

Mapping Decentralised Trust to the PKI/CA Model

Options: ETSI TS 119 612 Trusted Lists · ToIP TRQP v2.0 · OpenID Federation 1.0

Each row is one PKI/CA primitive; the columns show its equivalent in each model.

PKI/CA primitive (centralised baseline)	ETSI Trusted Lists	ToIP TRQP v2.0	OpenID Federation 1.0
Root of trust / pre-trust — Self-signed Root CA in the verifier's root store.	EU List of Trusted Lists (LOTL); verifier pre-trusts the Commission-published LOTL signing keys.	Query interface agnostic to the underlying ecosystem's root of trust	One or more Trust Anchors the verifier pre-configures; each anchor's signed statements are the root.
Authority hierarchy — Intermediate CAs signed beneath the root.	Two fixed levels: LOTL → national Trusted List → listed TSP services. Jurisdiction-scoped.	Recognition queries: one authority recognises another; a peer registry-of-registries, not only a tree.	Intermediates issue Entity Statements; multi-level chains; an entity may sit under several anchors.
Identity-key binding ("the certificate") — X.509 end-entity certificate.	A listed service entry (identity + status) pointing to the TSP's certificates; the list curates status.	An authority statement: "Entity X holds Authorization Y under Framework Z."	A signed Entity Statement / Configuration (JWT) carrying keys, metadata and policy.
Conveyance (how the verifier obtains it) — Certificate presented in-band; roots pre-installed.	Verifier pulls and parses a signed XML list (XAdES) on a cadence; offline-friendly snapshot.	Verifier queries a registry endpoint at decision time; read-only REST/HTTPS (OpenAPI 3.1.0).	Verifier fetches signed JWT statements over HTTPS at runtime and builds a Trust Chain.
Chain / path validation — Verify a leaf→root chain; enforce constraints.	Verify the list signature, then confirm the service is listed and "granted" at the relevant time.	Not in the query; the bridge to the system of record proves it. TRQP standardises the question, not the proof.	Resolve a Trust Chain of Entity Statements to the anchor, applying policy at each hop.
Revocation / status / freshness — CRL and OCSP (RFC 5280 / 6960).	Status value + history in the list; freshness bounded by the "next update" cadence.	Freshness is the live query itself; time passed as query context.	Short-lived signed statements re-fetched over HTTPS; Trust Marks convey qualification.
Governance / audit — CA/Browser Forum; WebTrust / ETSI audits.	eIDAS supervisory bodies; basis CID (EU) 2015/1505, amended by (EU) 2025/2164.	Each ecosystem's published governance framework defines authorities and actions; TRQP stays neutral.	Federation operator policy, enforced technically as metadata policy along the chain.

Net. The three are complementary layers, not rivals. OpenID Federation 1.0 is the closest dynamic re-expression of the PKI hierarchy (Trust Anchor ≈ root, Entity Statement ≈ certificate, Trust Chain ≈ path validation, just resolved live as JWTs); ETSI Trusted Lists is the supervised curated-list variant; TRQP is a read-only query seam that can sit above either (it bridges to X.509 and OpenID Federation).

References

ETSI TS 119 612 v2.4.1 (2025-08), Trusted List v6, mandatory in EU from 29 April 2026.
ToIP TRQP v2.0 (Trust Over IP / LF Decentralized Trust); REST/HTTPS over OpenAPI 3.1.0;
OpenID Federation 1.0 (OpenID Foundation) Final Specification, Feb 2026.
PKI baseline: IETF RFC 5280, RFC 6960; eIDAS Reg. (EU) 910/2014 Art. 22.