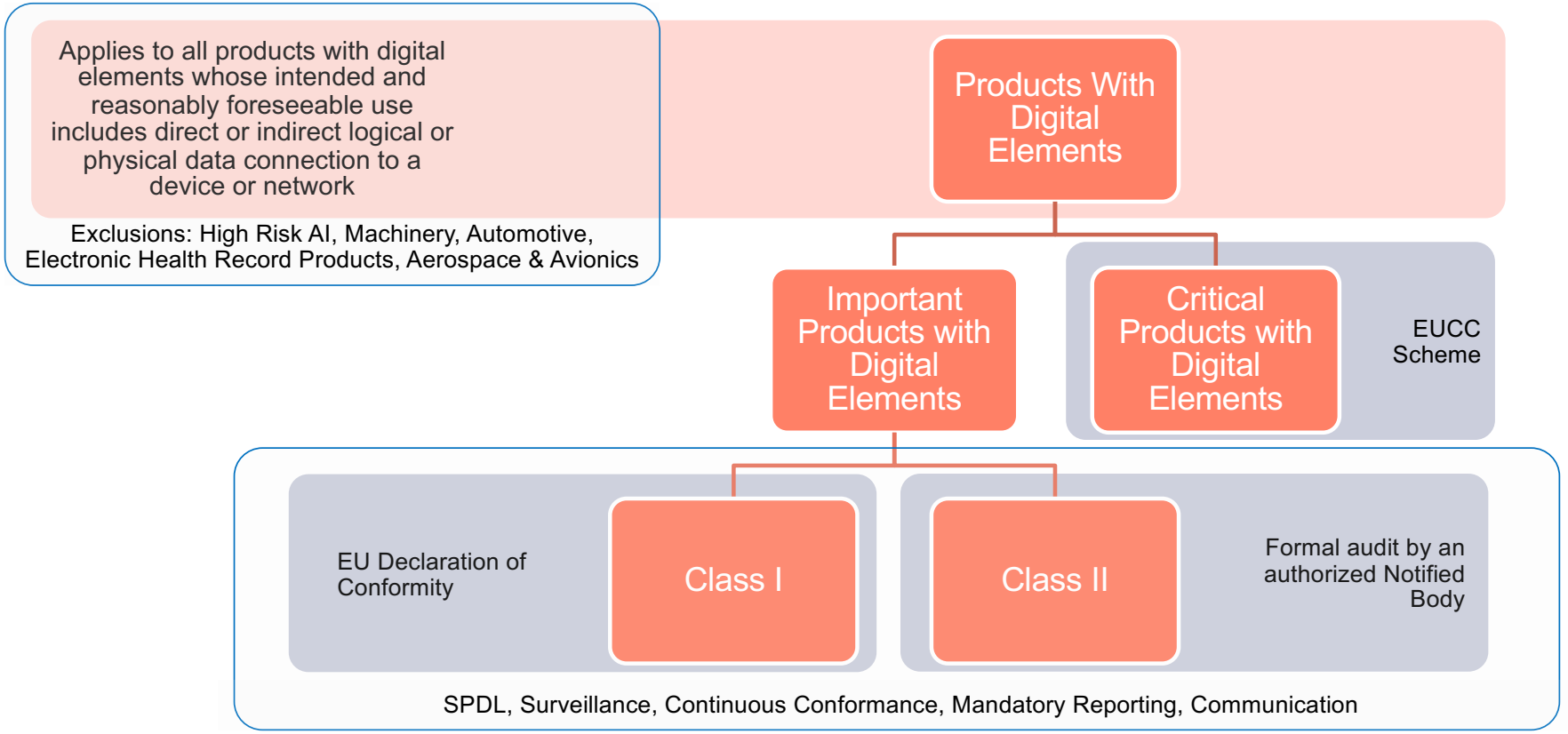
- Digital infrastructures (electronic communications, trust services, domain name services, top level domain registries, cloud services, data centers, internet exchange points, content delivery networks);

- ✓ Infrastructure required for production of identification infrastructure components, operation of the personalization and issuance infrastructure falls into NIS2, CRA, vertical regulation
- ✓ It must all be upgraded to support PQC algorithms, protocols, key and certificate sizes
- ✓ Complete high assurance infrastructure required for ensuring that the policy for the non-repudiation of signatures is fulfilled

Alongside the provisions of the NIS2, new requirements have been introduced from other key horizontal and sector-specific legislations, such as the Cyber Resilience Act (CRA) and the Digital Operational Resilience Act (DORA).
ENISA developed a NIS2 awareness campaign the effort to further support organisations and authorities in adhering with the provisions of the NIS 2 Directive. The purpose of this informative material and resources is to educate businesses and competent authorities by providing a comprehensive overview of the Directive's requirements, illustrating how it affects them.

Source: https://enisa.europa.eu/topics/cybersecurity-of-critical-sectors

Cyber Resiliency Act



DNV CYBER

Good News, Everyone!

- The IC Industry is Really Good at Designing, Manufacturing High Assurance ICs, SW
- The ITSEFs Are Really Good at Evaluating High Assurance ICs, SW, Life-Cycle Models
- There Is No Need to Reinvent the Wheel. Same Components Are Utilized in Different Applications. Certification Schemes Are Designed for Assurance Maintenance, Reuse
- With EUCC, There Will Be Additional High Assurance Certification Capacity
- The Regulators are Wide Awake
- The Industry Is Good at Adapting to Change, Responding to Emerging Security Demands

DNV
CYBER

Some Conclusions

- Identification is Largely a Question of Non-Repudiation
- Digital Signatures Are (Well, Should Be) Computed with Secure ICs
- Security of the Signatures Requires Action From Many Parties, Not Only IC Vendors
- Transitioning to PQC Requires Coordinated Effort To Ensure That the Entire Infrastructure Transitions Completely
- The EU, many non-EU Nations are Active and Driving the Change

DNV CYBER

Thank You

Jussi.Leiwo@dnv.com

www.dnv.com/cyber

DNV
CYBER