Trust management in the EUDI Wallet ecosystem

~12 minute overview with Giuseppe De Marco, *Technical Project Manager - Dipartimento per la trasformazione digitale, Presidency of the Council of Ministers of Italy*

Session 3: ITU Workshop on "Trustable and Interoperable Digital Identities for Human and Agentic AI", (Geneva, Switzerland, 30–31 March 2026)

2. eIDAS Trust Infrastructure Topics

1. **Awareness**... Trust management is a cross-cutting concern
2. **Governance**: Member States, European Commission, Certification Bodies, Standardization Bodies, Specific Sector Schemes
3. **Framework**: eIDAS uses an *Authoritative Listing* with PKI continuity and specific purpose extensions
4. **Enrollment**: registrars, accreditation, certification, notification mechanisms, activation of participants through publication within the Authoritative Lists (Trusted Lists)
5. **Runtime**: digital signature, timestamps, issuance, presentation, user-visible assurance
6. **Assurance & lifecycle**: **certification schemes** (**issuance**, **lifecycle**, **interoperability**), Trust Mark, revocation

*Both Trust and Scalability are about **risk** and **cost reduction**, a Trust that scales compounds its value!*

3. Trust in eIDAS Wallet: requirements and specifications

Sources	Kind	Count
ARF Annex II — high-level requirements whose specification directly affects **trust evaluation** (trusted lists / LoTE, registration, access & registration certificates, revocation, verifier behaviour); WP4 Task 2 *Trusted Lists, Registration & Trust Evaluation* matrix (ARF v2.8.0)	Requirements	**133** unique ids
ARF main document — each **own row** in the ARF *References* table for a standard or protocol (ISO, ETSI, RFC, W3C, OIDF, …)	Specifications	**44**
ARF Wallet TS1–TS11 in ARF v.8.0 `docs/technical-specifications/`	Specifications	**11**
Public roadmap — *Standards and Technical Specifications* (**STS**); GitHub tracker (see `docs/technical-specifications/README.md`) covering several SDOs (ISO, IETF, ITU, OpenID, W3C, ETSI, CEN/CELEC)	Specifications	**~200** tracked; **~34 essential** for the Wallet

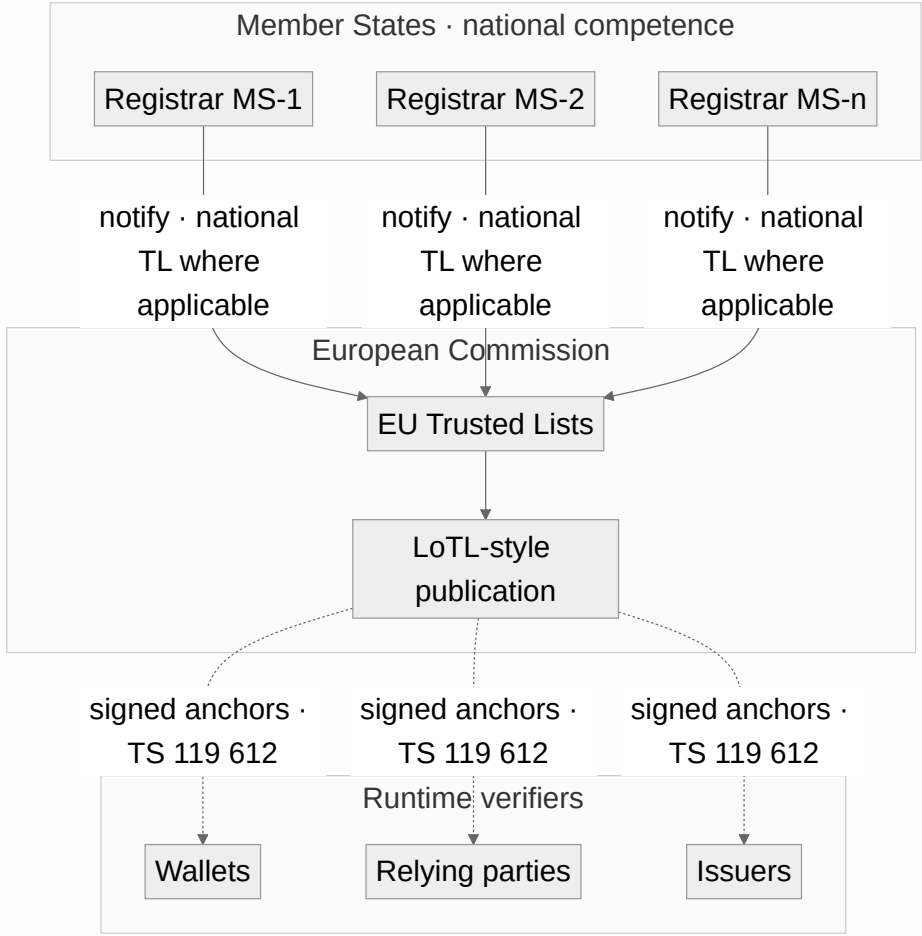
** EU acts and CIRs are not counted in this slide for technical purpose.*

4. eIDAS: national registration → EU lists → runtime verifiers

Many independent **actors**.
No EU-wide single “login authority”.
Shared rule and semantics inside the same interoperability patterns.

1. **Participants Enrolling / Onboarding / Registration**
2. **Notification** to the Root of Trust, the EU Commission
3. **Publication** and Participants **lifecycle**
4. **Usage**, mutual trust evaluation
5. **Dispute resolution** and regulated administrative security framework

Trust is the product of framework establishing registration, crypto,
published anchors and supervision.



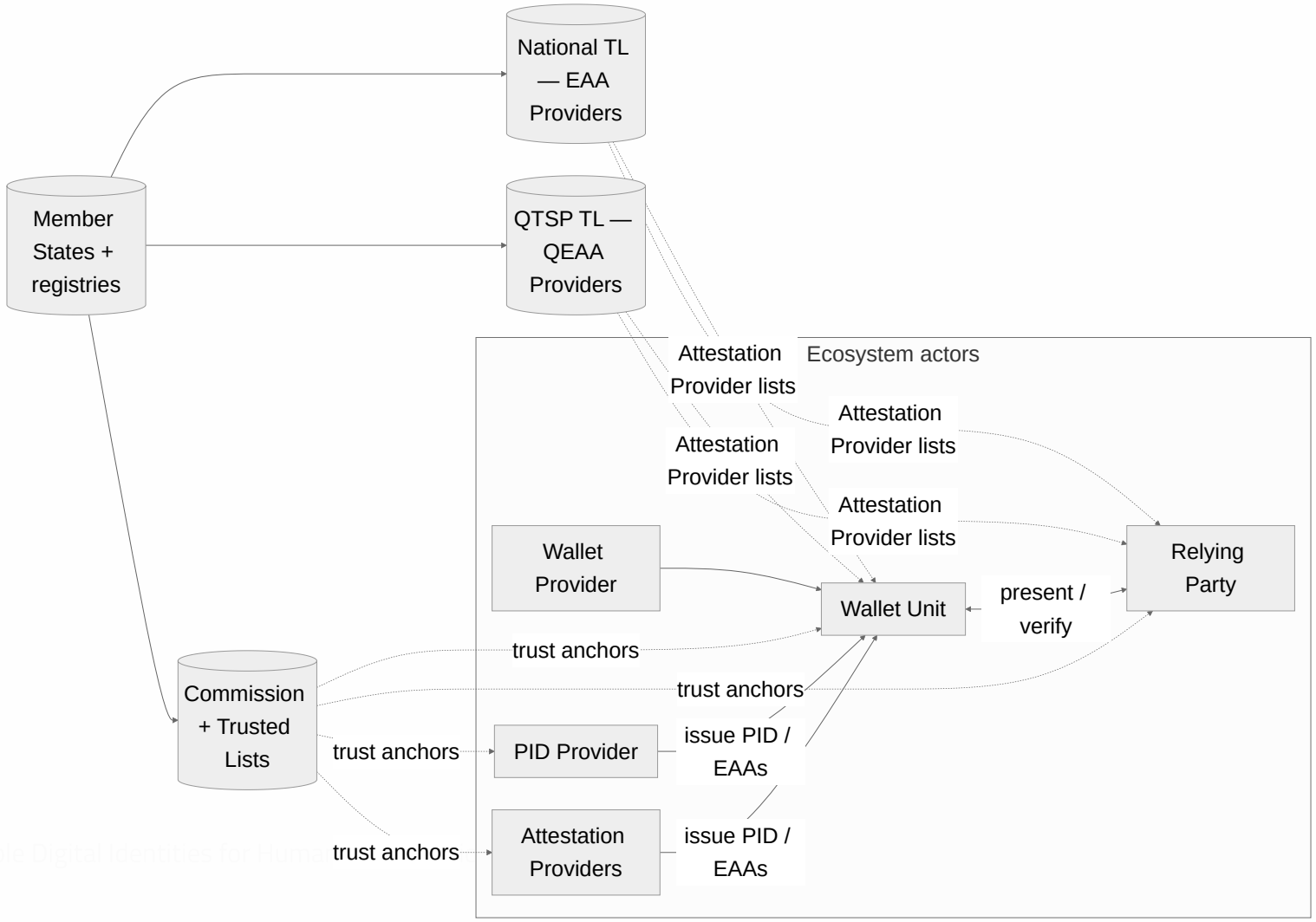
5. eIDAS Trust Infrastructure Responsibilities matrix

Trust evaluation depends on both who registers and who publishes.

Entity type	Registration	TL compilation (EC / MS TLP)	MS TLP role
PID Provider	MS **Registrar**	**European Commission** (EU PID TL)	None
Attestation Provider	MS **Registrar**	**MS TLP**: QTSP TL (QEAA); national TL (non-qualified EAA); **PuB-EAA** → **EC** TL	Compiles / signs / publishes national TLs; notifies EC
Wallet-Relying Party	MS **Registrar**	**N/A** (WRPAC; **not** EC/MS TL)	**MS** runs national registry + **ARF TS5** machine-readable format & API
Wallet Provider	*Notification only* (MS → EC)	**European Commission**	Evaluates certification and compliances
WRPAC Provider	*Notification only* (MS → EC)	**European Commission** (WRPAC / Access CA LoTE)	None (MS notifies EC; **no** MS TL for this role)
WRPRC Provider	*Notification only* (MS → EC)	**European Commission** (Provider of reg. certs LoTE)	None (MS notifies EC; **no** MS TL for this role)

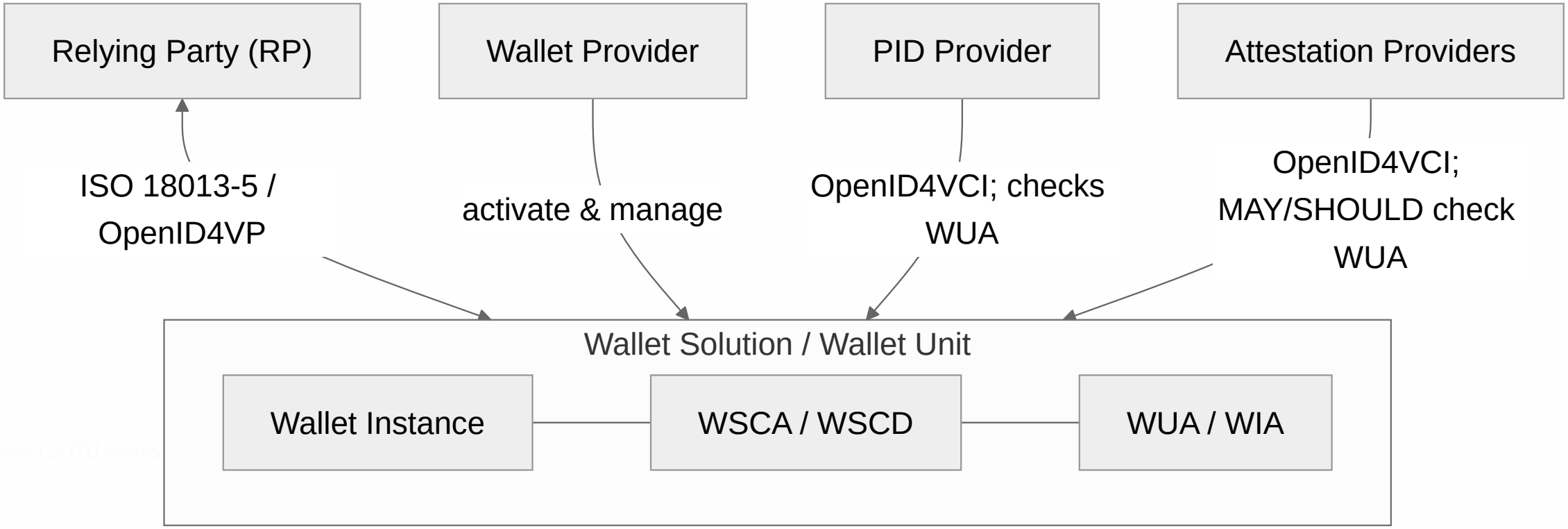
6. Does everything fit within it?

- **Duplication**: one **entity** playing multiple roles (QEAA+PubEAA Provider+RP) requires **separate trusted-list appearances**, **revocations** must stay consistent everywhere.
- **Verifier burden:** the Wallets/RPs must **resolve identity across different lists**. Possible **trust drift**.
- **Domestic Gaps:** PID/PubEaa/Wallet Solutions Trusted Lists are only hosted by EC, MS may implement other approaches.



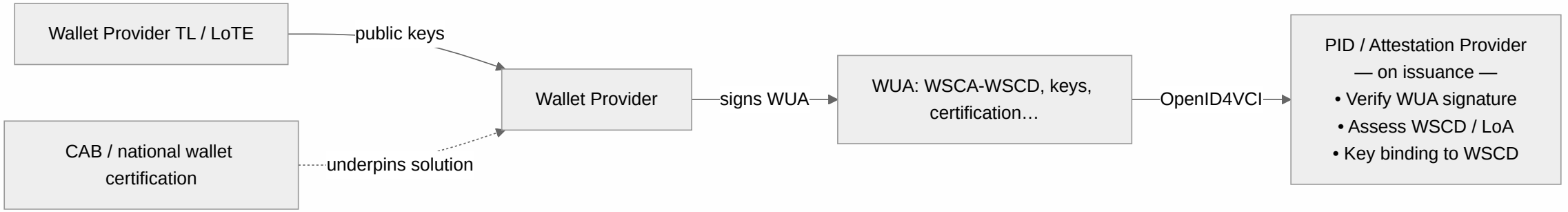
7. Wallet Architectures under the spotlight

Wallet Providers provide one/more **Wallet Solution(s)**. Each **Holder** (Wallet User) use a **Wallet Instance**, this includes **Wallet Unit** along with **WSCA/WSCD**, and **keystores** for non-critical crypto. **Wallet Unit Attestation (WUA)** and **Wallet Instance Attestation (WIA)** are presented to **PID / Attestation Providers** when requesting a PID or attestations.



8. WSCD trust evaluation challenges

- EC Trusted Lists contain **Wallet Providers**, not each single **WSCD** Trust Anchor.
- **WUA** = signed **certification** evidences, and **public cryptographic keys**, to be included in PID/EAA. Credential Issuers **checks** on their own according to associated WUA certification schemes, not a **Trusted List per chip**. **No** central, verifiable, WSCD vendor list.

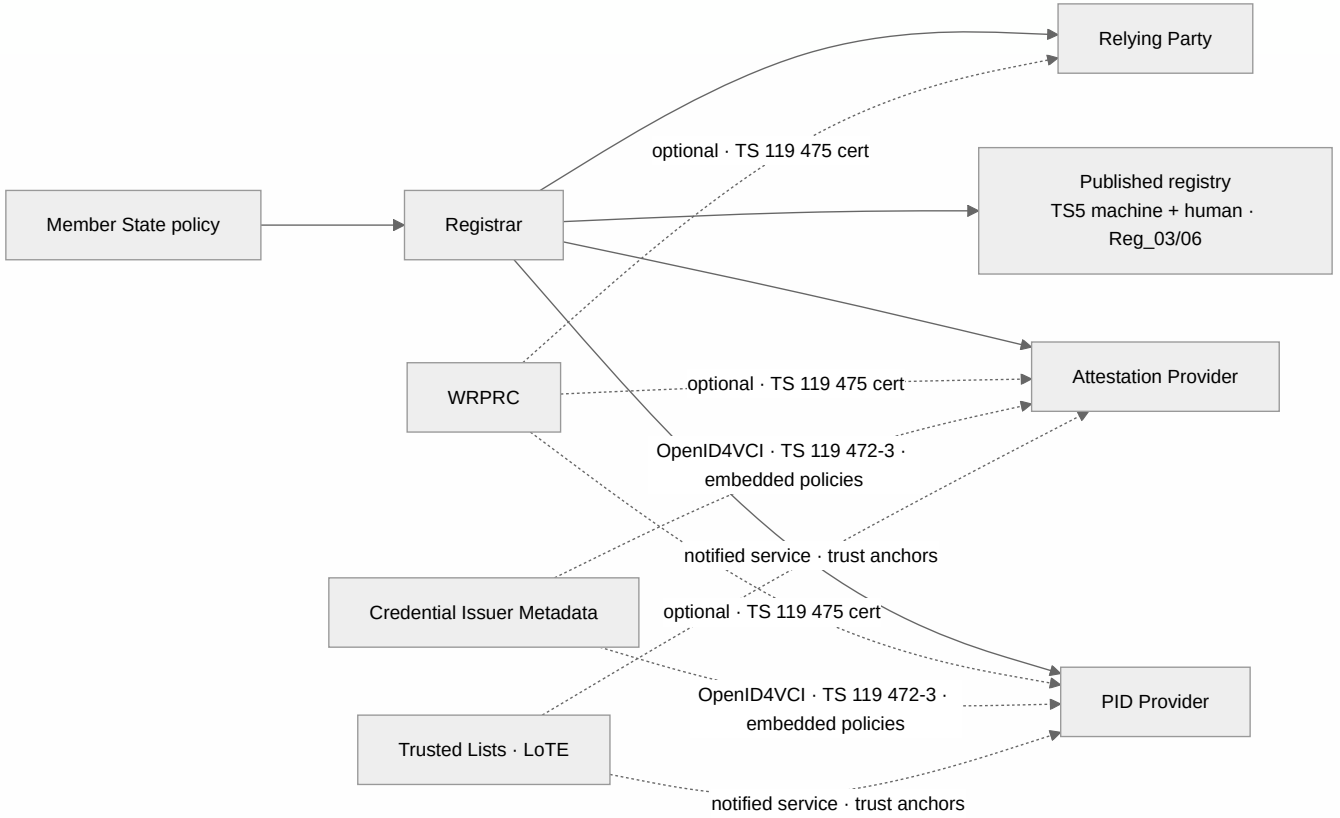


9. Policy Framework — Fragmentation and Overlaps

- **Registration Certificates**: **MS Registrar** may issue **registration certs** (**TS 119 475**) **or Embedded Policies** (**TS 119 472-3** Metadata members `entitlement` / `providesAttestations` not defined in OpenID). **RP** presentation may hint, only **Registrar RP API** is authoritative.
- **PID / Attestation Providers**: **TL** + **LoTE** — notified **who** may issue and **trust anchors**.
- **Registrar policy is national**: each **Member State** runs **its own** Registrar **rules—no** EU **central authority** that issues or harmonises those **registration policies**.
- **No shared "domestic" compliance across MS**: policies and safeguards anchored in **one** Registrar **do not** make an actor **automatically compliant** with **another** MS's Registrar regime; beyond **common specs** (ARF, TS, legal acts), there is **no** single **ecosystem-wide protection** or procedural baseline.

Is there a General Policy Framework definition? Subtractive/Additive-ZeroTrust approaches? *"everything allowed until filtered"*, always overridable by User.

10. A Picture of eIDAS Policy Issuance, Discovery, and Evaluation



11. Multiple Trust Sources for one Relying Party

RPs make wallets to juggle on the **presentation** path along with **five distinct trust sources**.

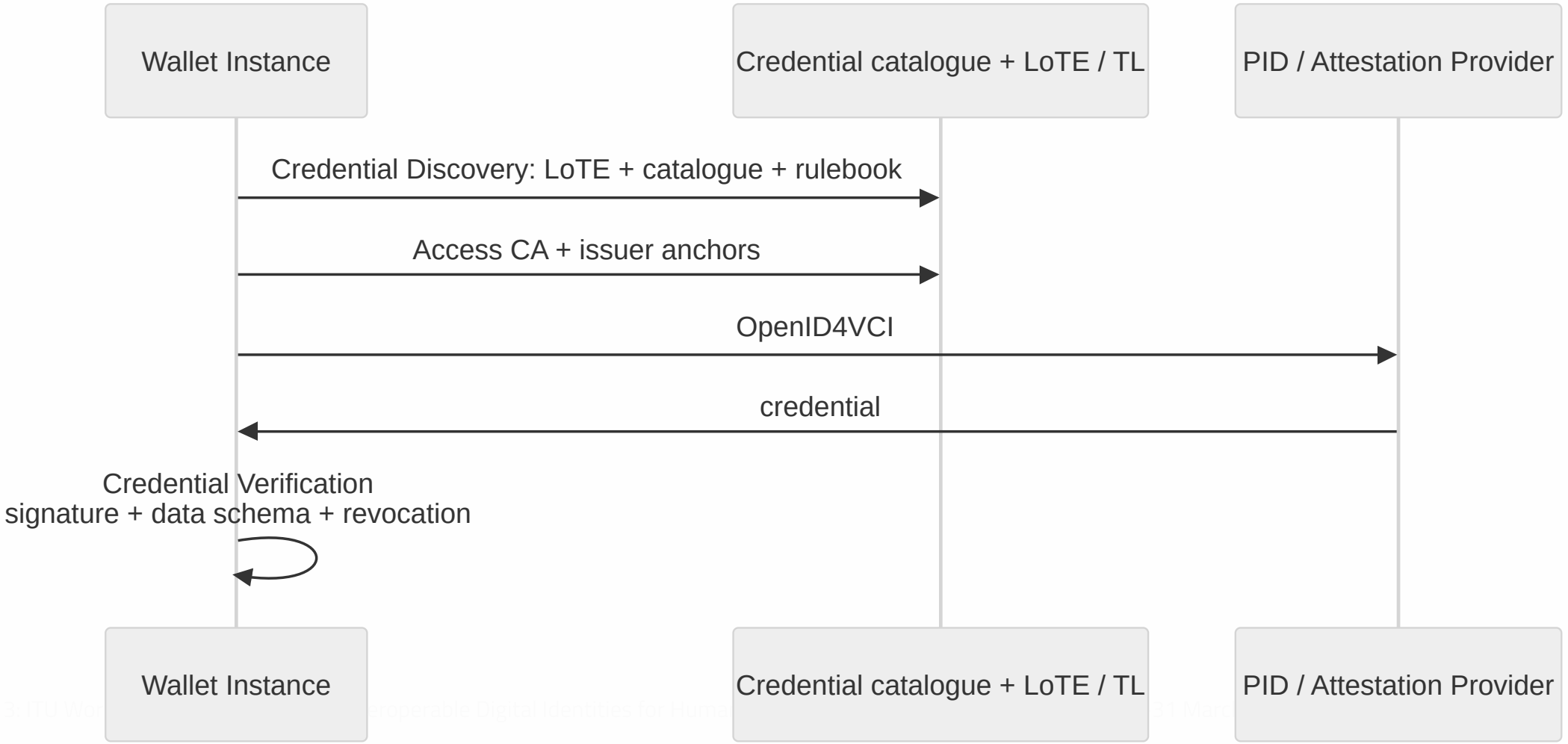
#	Surface	Example
1	**Protocol / transport trust**	**One** RP **access** (or TLS) **certificate** — path validation against **RP Access CA** trusted material.
2	**Revocation / freshness**	**One** (or few) **revocation endpoints** — **OCSP/CRL** (or stapled) so the access cert is still **valid now**.
3	**Registration / entitlement**	**N registration certificates** — possibly **several** for attributes, scopes, or sector registers.
4	**Status of those registrations**	**Multiple status lists** (or status services) — **WRPRC**, sector lists, **Registry** snapshots — not one check.
5	**Discovery API**	**One registration API** (or **Registry**) to **resolve** what the RP is allowed to ask when something is not in-band.

12. Pre-existing/parallel trust frameworks & sector-specific stacks

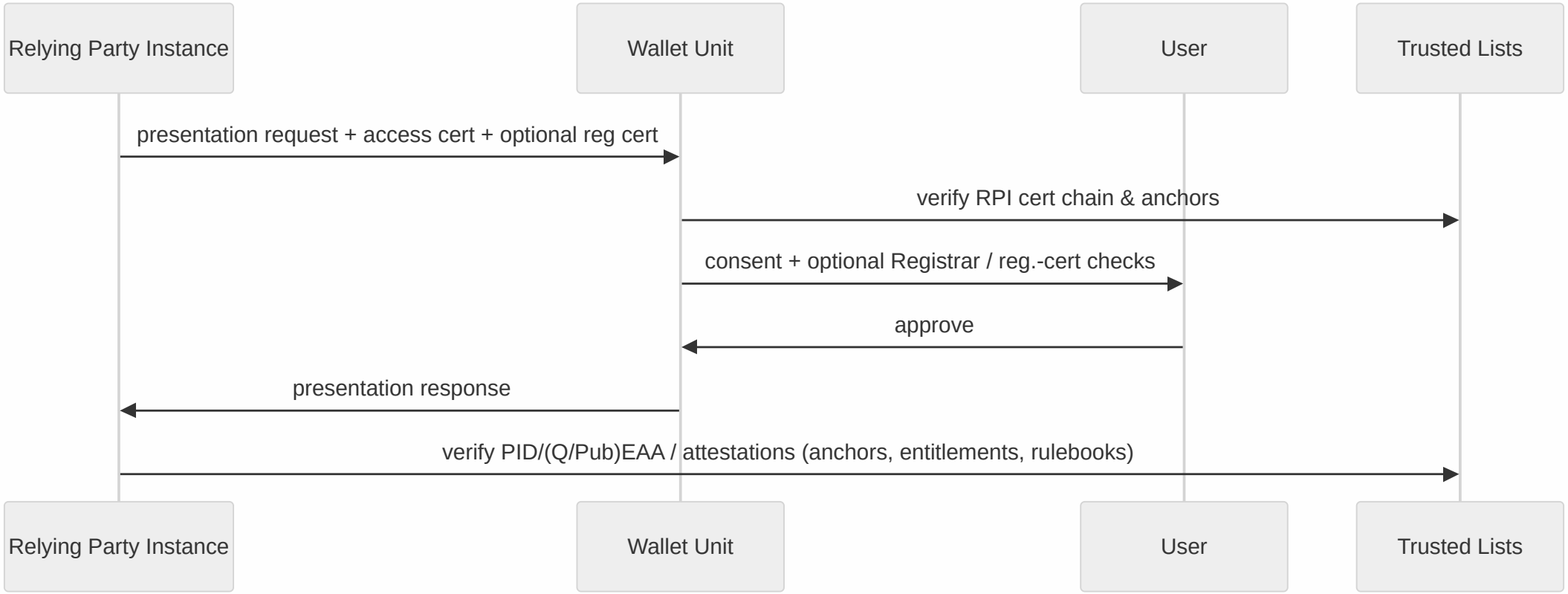
- **Legal**: **EUDI** amends **eIDAS**; **qualified artefact paths** still use **QTSPs**, **qualified certs**, **EU trusted lists / TSP**.
- **Technical** (**§6.1**): **X.509** for PID, QEAA, PuB-EAA, access/registration certs; wallet lists follow **TS 119 612 / LoTL** (same family as trust-service lists).
- **Deployment**: Member States may use **several CAs** or **reuse** national PKI / practice as **Access CA / Registrar**.
- **Non-qualified EAA** can follow **other trust models** (not only EU-wide PKI lists).

Many wallet-relevant sectors already run **parallel trust infrastructures** (e.g. **banking**, **eProcurement / eInvoicing**, **G2G evidence reuse**, **data spaces**) with **their own** CAs, registers, status services, and APIs (Peppol PKI, OOTS, iSHARE). Without **explicit** per-sector integration, implementations risk **duplicated validation**, **extra round-trips**, and **opaque** “which list wins?” behaviour.

13. Trust when issuing credentials



14. Trust when presenting to relying parties

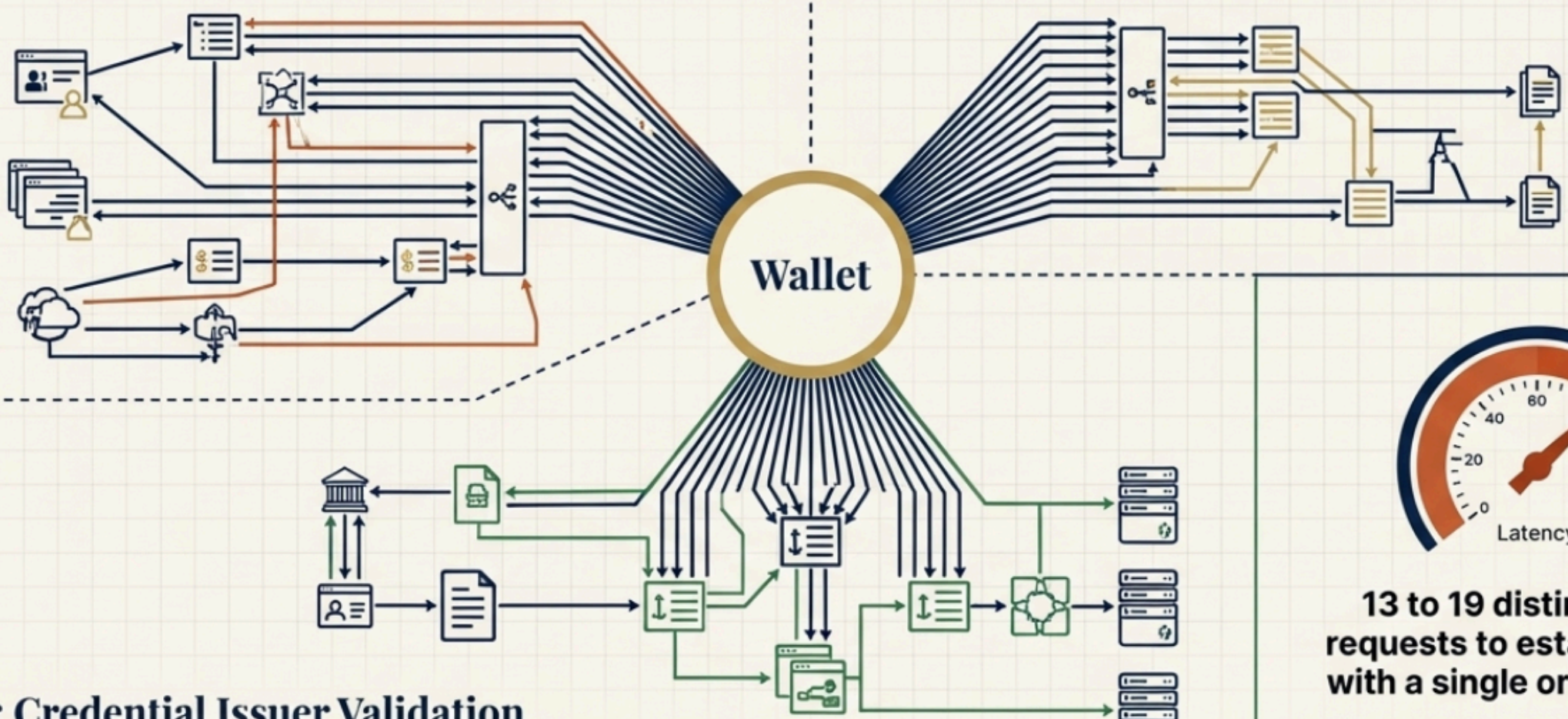


Path A: Relying Party Validation

5-7 requests (WRPAC, WRPRC, National Register).

Path B: QTSP Validation

2-3 requests (TSL lookup, certificate chain).



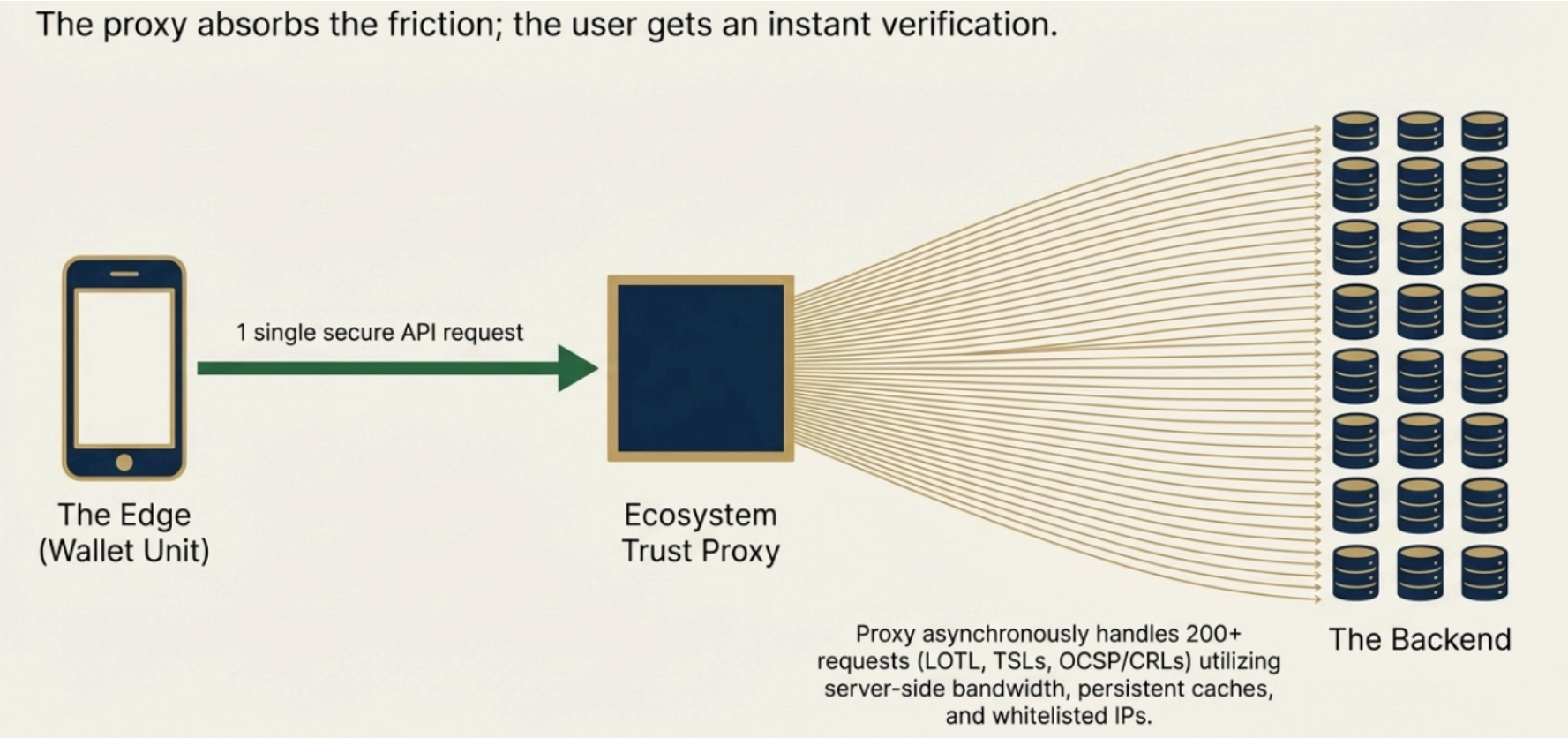
13 to 19 distinct HTTP requests to establish trust with a single organization.

Latency spikes to ... seconds if executed sequentially.

Path C: Credential Issuer Validation

2-4 requests (Issuer metadata, authorization server discovery).

15. Trust proxy — any privacy concerns?



16. Not discussed today (for time)

- **Certification schemes — issuance, lifecycle, interoperability**: how **NAB/CAB** and **national** schemes **issue** and **maintain** approvals for wallet solutions and QTSPs; **lifecycle** (surveillance, renewal, withdrawal); **cross-scheme** / **cross-border** recognition of conformity evidence and practical **interop** between schemes—only hinted on slide 8 (WUA schemes), not unpacked here.
- **Lifecycle & revocation operations**: how **LoTE/TL updates**, **access-certificate** revocation, **credential/attestation** revocation, and **WUA** revocation (**ARF Topic 38**) line up; **WURevocation_12** (PID Provider verifies who may request wallet revocation); **suspension** and **cancellation** in registers and lists.
- **Operational conformity & supervision**: **audit** programmes, ongoing **supervisory** practice, and **scheme** conformity—only named above, not walked through.
- **End-to-end sector paths**: **rulebook** governance, sector **topology** figures, and concrete **Peppol / OOTS / iSHARE**-class integrations (slide 12 only flags the need).

Thank you

Questions?