

# Project Hail Merkle

## Exploring MTCs for European Trust Service Providers

9/30/2026

Transparency.dev Summit 2026, Montreal  
Jan Klaußner, Bundesdruckerei



# European Digital Identity Framework eIDAS



- Certificate Authorities
- Time Stamping Authorities
- Electronic Identities
- Preservation Services
- Signature Services
- Validation Services
- EUDI Wallets

rely on X.509 PKI

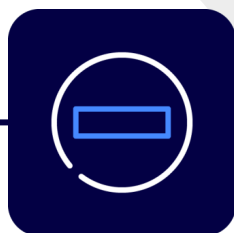
# Painpoints for eIDAS QTSPs



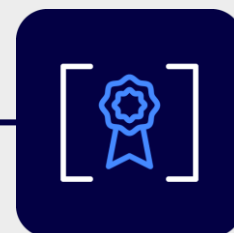
QWACs



Cosigner



Revocation



QES/QSeal



QPres

# MTCs and Qualified Website Authentication Certificate

2-QWAC



Keep qualified identity in the QWAC, move browser-facing TLS toward MTC

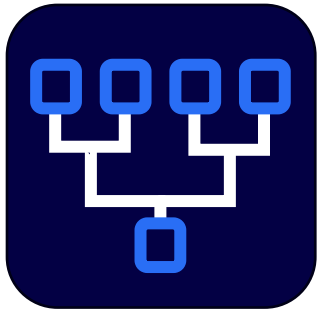
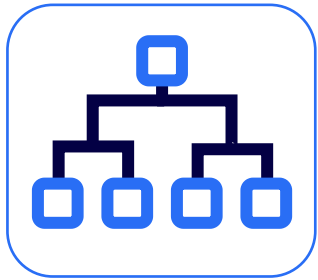
1-QWAC



Needs direct ETSI profiling of an MTC-based qualified TLS cert



# Mirror Cosigner



- currently not needed, **but**
- **1-QWAC** solution probably requires **transparency**
- traditionally via CT-Logs
- now as Mirror Cosigner



# To Revoke or not to Revoke



- Article 24(3): within 24 hours after request
- 24 hour lifetime? unlikely
- again CRL? OCSP?
- looking for more MTCish way → IETF PLANTS WG



# Qualified signatures & seals

## Conceptually still compatible

- Qualified identity semantics can still live in certificate fields and QC Statements
- QSCD indication is extension/policy question, not an MTC blocker
- The sign or seal operation itself does not depend on how issuer proof is encoded

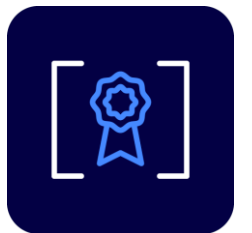
**Signature object still carries a signer certificate — but the evidence bundle grows.**

Signed document / transaction / payload

AdES signature value + signed attributes

**Signer / seal certificate  
plus validation material**

**The incompatibility is not “can I sign?”  
it is “can I prove validity and status  
later?”**



# Preservation – the hard part

Preserving enough state to prove validity years later.

## ETSI preservation model

**Signature / seal object**  
CADES / XAdES / PAdES payload

**Signer certificate**  
plus intermediate and root chain

**Status evidence**  
OCSP and/or CRL data

**Time proof**  
time-stamp and archive renewal

**Validator output**  
path validation report to trust anchor

## What an MTC validator needs

**MTC certificate**  
still X.509-shaped

**Revocation-by-index snapshot**  
not the same evidence object as OCSP / CRL

**Signed checkpoint / tree state**  
what log state was trusted at that time?

**Landmark state, if used**  
part of the proof may live outside the certificate

## Why this is difficult today

- 1 Evidence model gap**  
ETSI LTV archives certificate paths, status evidence, time-stamps, and reports — not inclusion proofs or checkpoints.
- 2 Revocation mismatch**  
Qualified status today means OCSP / CRL style evidence. MTC uses revoked index ranges instead.
- 3 External trust state**  
Landmark mode moves part of the proof outside the certificate, so preservation must capture the trusted state too.
- 4 Renewal scope**  
Archive renewal must protect not only the signed document, but also hashes, checkpoints, cosigners, and log state.



# Action!



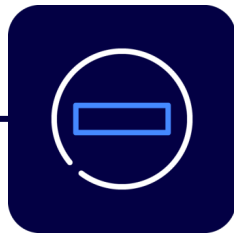
**2-QWAC**

**Pilot  
now**



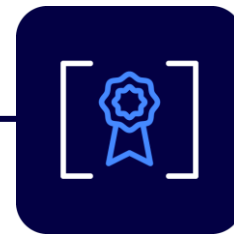
**Cosigner**

**Pilot  
now**



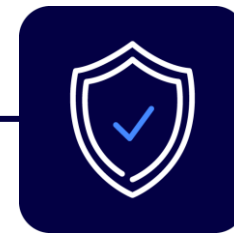
**Revocation**

**Research**



**QES/QSeal**

**Pilot  
now**



**QPres**

**Research**

**1-QWAC**

**Profile  
first**

**Bottom line: MTC is promising for eIDAS services, but revocation and long-term preservation needs a new ETSI evidence profile before qualified production use.**

# Thank You

**Jan Klaußner**

Bundesdruckerei GmbH  
Innovation  
E-Mail: [jan.klaussner@bdr.de](mailto:jan.klaussner@bdr.de)

Please note: This presentation is the property of Bundesdruckerei GmbH. All of the information contained herein may not be copied, distributed or published, as a whole or in part, without the approval of Bundesdruckerei GmbH.

© 2026 by Bundesdruckerei GmbH.