Tinexta infocert.

Think Next, Trust Now.

ITU-T workshop 2/6/2026

EU and ETSI Verifier Authentication & Registries

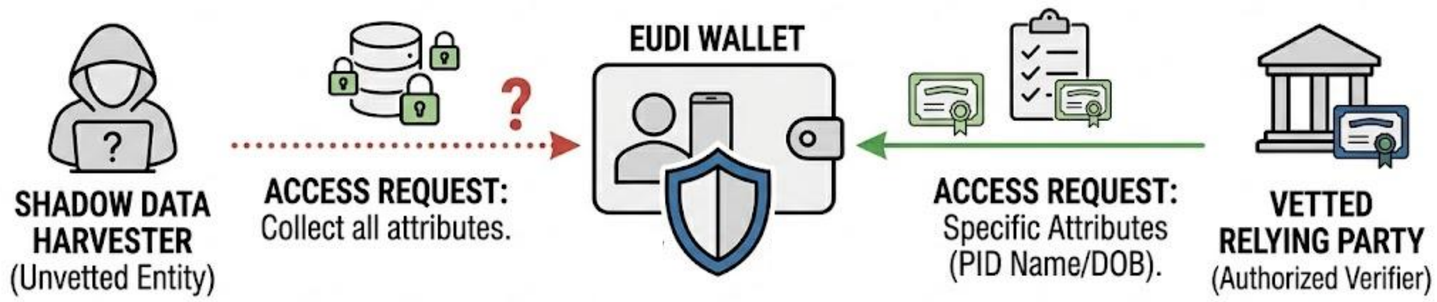
tinexta
infocert

Agenda

1. Framing the problem: how to trust a verifier
2. Verifier registration process
3. Verifier validation process
4. Remarks and open issues

tinexta infocert

Trust the Verifier



Protecting the citizen from data harvesters → only "vetted entities" can ask data.

Two trust questions:

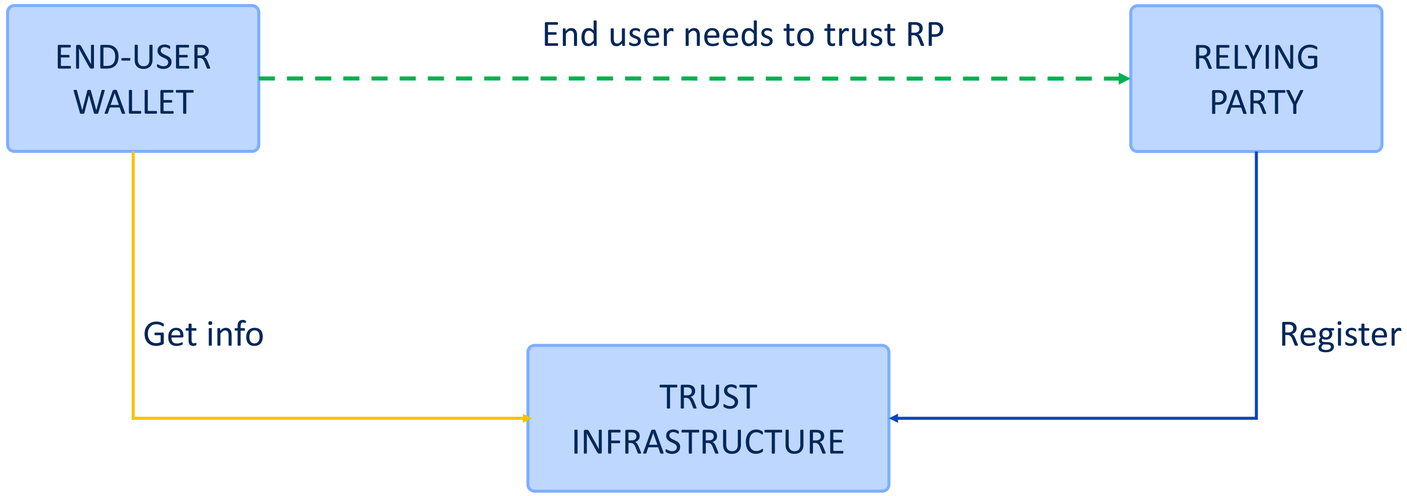
- **Verifier, WHO are you?** (are you an authorized verifier?)
- **Verifier, WHAT may you ask for?** (what are you entitled to ask for?)

tinexta
infocert

Trust the Verifier

This talk will cover:

(1) registration process + (2) verifier validation process

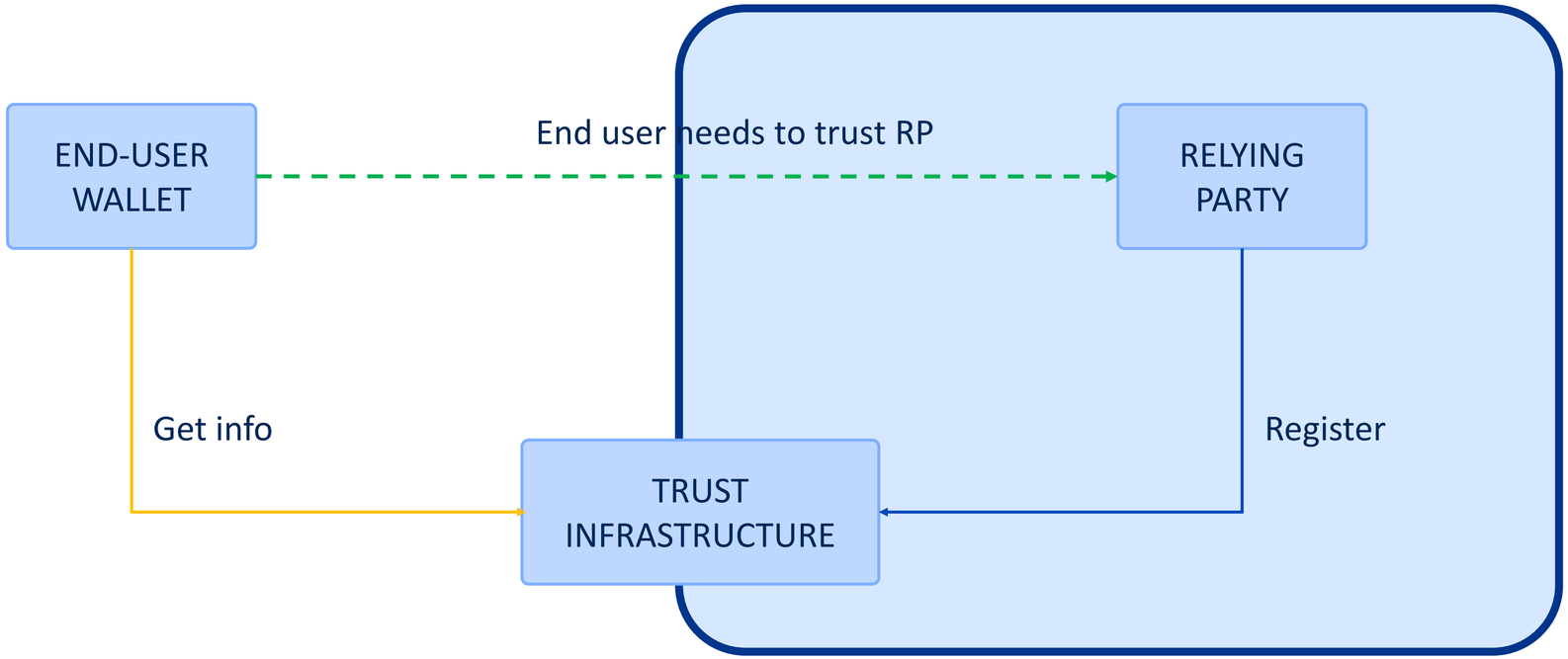


tinexta
infocert

Trust the Verifier

This talk will cover:

(1) registration process + (2) verifier validation process

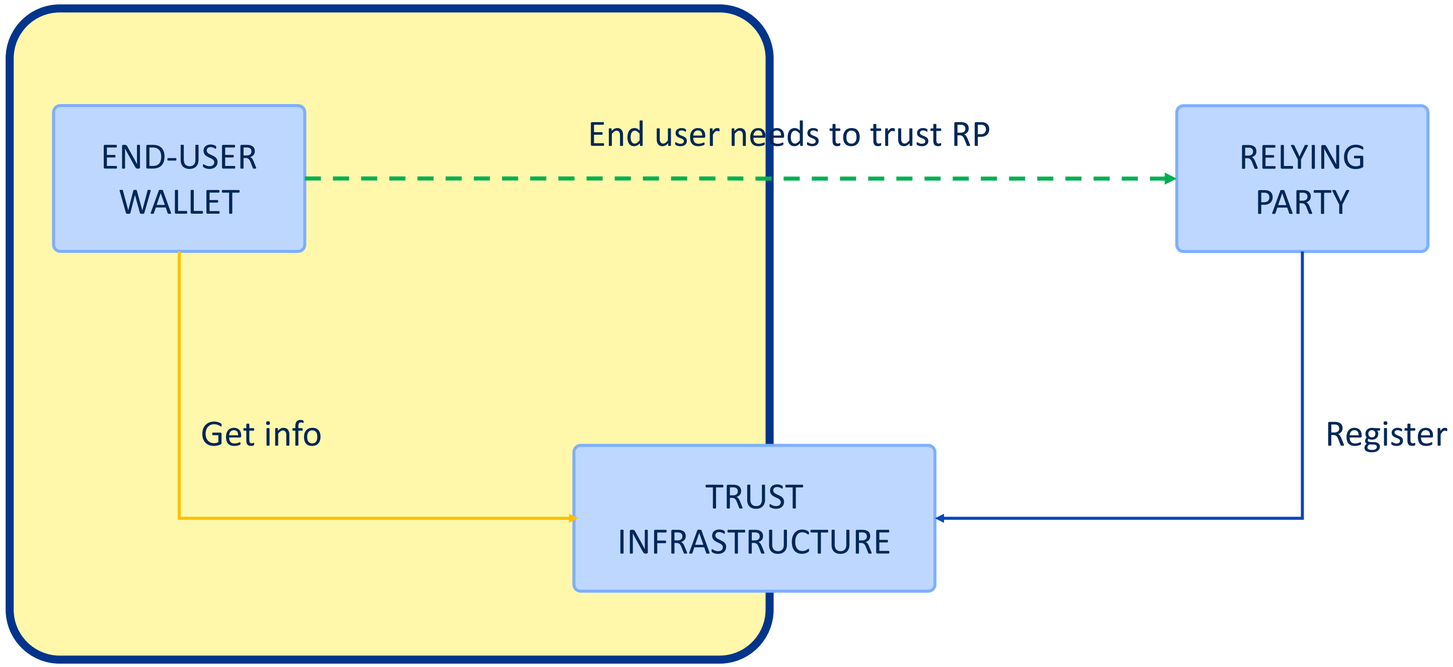


tinexta
infocert

Trust the Verifier

This talk will cover:

(1) registration process + (2) verifier validation process



tinexta
infocert

The legal & standard pillars

CIR 2025/848 (applies from **24 Dec 2026**)

ARF topic x-rr (RP data and format) → ETSI EN 319 475 (work in progress)

ARF ts-5 (API specification) → ETSI EN 319 486 (work in progress)

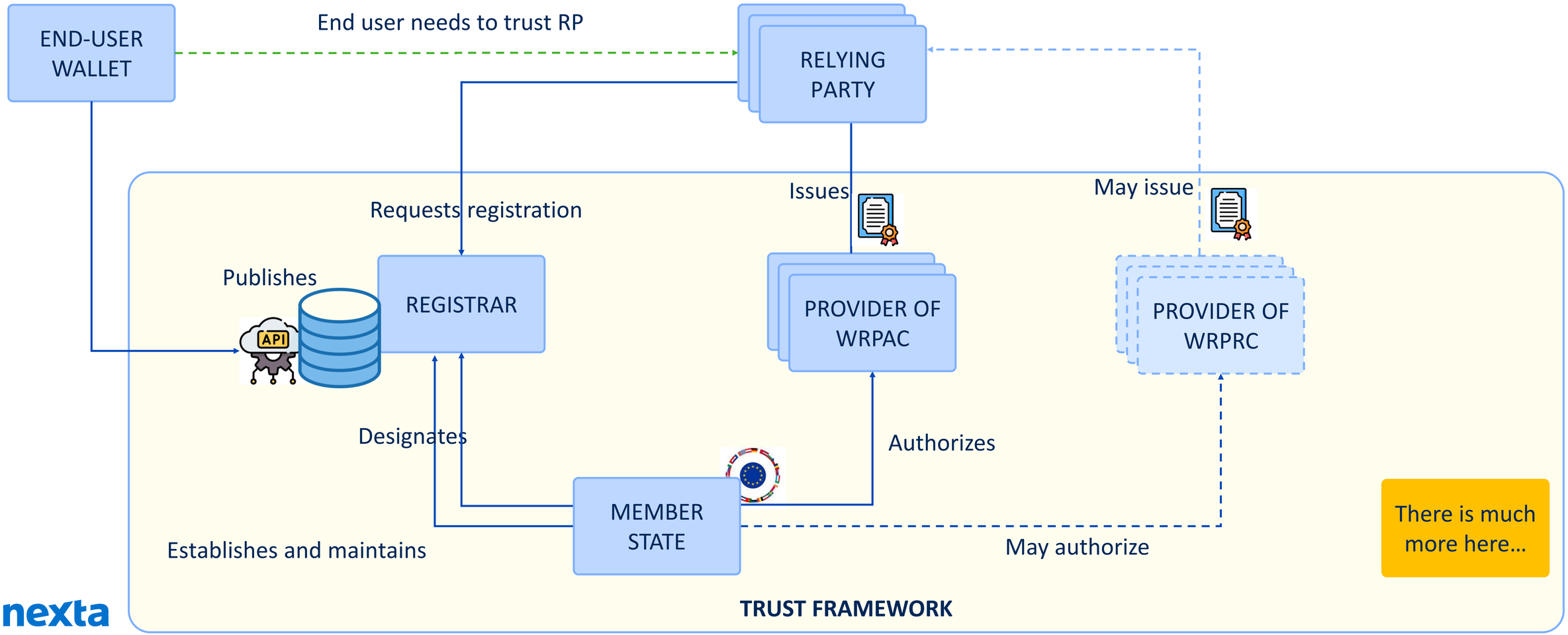
ETSI TS 119 411-8 (policies for RP certificates)

In the following:

- WRPAC: Wallet Relying Party Access Certificate
- WRPRC: Wallet Relying Party Registration Certificate

tinexta
infocert

Exploding the trust framework



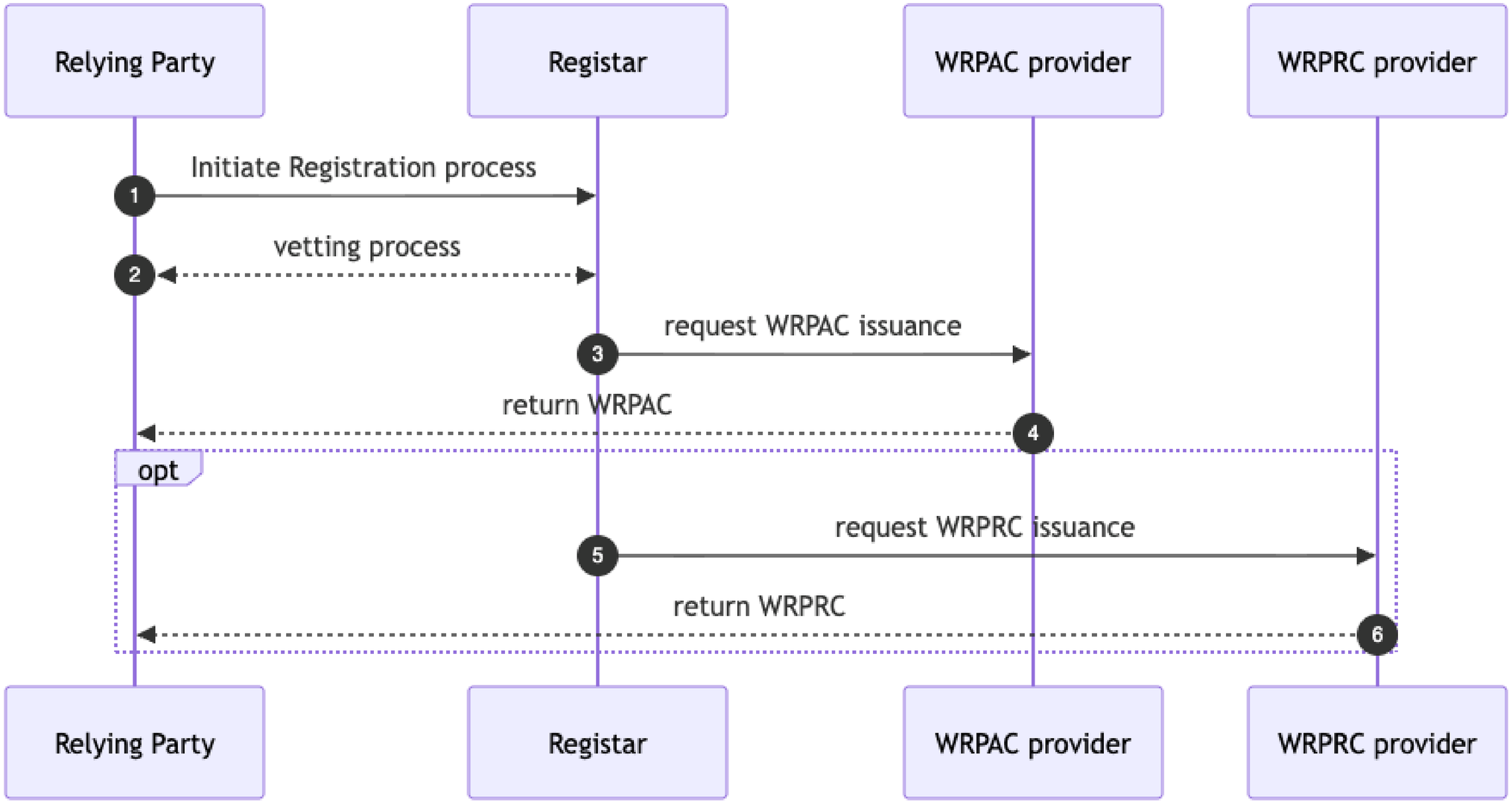
tinexta infocert

Agenda

1. Framing the problem: how to trust a verifier
2. Verifier registration process
3. Verifier validation process
4. Remarks and open issues

tinexta infocert

Registration process



tinexta
infocert

Registration process

Vetting process requests the following info:

- Legal person information
- List of offered services
- Entitlements (Service Provider)
- Attributes requested for each service
- is intermediated? (is the Service Provider intermediated by a technical provider acting on its behalf?)

Registration procedures

Member States publish **registration procedures** for relying parties based on principles defined in Implementing Regulation (EU) 2025/848:

- Non-Discriminatory Access
- Proportional Friction
- Identity Anchoring
- Entitlement Cross-Checking
- Purpose Limitation & Data Minimization
- Continuous Enforcement and Offboarding

Registration must be **efficient and scalable**

- Registrars provide **electronic / automated registration processes**
- Automated checks encouraged (records, powers, entitlements)
- Registrars may suspend/cancel if info is inaccurate, policy non-compliance, or oversharing request

tinexta
infocert

Registration process

At the end of registration process:

- The verifier is included in the register
- Verifier authorizations (what it can ask for) are listed on the register
- Veifier holds an access certificate
- Verifier may hold a registration certificate

Certificates

WRPAC (access certificate): authenticates the relying party to the wallet

X.509 format (specification in ETSI EN 319 475)

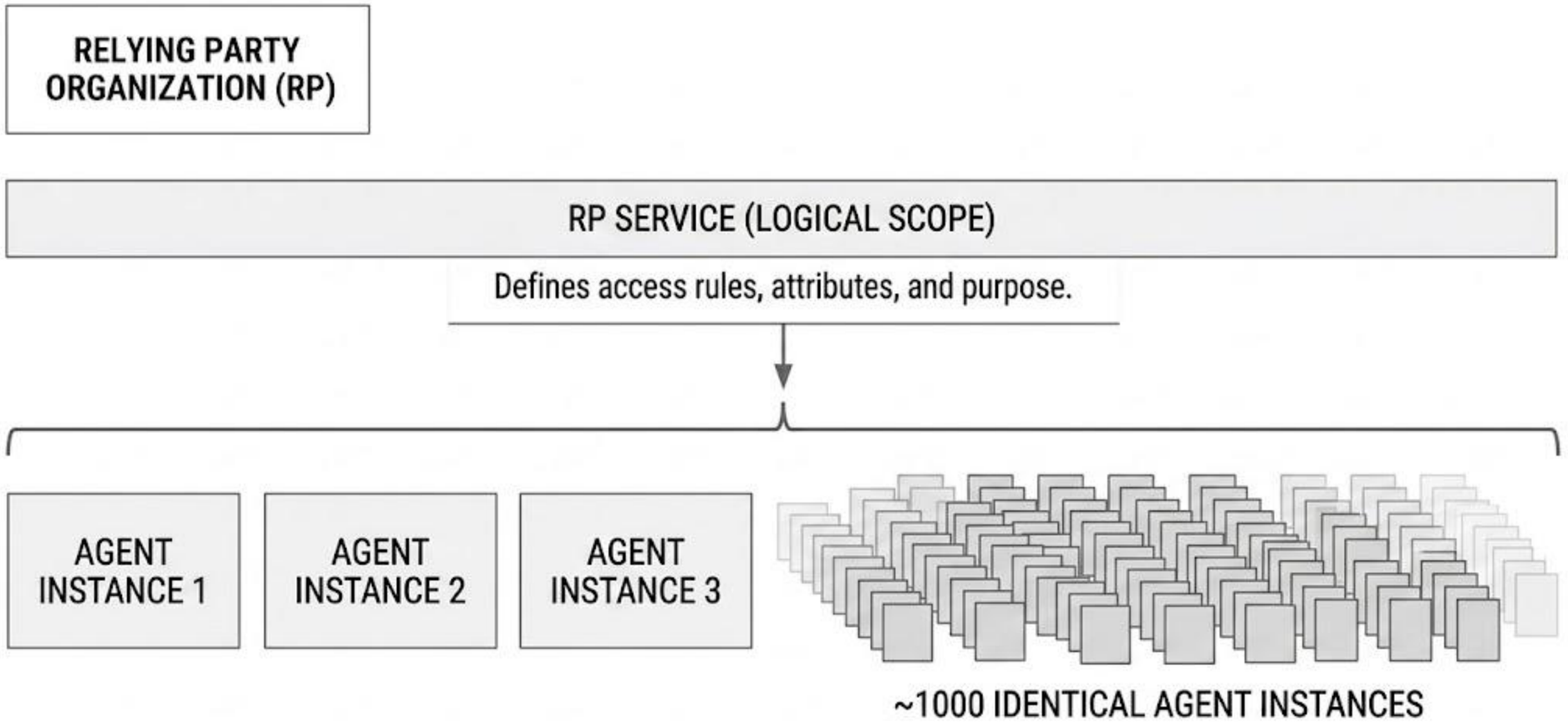
WRPRC (registration certificate, optional per MS): expresses intended use + authorized attributes

JWT or mDOC format (specification in ETSI EN 319 475)

WRPRC intended to act as a “cache”

tinexta
infocert

One RP, many services and instances



tinexta infocert

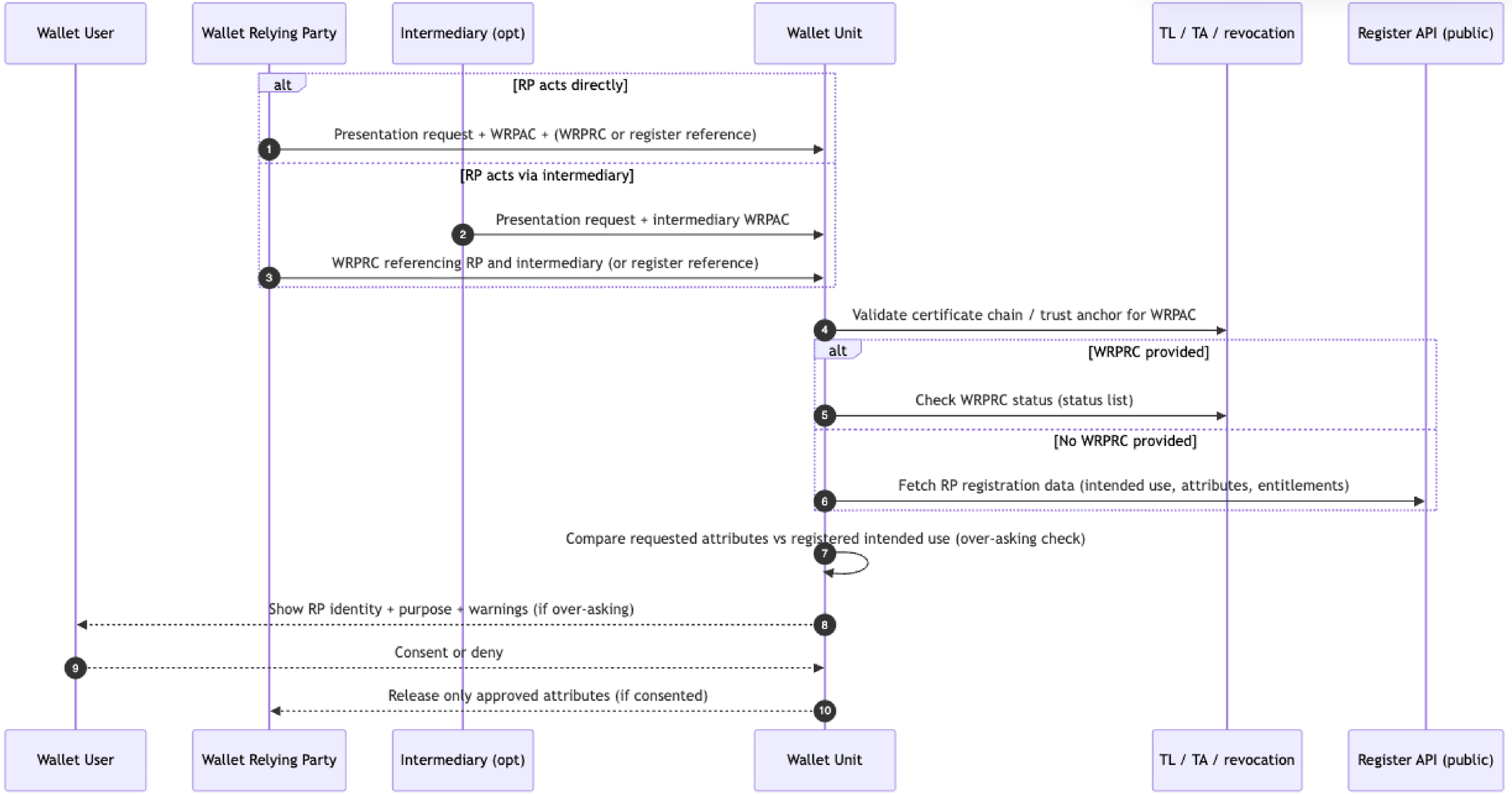
See topic x-rr discussion

Agenda

1. Framing the problem: how to trust a verifier
2. Verifier registration process
3. Verifier validation process
4. Remarks and open issues

tinexta infocert

Validation process



tinexta infocert

Embedded disclosure policies

EAA providers can constrain disclosure of EAA they issue. Wallets verify policy compliance and informs user of result

- ‘No policy’ – disclose to all
- ‘Authorised relying parties only policy’ – only disclose to RPs explicitly listed RPs
- ‘Specific root of trust’ - only disclose to RPs derived from a specific root

Still unclear if user can bypass…

WRPRC vs. register access

Both modes require, at some point, **online access to a service for RP validation**

- Access to registry
- Access to CRL/OCSP for revocation check

Certificates acts as a “cache”

- For CRL: no need to access at each validation
- expiration of WRPRC in discussion – from one day to one year…

Aditional interfaces for the wallet

Common interface for lodging complaints to DPAs (EN 319 482-1)

Common interface for data deletion requests to Relying Parties (EN 319 482-2)

tinexta
infocert

Agenda

1. Framing the problem: how to trust a verifier
2. Verifier registration process
3. Verifier validation process
4. Remarks and open issues

tinexta infocert

ISSUES

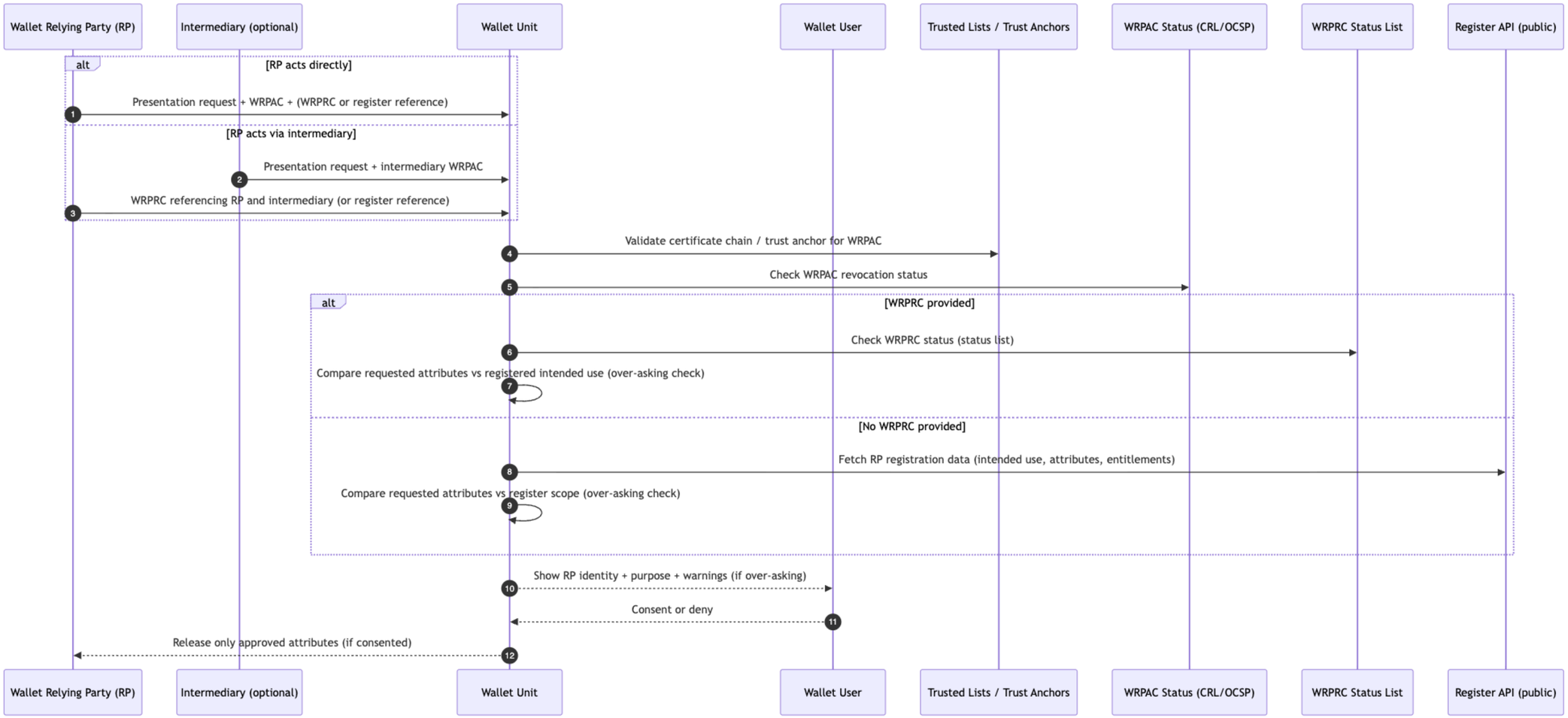
- Vetting process is MS specific
- RP auth framework currently limited to “access to attributes”.
    - What about transactions (e.g., payment, terms&conditions, signature)?
        - Need for specific policies for transaction authorization
    - What about ”right to be forgotten” in this case?
        - Implies renounce to right to dispute
- No global mechanism in sight
- How does the approach extend to RP’s agents?

tinexta
infocert

Grazie

tinexta
infocert

Detailed validation process



tinexta
infocert