ZKP in Production Wallets and Tenders: Where EU Standards Meet Real World Constraints

Aivo Kalu, lead security engineer, aivo.kalu@cyber.ee

Agenda

- What is ZKP in this talk
- Which tenders we are looking at
- Is there a problem?
- What could be done

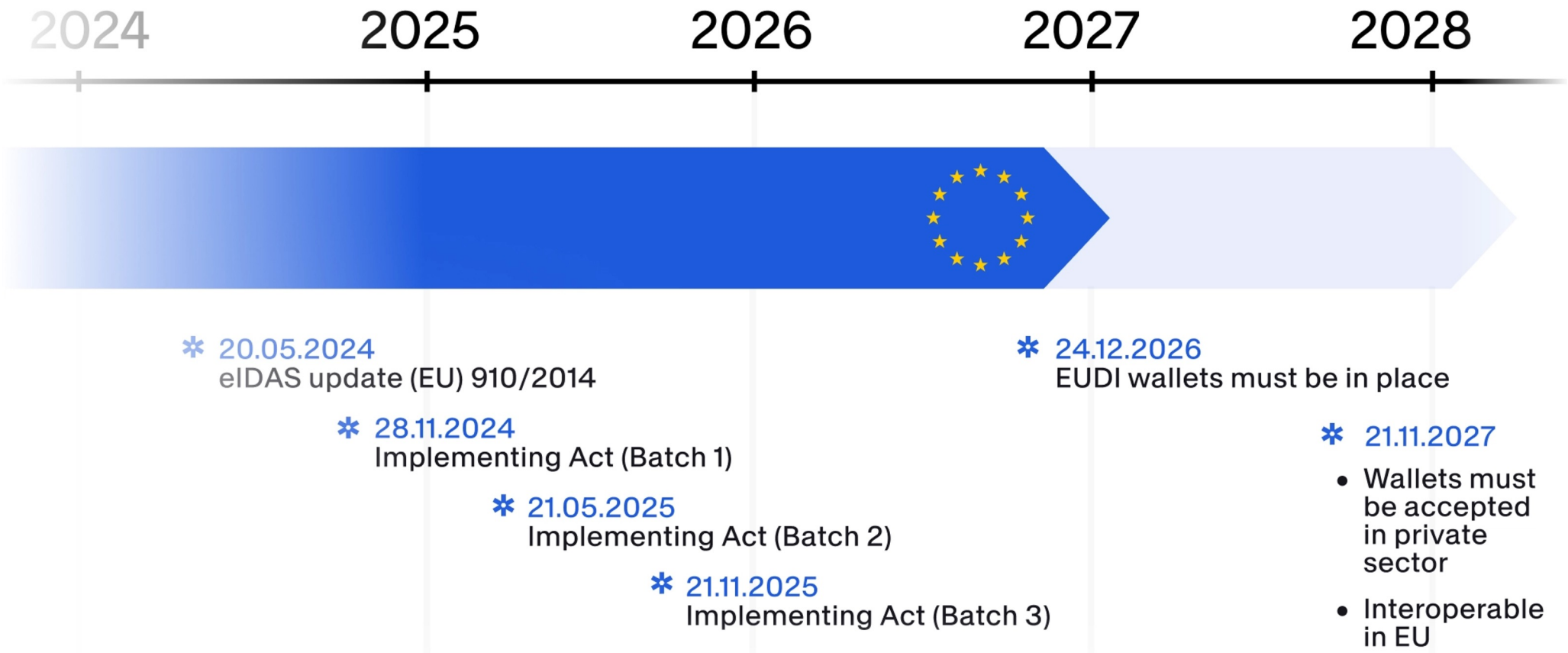
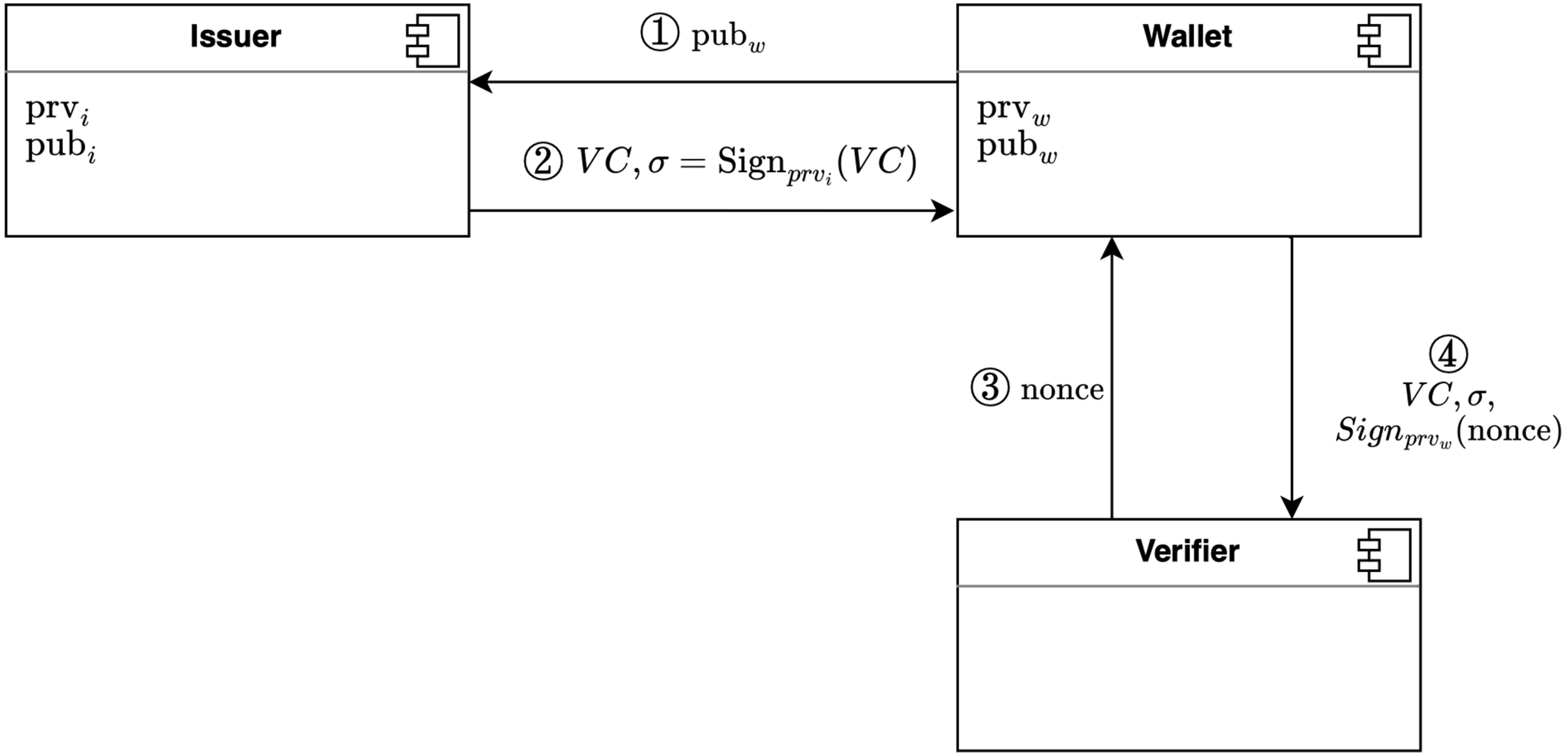


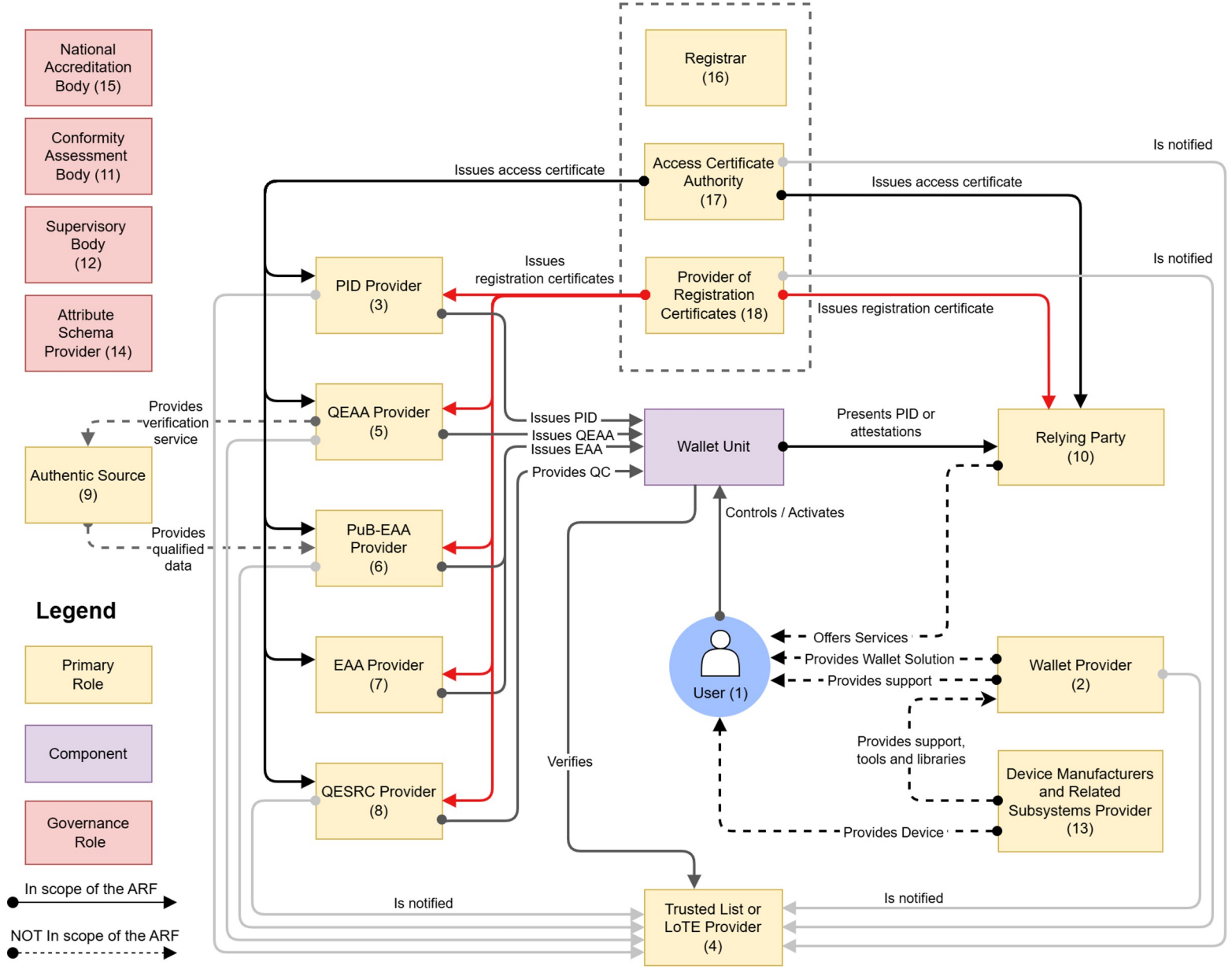
Image: https://www.procivis.ch/eidas-2-0

What is ZKP in this talk

- ETSI TR 119 476-1 – “SD and ZKPs applied to EAAs: Part 1 – Feasibility Study”
- ETSI TS 119 476-2 – “SD and ZKPs applied to EAAs: Part 2 – Implementation in EUDI Wallet”

- Salted Attribute Hashes
  - SD-JWT, mdoc
- Batch issuance and VC re-use policies
- Advanced ZKP
  - ARF - TS4, TS14
  - LongFellow
  - BBS+ signatures


Issuer
prv_i
pub_i
① pub_w
② $VC, \sigma = \text{Sign}_{prv_i}(VC)$
Wallet
prv_w
pub_w
③ nonce
④
$VC, \sigma,$
$Sign_{prv_w}(\text{nonce})$
Verifier


National Accreditation Body (15)
Conformity Assessment Body (11)
Supervisory Body (12)
Attribute Schema Provider (14)
Registrar (16)
Access Certificate Authority (17)
Provider of Registration Certificates (18)
PID Provider (3)
QEAA Provider (5)
PuB-EAA Provider (6)
EAA Provider (7)
QESRC Provider (8)
Authentic Source (9)
Wallet Unit
Relying Party (10)
User (1)
Wallet Provider (2)
Device Manufacturers and Related Subsystems Provider (13)
Trusted List or LoTE Provider (4)
Issues access certificate
Is notified
Issues access certificate
Issues registration certificates
Is notified
Issues registration certificate
Provides verification service
Issues PID
Issues QEAA
Issues EAA
Provides QC
Presents PID or attestations
Provides qualified data
Controls / Activates
Offers Services
Provides Wallet Solution
Provides support
Provides support, tools and libraries
Verifies
Provides Device
Is notified
Is notified
Legend
Primary Role
Component
Governance Role
In scope of the ARF
NOT In scope of the ARF

Tenders

- Latvian EUDIW development tender
  - qualifications in December 2025, overall budget 4MEUR
- Luxembourg EUDIW WSCA component procurement
  - RFP in March 2026, budget 140KEUR
- Estonian EUDIW development/service tender
  - first RFI in 2024, second RFI in 2025, RFP announced on 18th of May
  - budget over 5 years 21 MEUR
- Finnish EUDIW SDK and WSCA/WSCD solution tender
  - RFI in Spring 2026
- Lithuania EUDIW tender
  - no RFP yet

Technical requirements from tenders

Country	Selective disclosure (standard SD-JWT, mdoc)	Batch issuance, no-reuse	Advanced ZKP	
			Longfellow	BBS+
Latvia	no info yet	no info yet	no info yet	
Luxembourg	CIR 2024/2979 → ISO 18013-5:2021	-	-	
Estonia	eIDAS2 → every applicable CIR	no info yet	no info yet	
Finland	ETSI TS 119 472-2 V1.1.1 (ISO 18013-5, SD-JWT v22)	ETSI TS 119 472-3 V1.1.1	after CIR establishment: (EC TS13, EC TS14 ETSI EN 119 476-2)	
Lithuania	no info yet	no info yet	no info yet	
Germany	yes	yes	-	

ETSI TS 119 472-3

- “Profiles for EAAs – Part 3: Profiles for issuance of EAA or PID”
- Profile of OpenID4VC-HAIP, which defines a profile of OpenID4VCI
- Section 4.2.4 – “Provision of PID/EAA reuse policy”

EXAMPLE 5: Below follows a non-normative example for the type "per-relying-party".

```
{
  "credential_reuse_policy" : {
    "id": "arf_annex_ii",
    "options": [
      {
        "details": ["per-relying-party"],
        "batch_size": 10,
        "reissue_trigger_lifetime_left": 86400
      }
    ]
  }
}
```

ETSI TS 119 476-2

- “SD and ZKPs applied to EAAs: Part 2 – Implementation in EUDI Wallet”
- Version 0.0.1 released 2026-03-02
- Stable draft targeted 2026-10-15
- Work in Progress - https://portal.etsi.org/eWPM/index.html#/schedule?WKI_ID=74931

Is there a problem?

Hypotheses - what is the problem?

- H0 – EUDIWs are not really useful anyway?

Hypotheses - what is the problem?

- H0 – EUDIWs are not really useful anyway?
- H1 – We simply have limited visibility?

Hypotheses - what is the problem?

- H0 – EUDIWs are not really useful anyway?
- H1 – We simply have limited visibility?
  - We don’t know production configuration of Finland
  - Estonia, Latvia, Lithuania haven’t published their tender requirements anyway
  - There’s still some time?

Hypotheses - what is the problem?

- H0 – EUDIWs are not really useful anyway?
- H1 – We simply have limited visibility?
  - We don’t know production configuration of Finland
  - Estonia, Latvia, Lithuania haven’t published their tender requirements anyway
  - There’s still some time?
- H2 – Out-of-box selective-disclosure is good enough?
- H3 – Currently drafted batch-issuance/re-use policy is good enough?

Hypotheses - what is the problem?

- H0 – EUDIWs are not really useful anyway?
- H1 – We simply have limited visibility?
  - We don’t know production configuration of Finland
  - Estonia, Latvia, Lithuania haven’t published their tender requirements anyway
  - There’s still some time?
- H2 – Out-of-box selective-disclosure is good enough?
- H3 – Currently drafted batch-issuance/re-use policy is good enough?
- H4 – ZKP is not useful for EUDI wallets?
  - Unlinkability requirement is too vague
  - Pseudonyms (WebAuthn and passkeys) are there anyway

Hypotheses - what is the problem?

- H0 – EUDIWs are not really useful anyway?
- H1 – We simply have limited visibility?
  - We don't know production configuration of Finland
  - Estonia, Latvia, Lithuania haven't published their tender requirements anyway
  - There's still some time?
- H2 – Out-of-box selective-disclosure is good enough?
- H3 – Currently drafted batch-issuance/re-use policy is good enough?
- H4 – ZKP is not useful for EUDI wallets?
  - Unlinkability requirement is too vague
  - Pseudonyms (WebAuthn and passkeys) are there anyway
- H5 – ZKP is too expensive to procure, certify and maintain?
  - So, we will implement SD (and batch issuance) or just ignore EU laws?

Hypotheses - what is the problem?

- H0 – EUDIWs are not really useful anyway?
- H1 – We simply have limited visibility?
  - We don't know production configuration of Finland
  - Estonia, Latvia, Lithuania haven't published their tender requirements anyway
  - There's still some time?
- H2 – Out-of-box selective-disclosure is good enough?
- H3 – Currently drafted batch-issuance/re-use policy is good enough?
- H4 – ZKP is not useful for EUDI wallets?
  - Unlinkability requirement is too vague
  - Pseudonyms (WebAuthn and passkeys) are there anyway
- H5 – ZKP is too expensive to procure, certify and maintain?
  - So, we will implement SD (and batch issuance) or just ignore EU laws?
- H6 – ZKP is not production ready?
  - European Parlament was too ambitios with their eIDAS2 legislation?

What do we do?

What could be or should be done?

- Engage with your customer
- Test configurations with production-level load
- Contribute to standards developing working groups
- Talk to your favourite academic researchers and government regulatory authorities

Thank you

Aivo Kalu, aivo.kalu@cyber.ee

https://cyber.ee/
info@cyber.ee
cybernetica
CyberneticaAS
cybernetica_ee
Cybernetica