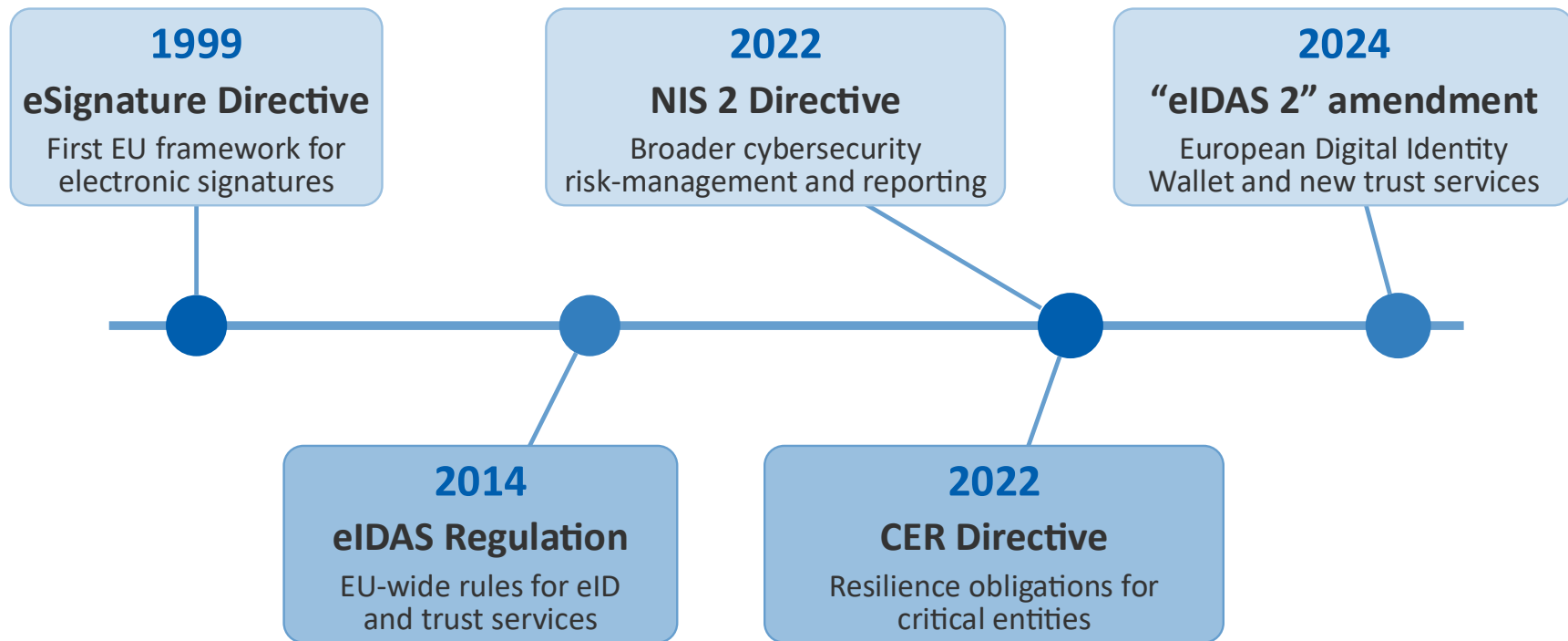


ECATS in Transition

Building a European Supervisory Community for the
Next Generation of Trust Services

Ulrich Latzenhofer
Tallinn, 15 September 2026

Evolution of the European framework



Cross-border services required supervisory dialogue from day one

eSignature Directive (1999)

- Supervision of qualified certification service providers within a Member State
- But no restriction of certification services originating in another Member State
- Practical need for cooperation among supervisory bodies and harmonisation of their activities
- **Forum of European Supervisory Authorities for Electronic Signatures (FESA)** established as independent group in 2001 (now **for Trust Service Providers** and still very successful)

eIDAS Regulation (2014)

- More detailed provisions for supervision of trust service providers (TSPs)
- Specific provisions for cooperation and mutual assistance between supervisory bodies
- Security requirements and reporting obligations of TSPs (Article 19)
- **Article 19 Expert Group** established by ENISA in 2015

Expert Group created long-term practical value for supervisory ecosystem



Objective	Achievements (examples)
Harmonised security implementation	Incident reporting framework Cooperation with ETSI on specific standardisation issues
Voluntary information exchange	Communications on specific vulnerabilities affecting trust services
Review of ENISA deliverables	Feedback on various ENISA frameworks, reports, guidelines and recommendations relevant to TSPs
Input to the ENISA work programme	Trainings and workshops on key topics like remote ID proofing, cloud security and blockchain
Regulatory and policy feedback	Feedback for eIDAS review, position paper on NIS 2 proposal, input to NIS 2 implementing regulation

Transition from eIDAS Article 19 to a comprehensive security framework

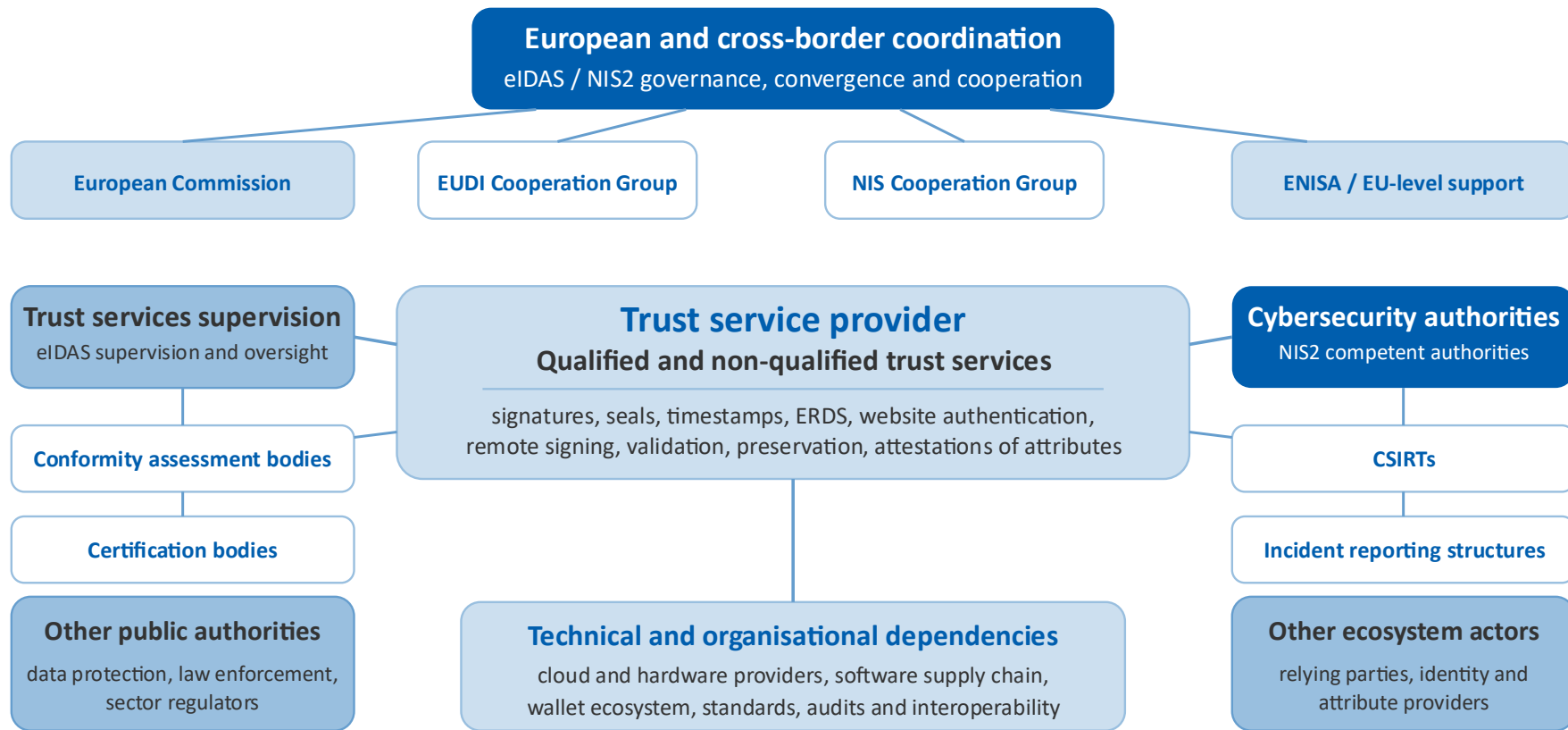
Cybersecurity risk-management measures and reporting obligations (NIS 2 Articles 21 and 23)

- Further specified by Commission Implementing Regulation (EU) 2024/2690

Security requirements beyond cybersecurity (eIDAS Articles 19a and 24)

- Specific security measures for non-qualified TSPs
- Additional security measures for qualified TSPs
- Additional reporting to supervisory body for trust services
- Further specified by many implementing acts and reference standards

A more interconnected supervisory environment RTR



Trust services becoming part of a broader ecosystem

Higher level of alignment required among relevant authorities, both nationally and cross-border

- Double burdens for TSPs (incident reporting, compliance audits) to be avoided
- The challenge is not only compliance – it is cross-regime consistency

Transition of ENISA Article 19 Expert Group into ECATS Expert Group in 2022

- ECATS = European Competent Authorities for Trust services
- Collaboration of supervisory bodies for trust services and cybersecurity authorities on an equal footing
- Addressing security aspects of trust services, regardless of whether the legal basis is NIS 2 or eIDAS 2
- Otherwise same objectives and working methods as before

NIS Cooperation Group — EU strategic cybersecurity coordination forum

Key tasks (NIS 2 Article 14)

- Support harmonised NIS 2 implementation
- Exchange cyber threat intelligence and best practices
- Coordinate EU cybersecurity policies and guidance
- Conduct strategic cyber risk assessments
- Provide guidance to CSIRTs Network and EU-CyCLONe (European cyber crisis liaison organisation network)
- Support peer reviews, exercises and capacity building

Activities organised in thematic workstreams (e.g., security measures, incident reporting, supervision, PQC, digital infrastructure & providers)

Why ECATS joined the Digital Infrastructures & Providers workstream as a dedicated subgroup (2026)

- Trust services no longer isolated legal domain but rather critical “crypto & identity infrastructure” for all other NIS 2 sectors (banking, energy, healthcare etc.)
- Streamline incident reporting under NIS 2 and eIDAS wherever possible
- Align trust service security requirements with NIS 2 risk-management measures
- Strengthen cooperation between NIS 2 competent authorities and eIDAS supervisory bodies to ensure consistent supervision and risk-management practices
- Address the lack of a dedicated trust services focus within the NIS Cooperation Group
- Support cooperation with the European Digital Identity Cooperation Group, including joint activities foreseen under eIDAS 2

Cross-border consistency even more important in the wallet era

Cross-border relevance of trust services, need for consistency even growing

- TSPs typically rely on components provided in different Member States
- TSP may be supervised in one Member State and relied upon in many others
- Incidents may have technical, legal and operational consequences across multiple jurisdictions at the same time
- EUDI Wallet ecosystem increases interdependence between providers, authorities and relying parties
- Shared understanding between competent authorities becomes even more important

ECATS does not centralise powers — it helps build coherence where cross-border effects are real

Issues to shape the next phase of trust services supervision

- **EUDI Wallet ecosystem:** New trust chains, actors, dependencies and incident scenarios
- **Qualified Electronic Attestations of Attributes:** Source reliability, freshness, status management and accountability
- **Coherent incident reporting:** Timely, meaningful communication across overlapping legal frameworks
- **Supply-chain and concentration risks:** Common dependencies and possible single points of failure
- **Cryptographic agility:** Governance and long-term planning for future migration, including post-quantum readiness

Future supervision will increasingly mean ecosystem supervision

ECATS in a changing trust landscape — The evolution of digital trust supervision



Electronic Identification

EUDI Wallet Ecosystem

- Cross-border digital identity
- Interdependent trust chains
- User-controlled attributes



Trust Services

QTSPs including QEAA Providers

- Signatures, seals & timestamps
- Attestation of attributes (QEAA)
- Post-quantum readiness (PQC)



Digital Infrastructure

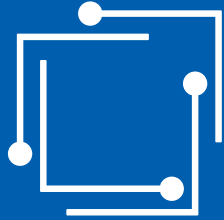
Essential & Important Entities

- Critical sector dependencies
- Supply chain resilience
- Harmonised risk management

Vital foundation: coordinated supervisory cooperation (ECATS)

“If trust services are digital infrastructure, cooperation among competent authorities is a vital foundation of that infrastructure.”

Thank you for your attention!



RTR

We stand for competition and media diversity



<https://www.rtr.at>



@Rundfunk und Telekom Regulierungs-GmbH (RTR)



<https://x.com/rtrgmbh>



Ulrich.Latzenhofer@rtr.at