Enabling Anonymous Credentials for Digital Identity Wallets

EIC Conference 2026

Christian Bormann

Prof. Anja Lehmann

SPRIN-D
BUNDESAGENTUR
FÜR SPRUNGINNOVATIONEN

HPI Hasso Plattner Institut
Digital Engineering · Universität Potsdam

European Digital Identity Wallet (EUDI)

- All EU member states must provide EUDI Wallets to their citizens by the end of 2026 according to eIDAS (Regulation 2024/1183)

Example Visualization

eIDAS

- ..aims at ensuring **user data protection, non-discriminatory** access to wallets, and **interoperability** among wallets across the EU.
- ..standardizes the Feature Set and Security Requirements of Wallets
- ..is a **blueprint** for the rollout of the overall ecosystem.

EUDI | Privacy & Security Requirements in eIDAS

Privacy: *The technical framework of the European Digital Identity Wallet shall*

(a) *not allow providers of electronic attestations of attributes or any other party […] to obtain data that allows transactions or* ***user behaviour to be tracked, linked or correlated*** *[…]*

(b) *enable privacy preserving techniques which* ***ensure unlinkability****, where the attestation of attributes does not require the identification of the user.*

https://eur-lex.europa.eu/eli/reg/2024/1183/oj

EUDI | Privacy & Security Requirements in eIDAS

Privacy: *The technical framework of the European Digital Identity Wallet shall*

(a) *not allow providers of electronic attestations of attributes or any other party […] to obtain data that allows transactions or* ***user behaviour to be tracked, linked or correlated*** *[…]*

(b) *enable privacy preserving techniques which* ***ensure unlinkability****, where the attestation of attributes does not require the identification of the user.*

User-control: *Users shall have full control of the* ***use of and of the data*** *in their European Digital Identity Wallet. The provider of the European Digital Identity Wallet* ***shall neither collect information*** *about the use of the European Digital Identity Wallet […]*

https://eur-lex.europa.eu/eli/reg/2024/1183/oj

EUDI | Privacy & Security Requirements in eIDAS

Privacy: *The technical framework of the European Digital Identity Wallet shall*

(a) *not allow providers of electronic attestations of attributes or any other party […] to obtain data that allows transactions or* ***user behaviour to be tracked, linked or correlated*** *[…]*

(b) *enable privacy preserving techniques which* ***ensure unlinkability****, where the attestation of attributes does not require the identification of the user.*

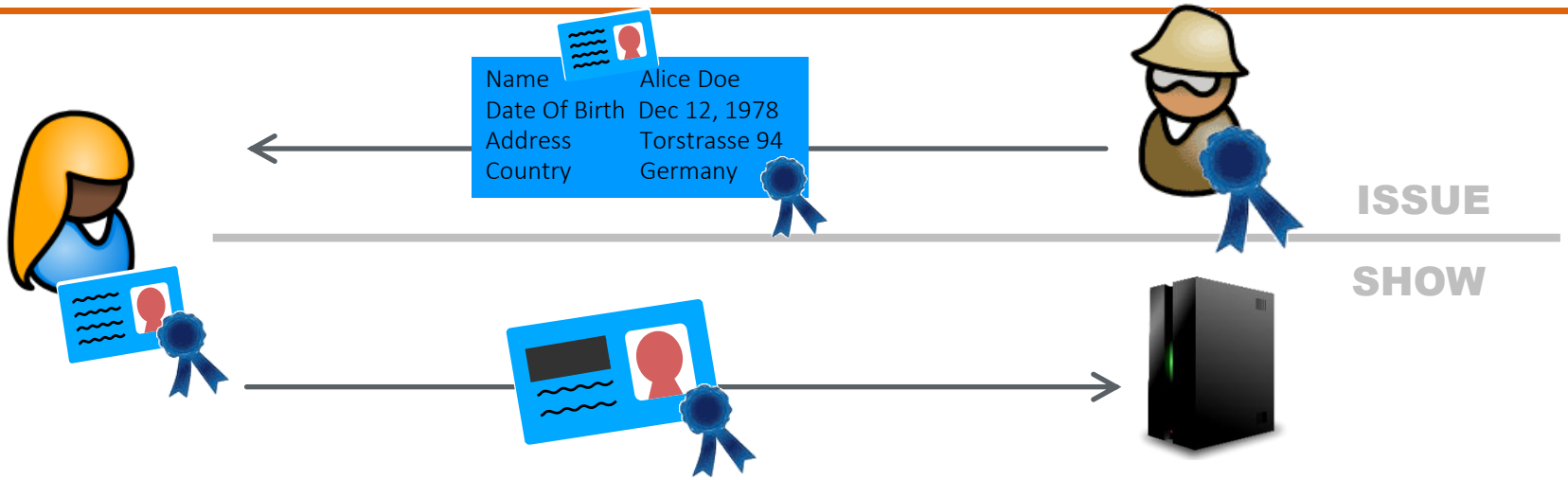
User-control: *Users shall have full control of the* ***use of and of the data*** *in their European Digital Identity Wallet. The provider of the European Digital Identity Wallet* ***shall neither collect information*** *about the use of the European Digital Identity Wallet […]*

Security:

- **Level of Assurance High** (for PID), but not for all credentials
- **Accepted schemes** → ENISA Agreed Cryptographic Mechanisms
- **Hardware certification** requirements
- Secure cryptographic **device binding**

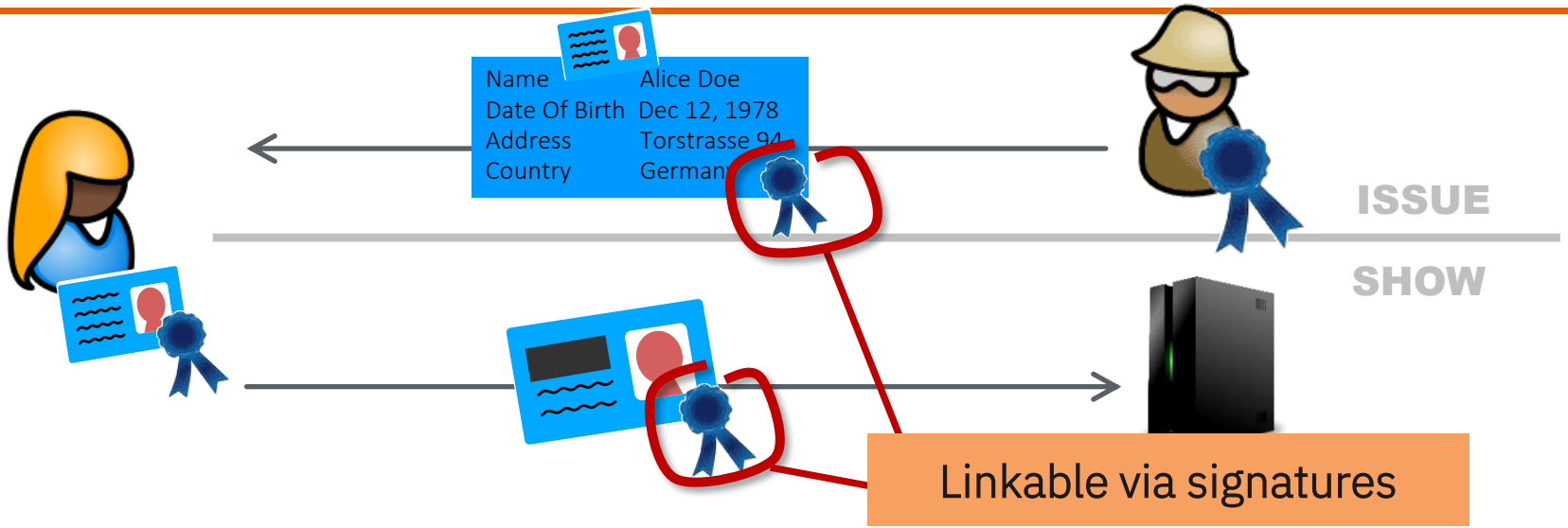
https://eur-lex.europa.eu/eli/reg/2024/1183/oj

EUDI | Solution with Classical Signatures



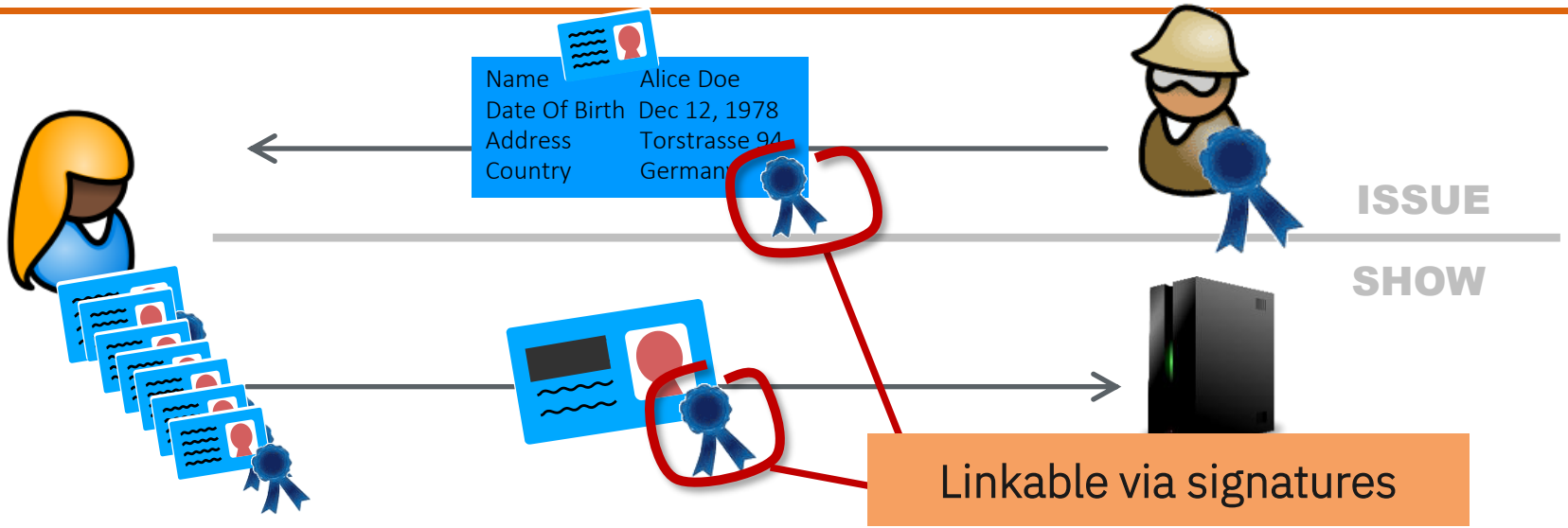
- Digital identity credentials based on cryptographic signatures

EUDI | Solution with Classical Signatures



- Digital identity credentials based on cryptographic signatures
- Digital Signatures are great for security, especially for a highly distributed system but bad for privacy → unique identifier

EUDI | Solution with Classical Signatures



- Digital identity credentials based on cryptographic signatures
- Digital Signatures are great for security, especially for a highly distributed system but bad for privacy → unique identifier
- Current solution: **batch issuance** of one-time use credentials & holder keys

EUDI | Batch Issuance

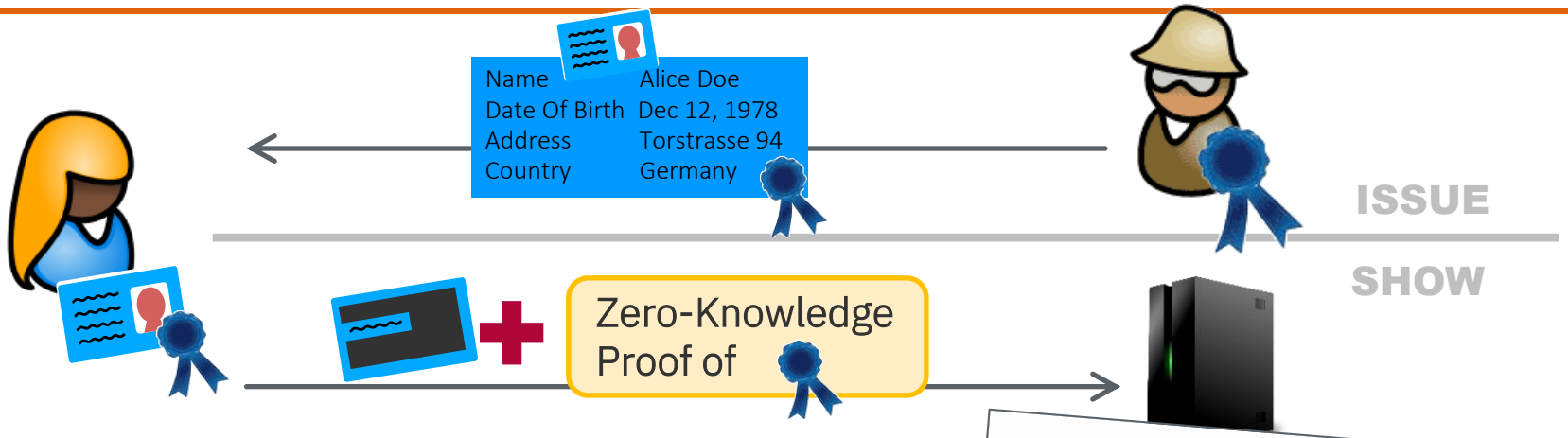
- Batch Issuance needed for **every statement with a signature** that might be used for correlation
  - Credentials (PID, EAAs)
  - Wallet Attestations (used towards issuers)

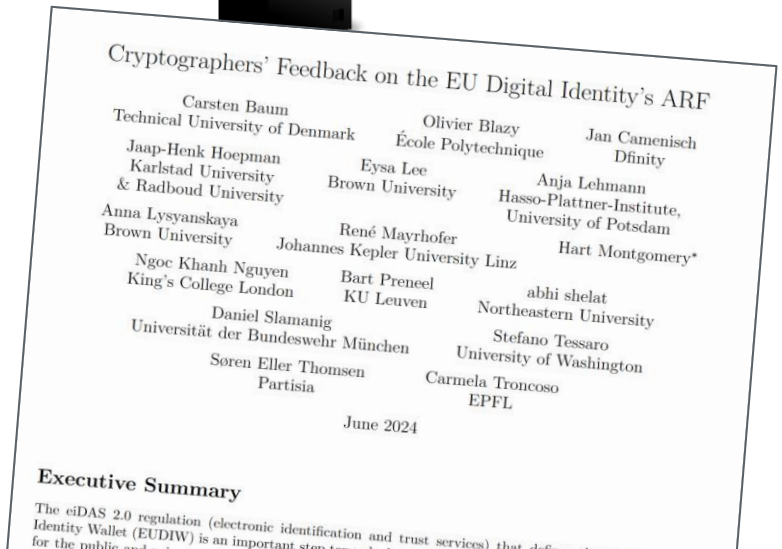
- Creates **complexity & burden** in the overall system & infrastructure:
  - Issuers need to issue and manage batches of credentials
  - Wallets need to generate and manage a lot of keys (which is costly if we are talking about server-based HSMs)

- A **malicious issuer** would still be able to link those one-time use signatures & keys

Can we get to even stronger **privacy guarantees** & make the **overall system simpler**?

Anonymous Credentials & Zero-Knowledge Proofs





Cryptographers' Feedback on the EU Digital Identity's ARF

Carsten Baum, Technical University of Denmark
Olivier Blazy, École Polytechnique
Jan Camenisch, Dfinity
Jaap-Henk Hoepman, Karlstad University & Radboud University
Eysa Lee, Brown University
Anja Lehmann, Hasso-Plattner-Institute, University of Potsdam
Anna Lysyanskaya, Brown University
René Mayrhofer, Johannes Kepler University Linz
Hart Montgomery*
Ngoc Khanh Nguyen, King's College London
Bart Preneel, KU Leuven
abhi shelat, Northeastern University
Daniel Slamanig, Universität der Bundeswehr München
Stefano Tessaro, University of Washington
Søren Eller Thomsen, Partisia
Carmela Troncoso, EPFL

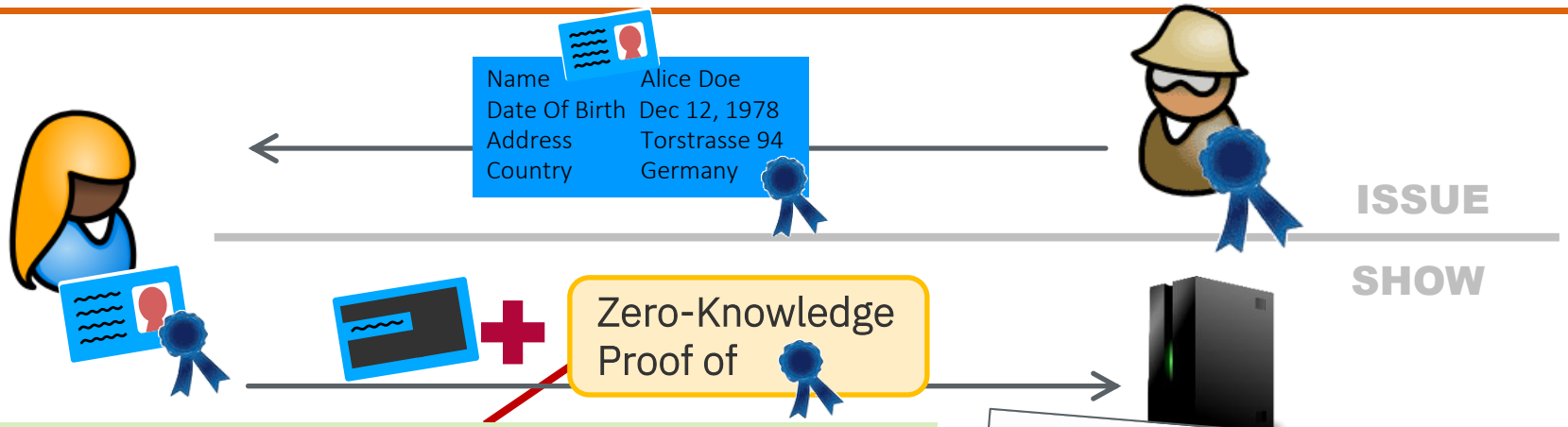
June 2024

Executive Summary

The eIDAS 2.0 regulation (electronic identification and trust services) that defines Identity Wallet (EUDIW) is an important step for the public and

https://github.com/eu-digital-identity-wallet/eudi-doc-architecture-and-reference-framework/issues/200

Anonymous Credentials & Zero-Knowledge Proofs

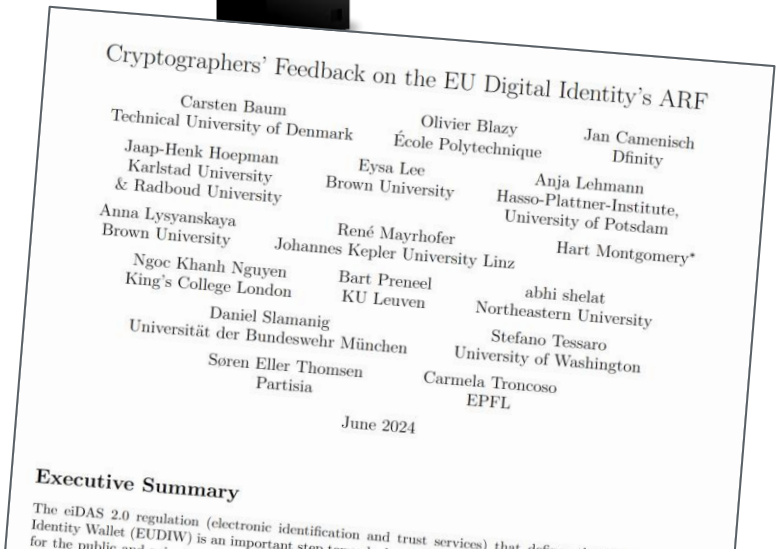


Zero-Knowledge Proof (ZKP)

Proof that reveals nothing beyond validity

→ multi-show unlinkability & untraceability

Practical ZKP-based solutions exist since 25 years



Cryptographers' Feedback on the EU Digital Identity's ARF

Carsten Baum
Technical University of Denmark
Olivier Blazy
École Polytechnique
Jan Camenisch
Dfinity
Jaap-Henk Hoepman
Karlstad University
& Radboud University
Eysa Lee
Brown University
Anja Lehmann
Hasso-Plattner-Institute,
University of Potsdam
Anna Lysyanskaya
Brown University
René Mayrhofer
Johannes Kepler University Linz
Hart Montgomery*
Ngoc Khanh Nguyen
King's College London
Bart Preneel
KU Leuven
abhi shelat
Northeastern University
Daniel Slamanig
Universität der Bundeswehr München
Stefano Tessaro
University of Washington
Søren Eller Thomsen
Partisia
Carmela Troncoso
EPFL

June 2024

Executive Summary

The eIDAS 2.0 regulation (electronic identification and trust services) that defines ... Identity Wallet (EUDIW) is an important step ... for the public and ...

https://github.com/eu-digital-identity-wallet/eudi-doc-architecture-and-reference-framework/issues/200

Why does EUDI not use Anonymous Credentials (yet) ?

1 | All protocols and schemes must be **standardized** → interoperability (& sign of maturity)

Regulated use cases (e.g. eID): all crypto must be in "Agreed Cryptographic Mechanisms" by ENISA (previously SOG-IS catalogue)

Primitive	Scheme	R/L	Notes
RSA	PSS (PKCS#1v2.1) [RFC8017, PKCS1, ISO9796-2]	R	
FF-DLOG	KCDSA [ISO14888-3]	R	
	Schnorr [ISO14888-3]	R	41-DSARandom
	DSA [FIPS186-4, ISO14888-3]	R	
EC-DLOG	EC-KCDSA [ISO14888-3]	R	
	EC-DSA [FIPS186-4, ISO14888-3]	R	41-DSARandom
	EC-GDSA [TR-03111]	R	
	EC-Schnorr [ISO14888-3]	R	
RSA	PKCS#1v1.5 [RFC8017, PKCS1, ISO9796-2]	L	40-PKCSFormatCheck

List of „approved" crypto when EUDI ARF was designed (now it also includes PQC)

Why does EUDI not use Anonymous Credentials (yet) ?

1 | All protocols and schemes must be **standardized** → interoperability (& sign of maturity)

Regulated use cases (e.g. eID): all crypto must be in "Agreed Cryptographic Mechanisms" by ENISA (previously SOG-IS catalogue)

Primitive	Scheme	R/L	Notes
RSA	PSS (PKCS#1v2.1) [RFC8017, PKCS1, ISO9796-2]	R	
FF-DLOG	KCDSA [ISO14888-3]	R	
	Schnorr [ISO14888-3]	R	41-DSARandom
	DSA [FIPS186-4, ISO14888-3]	R	
EC-DLOG	EC-KCDSA [ISO14888-3]	R	
	EC-DSA [FIPS186-4, ISO14888-3]	R	41-DSARandom
	EC-GDSA [TR-03111]	R	
	EC-Schnorr [ISO14888-3]	R	
RSA	PKCS#1v1.5 [RFC8017, PKCS1, ISO9796-2]	L	40-PKCSFormatCheck

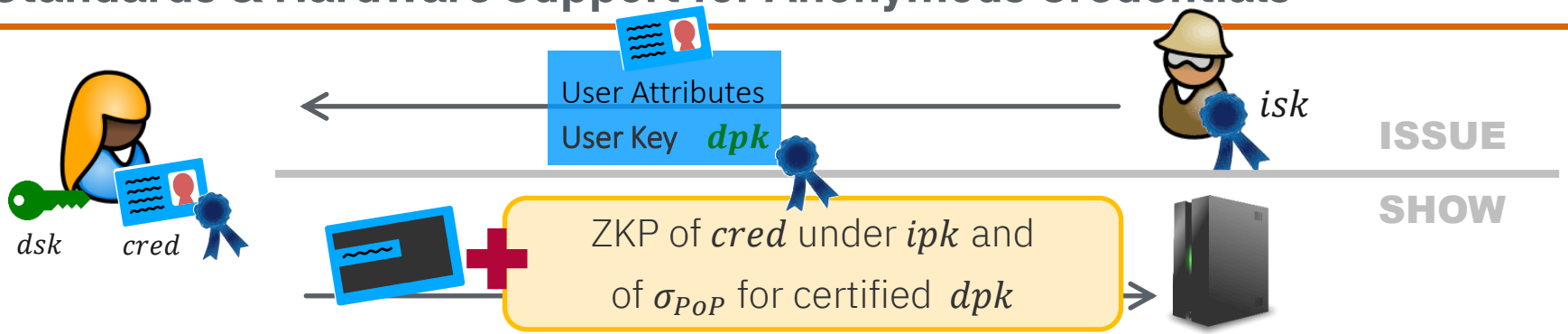
List of „approved" crypto when EUDI ARF was designed (now it also includes PQC)

2 | Credential must be bound to **hardware**-protected device key

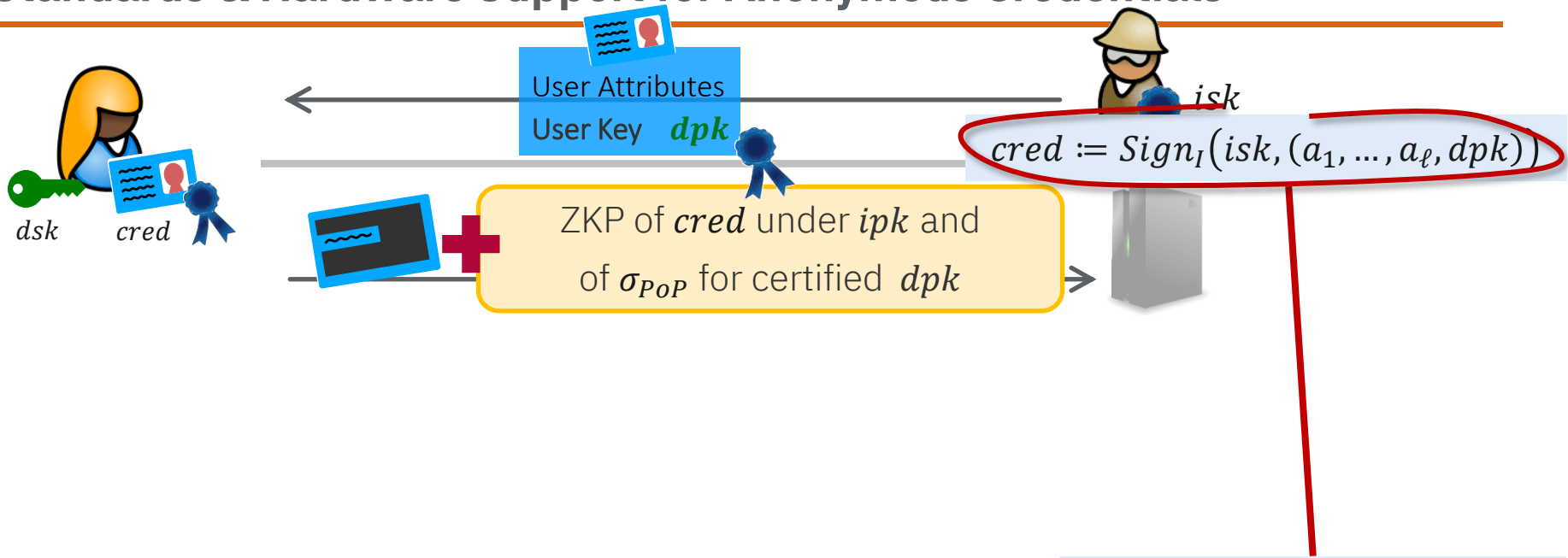
EUDI Wallet requires Level-of-Assurance (LoA) High

Secure Elements support only ECDSA (and curve P256)

Standards & Hardware Support for Anonymous Credentials



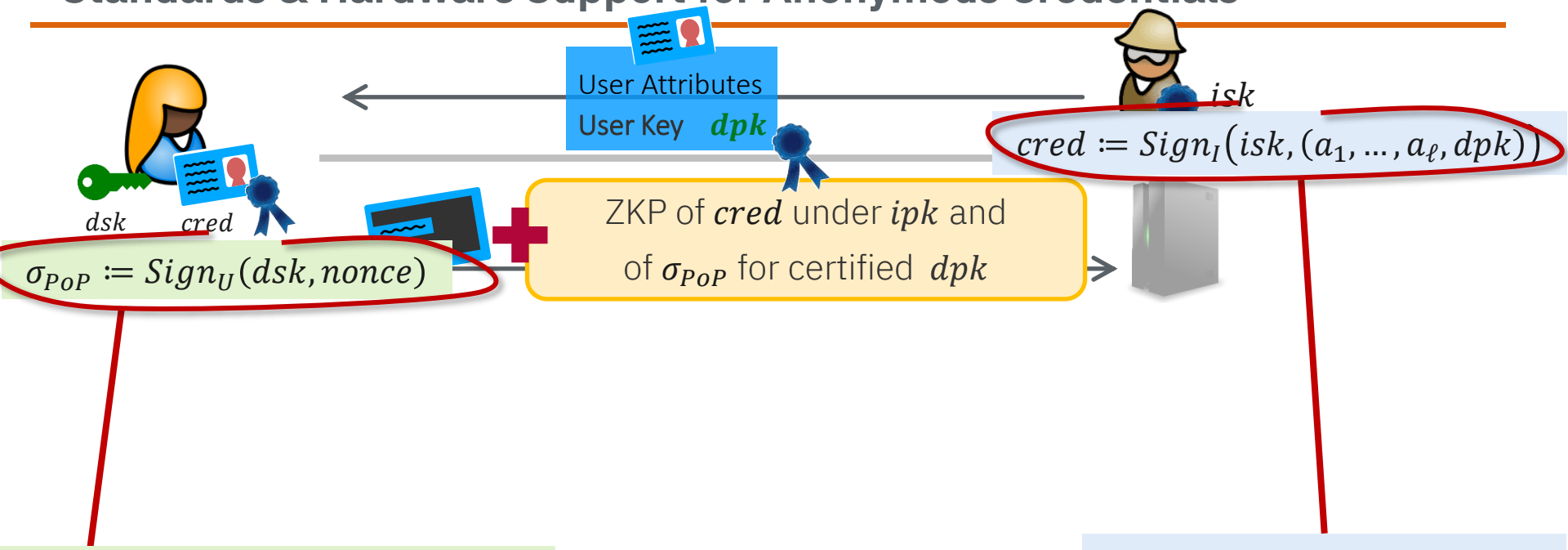
Standards & Hardware Support for Anonymous Credentials



Issuer signature scheme:

- ZKP-friendly
- Hardware support for LoA high credentials

Standards & Hardware Support for Anonymous Credentials



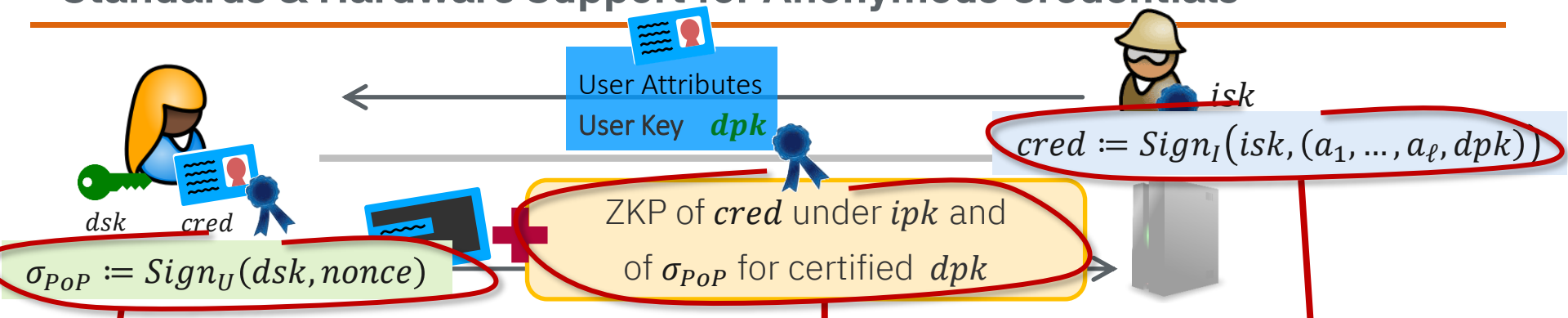
Device signature scheme

- (somewhat) ZKP-friendly
- Hardware support essential for non-transferability

Issuer signature scheme:

- ZKP-friendly
- Hardware support for LoA high credentials

Standards & Hardware Support for Anonymous Credentials



ZKP scheme

- ZKP runs entirely on "public" values

→ ZKP not needed in secure hardware, only standardized
(and "approved" for LoA high)

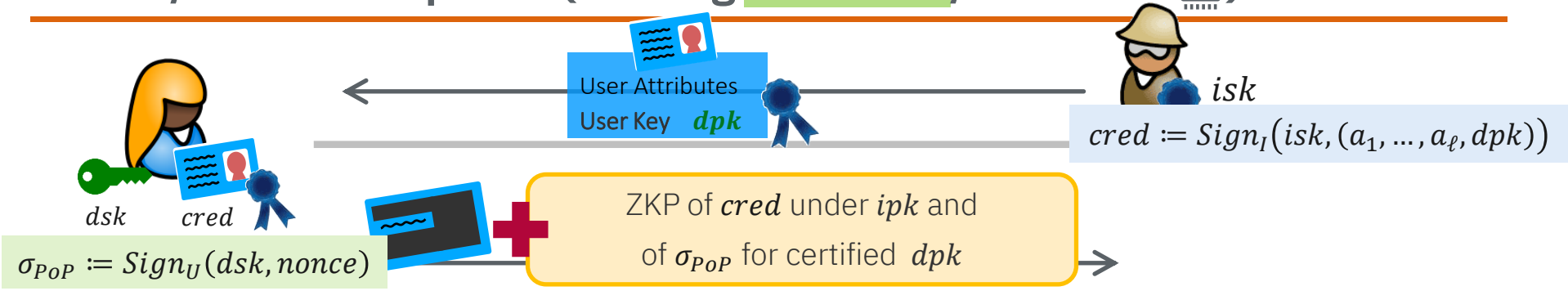
Device signature scheme

- (somewhat) ZKP-friendly
- Hardware support essential for non-transferability

Issuer signature scheme:

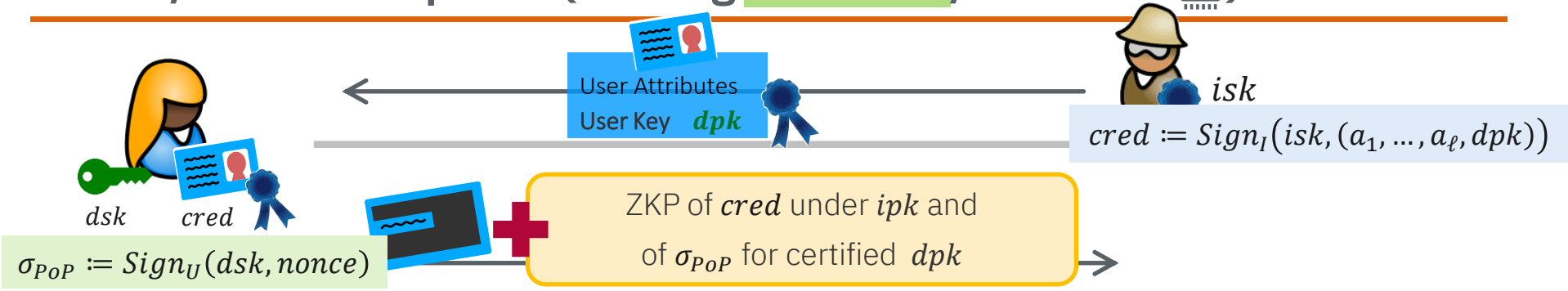
- ZKP-friendly
- Hardware support for LoA high credentials

Short/Mid-Term Options (Existing Standards/Hardware)



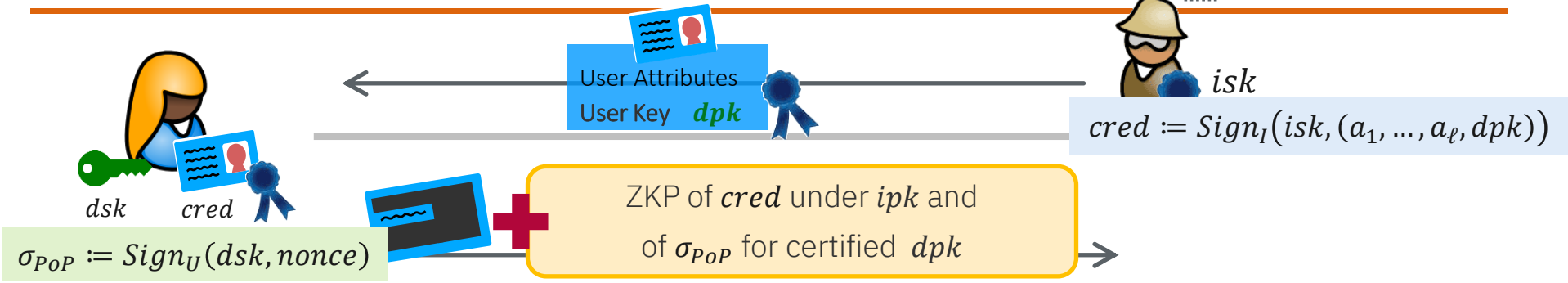
Issuer ($Sign_I$)	Device ($Sign_U$)	ZKP	Efficiency (rough guestimates)	Advantages

Short/Mid-Term Options (Existing Standards/Hardware)



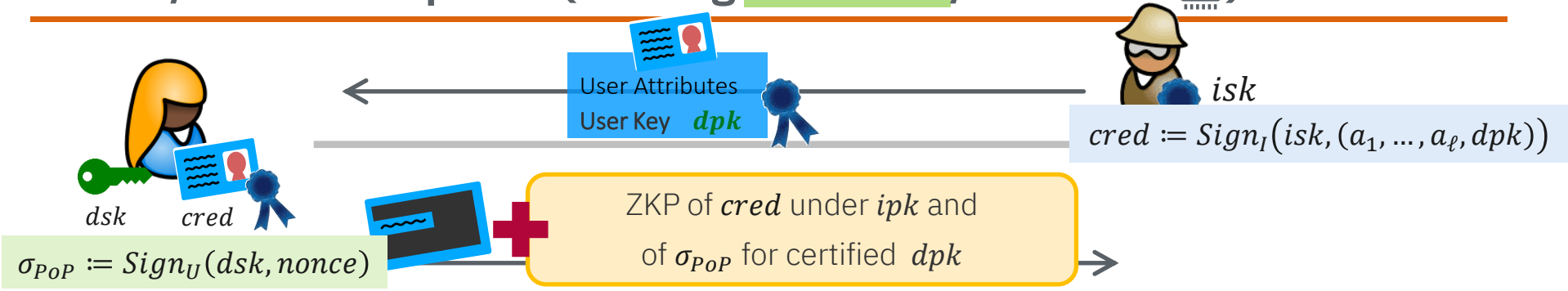
Issuer ($Sign_I$)	Device ($Sign_U$)	ZKP	Efficiency (rough guestimates)	Advantages
BBS	BLS/Schnorr	Schnorr	~10ms, 1kB	Most simple & efficient Privacy in cloud HSM setting

Short/Mid-Term Options (Existing Standards/Hardware)



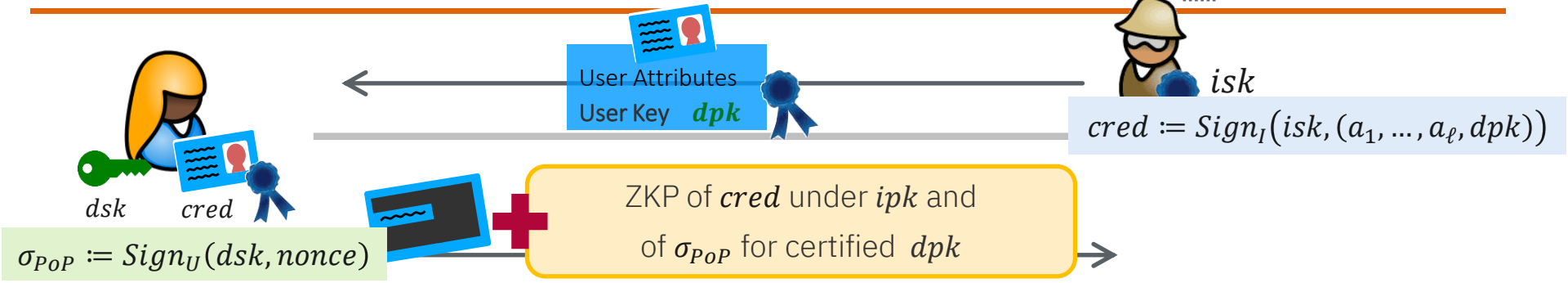
Issuer ($Sign_I$)	Device ($Sign_U$)	ZKP	Efficiency (rough guestimates)	Advantages
BBS	BLS/Schnorr	Schnorr	~10ms, 1kB	Most simple & efficient Privacy in cloud HSM setting
ECDSA	ECDSA	Circuit (complex)	~400ms, ~300kB	No changes to issuer

Short/Mid-Term Options (Existing Standards/Hardware)



Issuer ($Sign_I$)	Device ($Sign_U$)	ZKP	Efficiency (rough guestimates)	Advantages
BBS	BLS/Schnorr	Schnorr	~10ms, 1kB	Most simple & efficient Privacy in cloud HSM setting
BBS	ECDSA	Schnorr (a lot for ECDSA)	~400ms, ~175kB	Relatively simple. No circuit Easy to extend & standardize
ECDSA	ECDSA	Circuit (complex)	~400ms, ~300kB	No changes to issuer

Short/Mid-Term Options (Existing Standards/Hardware)

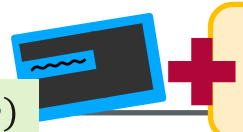


Issuer ($Sign_I$)	Device ($Sign_U$)	ZKP	Efficiency (rough guestimates)	Advantages
BBS	BLS/Schnorr	Schnorr	~10ms, 1kB	Most simple & efficient Privacy in cloud HSM setting
BBS	ECDSA	Schnorr (a lot for ECDSA)	~400ms, ~175kB	Relatively simple. No circuit Easy to extend & standardize
BBS	ECDSA	Circuit (simple)	~400ms, **~1.5kB**	Easy to extend & standardize Short proofs
ECDSA	ECDSA	Circuit (complex)	~400ms, ~300kB	No changes to issuer

Short/Mid-Term Options (Existing Standards/Hardware)

$cred := Sign_I(isk, (a_1, \dots, a_\ell, dpk))$

$\sigma_{PoP} := Sign_U(dsk, nonce)$



ZKP of $cred$ under ipk and of σ_{PoP} for certified dpk

BBS/ECDSA and ECDSA/Circuit considered for EUDI Wallet „v2“ [TS13& TS14]
Currently undergoing standardization in ETSI

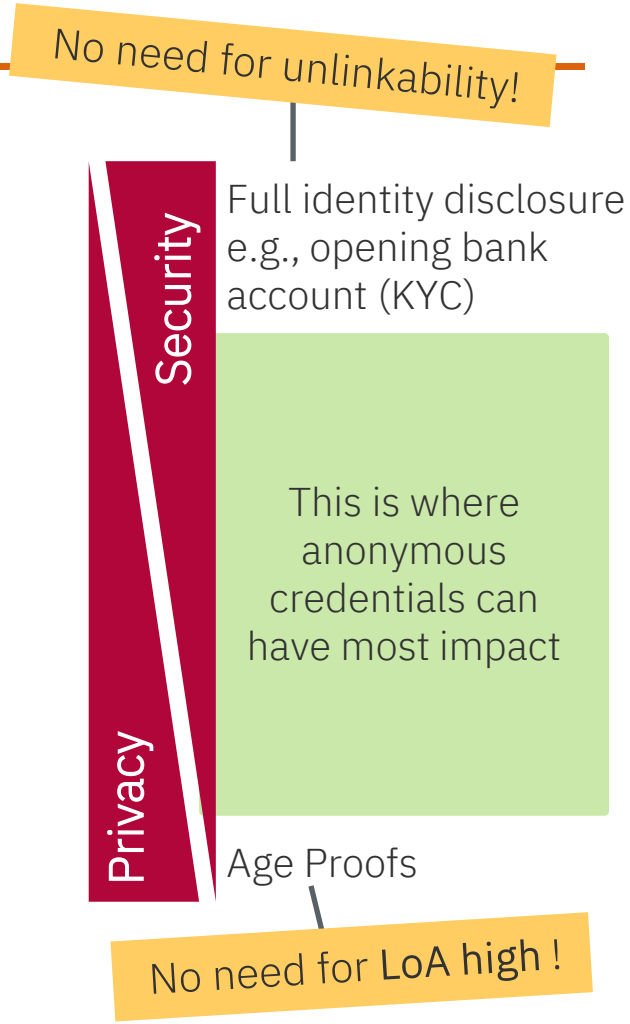
Issue

BBS	BLS/Schnorr	Schnorr	~10ms, 1kB	Privacy in cloud HSM setting
BBS	ECDSA	Schnorr (a lot for ECDSA)	~400ms, ~175kB	Relatively simple. No circuit Easy to extend & standardize
BBS	ECDSA	Circuit (simple)	~400ms, ~1.5kB	Easy to extend & standardize Short proofs
ECDSA	ECDSA	Circuit (complex)	~400ms, ~300kB	No changes to issuer

ZKP-EUDI Roadmap | Next Steps

Short/Mid-term: show feasibility and benefits

- Shape sensible requirements
- Many additional features: pseudonyms, blind issuance, …
  → Build modular & crypto-agile protocols
- ZKP-compatible protocols (OID4VC) & data formats



ZKP-EUDI Roadmap | Next Steps

Short/Mid-term: show feasibility and benefits

- Shape sensible requirements
- Many additional features: pseudonyms, blind issuance, …
  → Build modular & crypto-agile protocols
- ZKP-compatible protocols (OID4VC) & data formats

Longterm: full post-quantum security

- Current solutions have PQC-privacy, but classic soundness
- PQC solutions need (a bit) more research & time to analyse
  - Current work provides concrete target for PQC research
    Insights from pre-PQC serve as blueprint
  - Shape PQC base standards & hardware APIs now(ish)

Summary

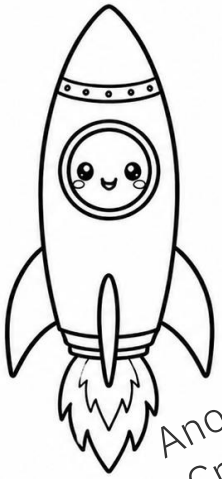
- Anonymous credentials improve deployment challenges, security & privacy
- Core challenges have been addressed: device binding, standards (ongoing)
  Different options with complementary legacy/complexity tradeoffs
- Need modular solution for extensibility & crypto agility

Summary

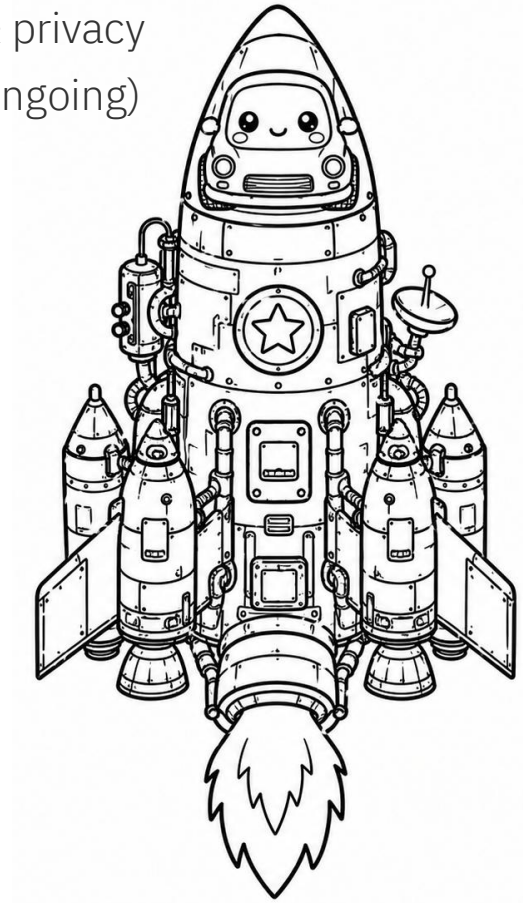
- Anonymous credentials improve deployment challenges, security & privacy
- Core challenges have been addressed: device binding, standards (ongoing)
  Different options with complementary legacy/complexity tradeoffs
- Need modular solution for extensibility & crypto agility

eIDAS: lets fly to the moon
ARF: but you must use a car ....

ECDSA



Anonymous Credentials



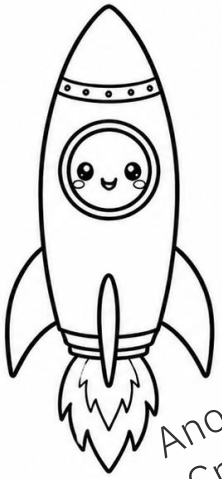
Summary

- Anonymous credentials improve deployment challenges, security & privacy
- Core challenges have been addressed: device binding, standards (ongoing)
  Different options with complementary legacy/complexity tradeoffs
- Need modular solution for extensibility & crypto agility

More information: https://ia.cr/2026/330 & https://ia.cr/2025/1981

eIDAS: lets fly to the moon
ARF: but you must use a car ....

ECDSA



Anonymous Credentials