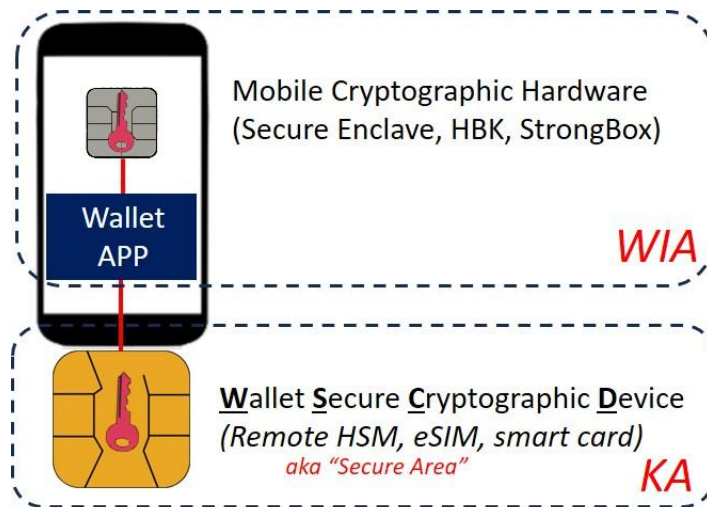


The two EU Wallet Unit Attestations— Objectives, Issues and Solutions

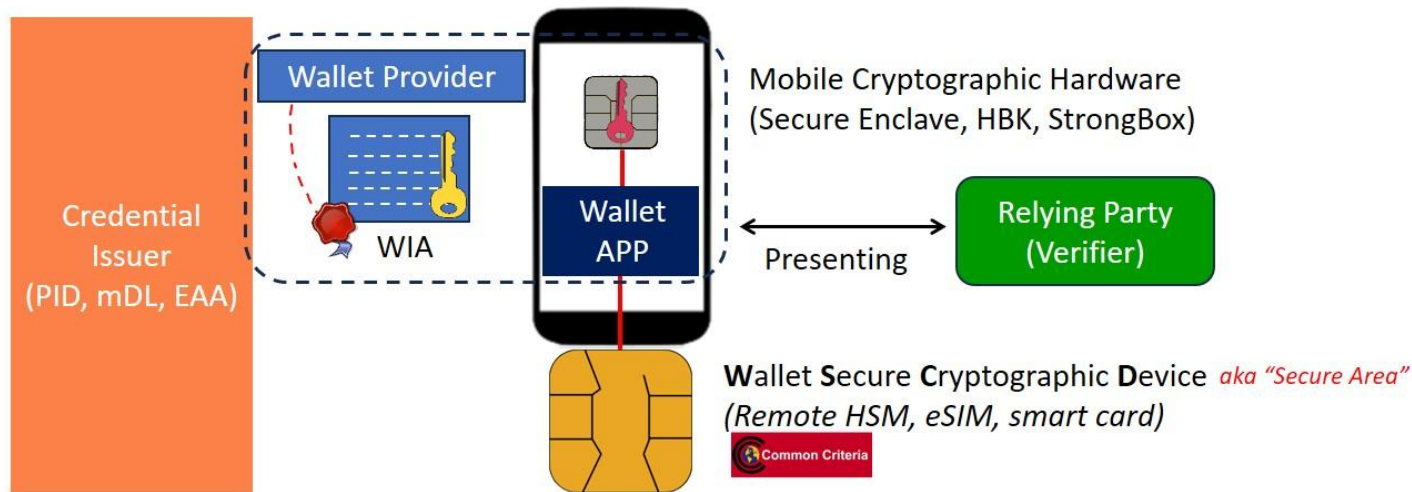
ITU Workshop 2 June 2026

Session 3: Trust management of wallets

Eric Verheul — Eric.Verheul@wellet.nl

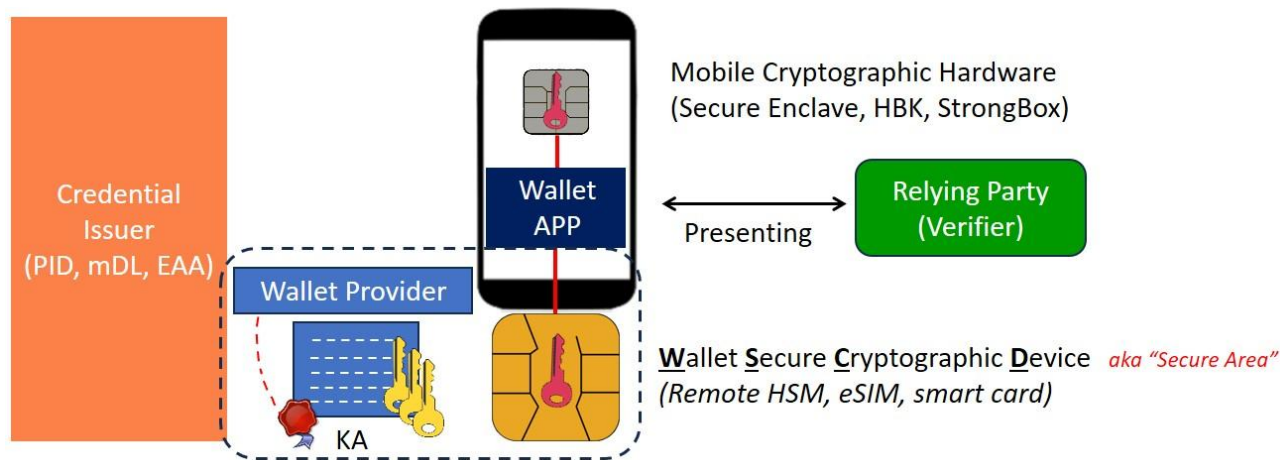


The Wallet Instance Attestation (WIA)



WIA Security & Privacy Objectives	Issues	Solutions
Fresh assurance Wallet APP is authentic	iOS gap on key- and APP attestation	Talk to Apple
Binds Wallet APP to mobile crypto hardware	WIA scoped to issuance only	Open WIA to (some) Relying Parties
Provides a Wallet APP revocation reference	Mobile crypto hardware identification not supported for privacy reasons	Same-hardware verification without identification — Proof of Association (*)
Not a 'super-cookie'		(*) See eprint.iacr.org/2024/1444

The Key Attestation (KA)



KA Security & Privacy Objectives	Issues	Solutions
Provides Issuer assurance that WSCD is authentic	Tension with GDPR data minimisation — Wallet Provider gets access to all credential public keys	Same-hardware verification without identification — Proof of Association (*) — Wallet/WSCD directly prove to credential issuers that credential public keys are from same WSCD the Issuer-Specific KAs refer to; no Wallet Provider involvement (*) also suggested in ISO 23220-3
Provides Issuer assurance that prospect credential keys are bound to WSCD		
Provides Issuer WSCD revocation reference		
Not a 'super-cookie'		