

# Supervising Trust Services: Balancing Diversity and Harmonisation in Europe

eIDAS 2, NIS 2 and the Future of Digital Trust

Ulrich Latzenhofer  
Split, 24 September 2025

# The role of supervisors

## **In the narrower sense: to ensure that trust service providers meet legal requirements**

- National transpositions of NIS 2 Directive: general cybersecurity requirements (e.g., cybersecurity risk management measures) [competent authorities]
- Amended eIDAS Regulation: specific requirements for TSPs [supervisory bodies]
- GDPR, CER Directive etc.: other related requirements [other authorities]
- Ex-post supervision for all TSPs (e.g., after security breaches),  
ex-ante supervision for qualified TSPs (eIDAS) and essential entities (NIS 2)

## **In the broader sense: supervisors as enablers**

- No (cross-border) recognition of qualified TSPs without (harmonised) supervision
- Supervision as silent backbone of digital trust: If supervision fails, trust is lost

## A major breakthrough

- Bridging of electronic identification and trust services through EUDI Wallet
- Inclusion of related services in notion of trust services (e.g., electronic attestation of attributes)
- Specification of requirements for trust services through implementing acts: long-standing desideratum of supervisory bodies
- Alignment of eIDAS with NIS 2 (e.g., conformity assessment, incident reporting)
- Restoring what would have been lost by NIS 2 (e.g., requirements for non-qualified TSPs)

**However, there are still challenges ...**

## **Long transition period for “other” identification methods (requiring confirmation by conformity assessment body)**

- Old confirmations usually not assuring high level of confidence
- National requirements for verification of identity no longer relevant
- Commission Implementing Regulation (EU) 2025/1566 (ETSI TS 119 461 V2.1.1 as reference standard for verification of identity) not applicable before August 2027
- Considerable discretion of conformity assessment bodies until Commission Implementing Regulation becomes applicable

## **Long transition periods for conformity assessment**

- Standardisation still in progress → Delayed update of accreditation scope
- Some conformity assessment bodies applying outdated standards

## **Supervision of new types of qualified trust services still in development**

- Management of remote SCDs, electronic attestation of attributes etc.
- Criteria for electronic archiving and electronic ledgers yet to be established
- Inclusion in Trusted List not yet possible

## **Different national implementations of NIS 2 Directive**

- Cybersecurity risk management measures (Article 21 of NIS 2 Directive) to be considered in conformity assessment reports
- National cybersecurity requirements possibly beyond those measures
- Security audit under NIS 2 in addition to conformity assessment under eIDAS
- Additional institutions involved → increased complexity of the ecosystem

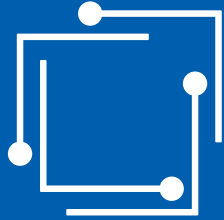
## Transition to post-quantum cryptography

- Speed of progress in quantum computing unclear: Q-Day in 2030, 2035 or 2040?
- Standardisation of PQC algorithms still in progress
- Security of PQC algorithms not as proven as traditional public-key algorithms
- Planning security vs. difficult-to-predict technological aspects
- RSA, ECDSA “deprecated” after 2030, “disallowed” after 2035 (NIST IR 8547 ipd)?
- Qualified certificates often valid for several years
- Standardisation of algorithms → update of agreed cryptographic mechanisms → development and certification of cryptographic modules → integration into systems of TSPs → issuance of certificates, creation of electronic signatures
- Harmonised roadmap to be sharpened with respect to trust services

# Conclusion and outlook

- Supervision: the silent backbone of digital trust
- Transition to a changing ecosystem under eIDAS 2 and NIS 2
- Supervisors striking a careful balance: enabling innovation, ensuring security
  - Cooperating at European level to overcome challenges (FESA, ECATS)
  - Listening to market actors and other stakeholders
  - Preparing today for challenges of tomorrow – from EUDI Wallet to post-quantum cryptography
- ENISA Trust Services and eID Forum: indispensable basis for such a balance

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](mailto:ulrich.latzenhofer@rtr.at)