Svenska Institutet för Standarder

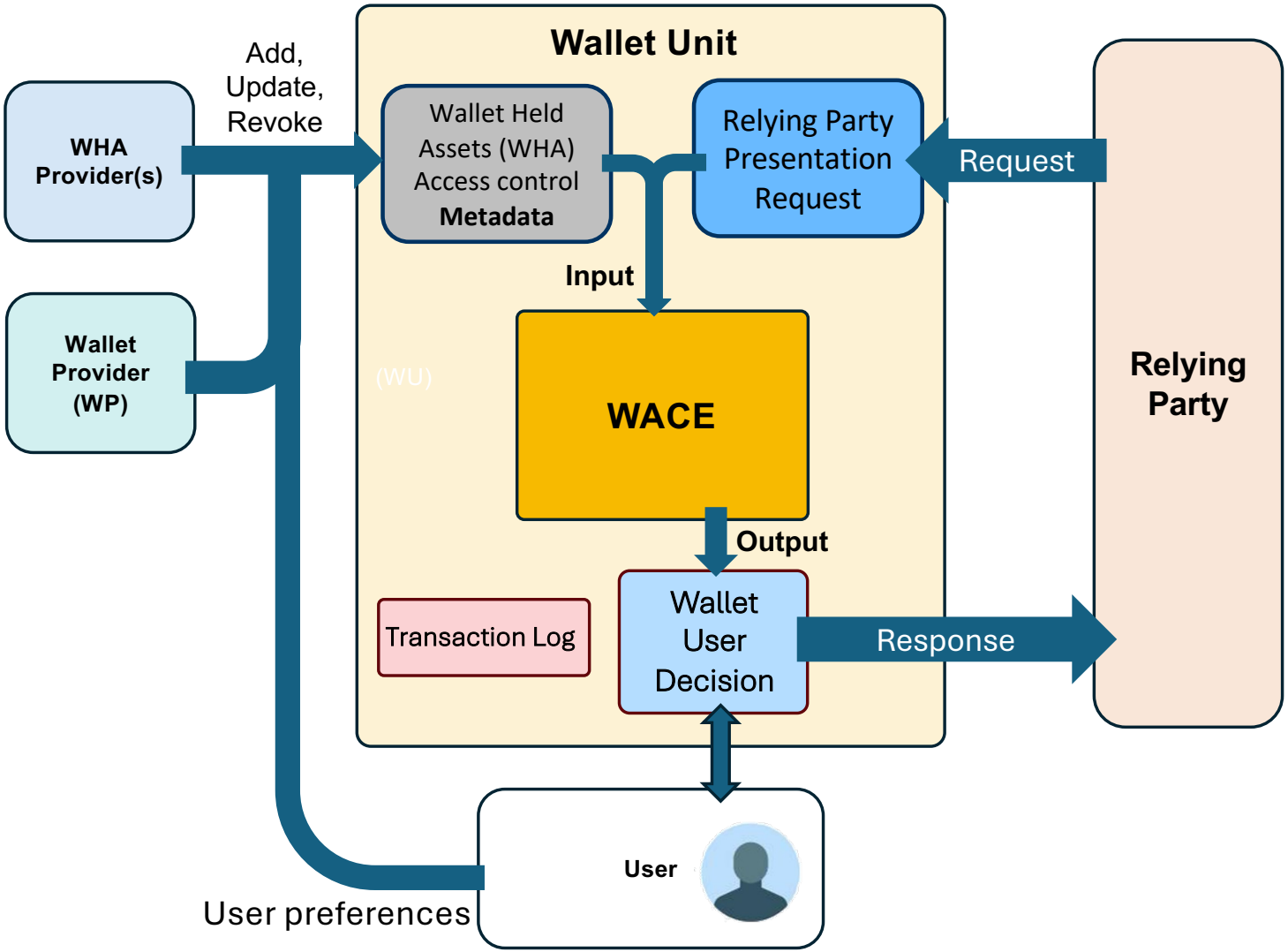
EUDI Wallet Access Control

https://linaltec.com/tools/wallet-access-control/

CEN/TS 18297 in conversation with Termont & Esteves
(2026)

sis.se

WACE Overview

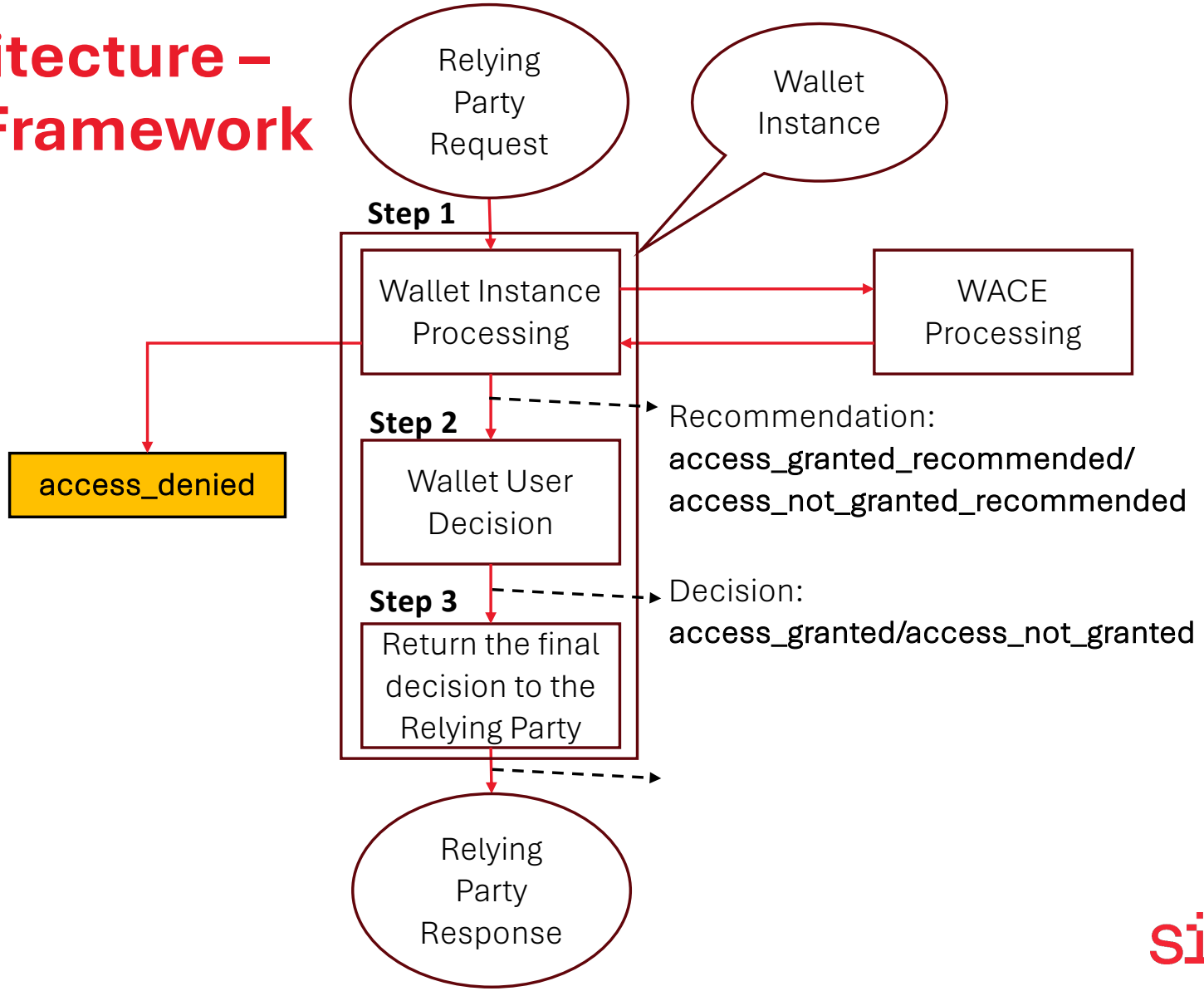


WACE INPUT:
Request_parameters {
requested WHA(s),
privacy notification(s),
security status {
RP Authentication,
RP Authorization,
User Authentication,
Session Encryption,
Cryptosuite choice,
etc.
}}

WACE OUTPUT:
decision{
access_denied,
access_granted_recommended,
access_not_granted_recommended }
justification{
text_notice_to_RP }
etc.}

sis

Wallet Unit Architecture – Access Control Framework (Relying Party)



Where CEN/TS 18297 and the paper line up

The paper says control is missing

- EUDI/OpenID gives the illusion of control
- Selective disclosure ≠ informed consent
- Wallet provider becomes the new chokepoint

WACE puts policy back in the wallet

- Decisions made before the user prompt
- Three policy sources, auditable combination
- Transaction log = contestable history
- Issuer policies survive a malicious UI

sis

Where the paper still pushes us further

What CEN/TS 18297 does NOT yet do

- Static credential model — same as OpenID4VC
- No uniform query meta-language
- No native asynchronous / agent flows
- Trusted-list problem unchanged

Where to look next

- OAuth UMA — User Managed Access
- A4DS — Authorization for Data Spaces
- GNAP — Grant Negotiation and Authorization
- W3C VC + DID as foundation

sis

One question for the panel

> If the issuer's policy and the user's preference disagree — who wins?

Try it — and tell me where it breaks

linaltec.com/tools/wallet-access-control

Interactive access-control template

Walks through how a wallet should evaluate a request — RP authentication, authorization, policy combination, and the decision the user actually sees.

Use it as a strawman. Break it. Send me the cases where it gives the wrong answer.

Jan Lindquist · Linaltec · CEN/TC 224 WG20

Sponsored by StandICT.eu

sis