

EU Digital Identity & Anonymous Credentials

A Happy End?

Real-World Crypto Symposium 2025

Anja Lehmann



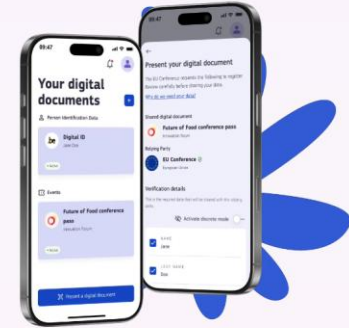
European Digital Identity Wallet (EUDI)

“fully mobile, secure and user-friendly”

A digital ID and personal digital wallet for EU citizens, residents and businesses

EU Digital Identity Wallets will provide a safe, reliable, and private means of digital identification for everyone in Europe. Every Member State will provide at least one wallet to all its citizens, residents, and businesses allowing them to prove who they are, and safely store, share and sign important digital documents.

[Discover the wallet >](#)



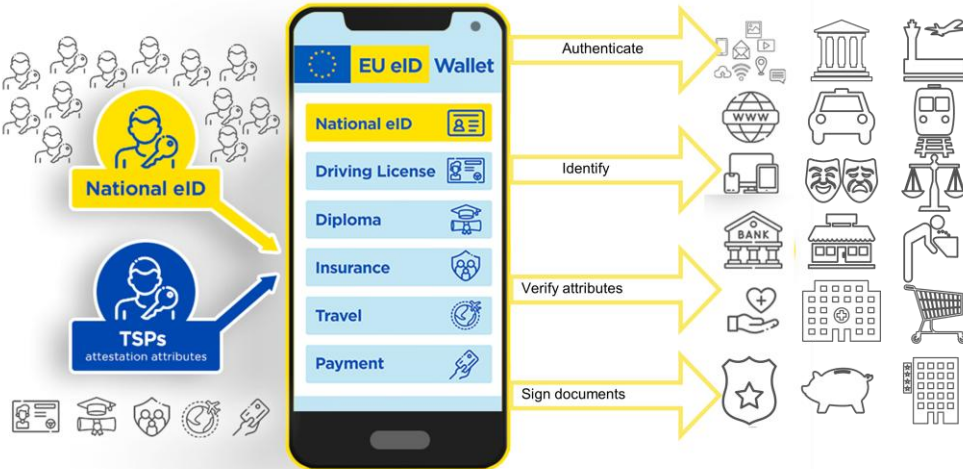
European Digital Identity Wallet (EUDI)

“fully mobile, secure and user-friendly”

Issuer

Holder

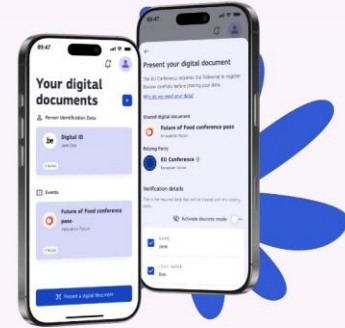
Relying Parties



A digital ID and personal digital wallet for EU citizens, residents and businesses

EU Digital Identity Wallets will provide a safe, reliable, and private means of digital identification for everyone in Europe. Every Member State will provide at least one wallet to all its citizens, residents, and businesses allowing them to prove who they are, and safely store, share and sign important digital documents.

[Discover the wallet >](#)



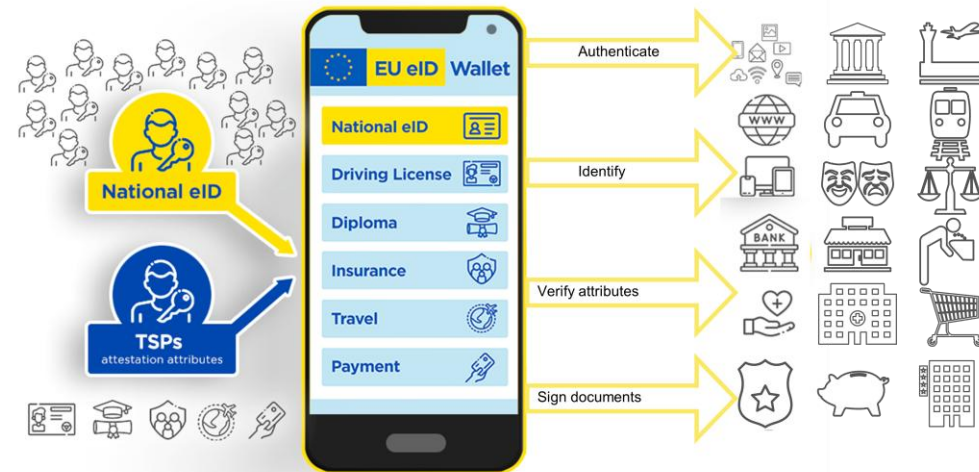
European Digital Identity Wallet (EUDI)

“fully mobile, secure and user-friendly”

Issuer

Holder

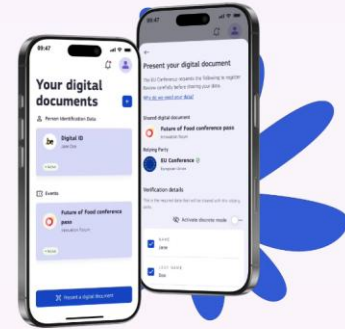
Relying Parties



A digital ID and personal digital wallet for EU citizens, residents and businesses

EU Digital Identity Wallets will provide a safe, reliable, and private means of digital identification for everyone in Europe. Every Member State will provide at least one wallet to all its citizens, residents, and businesses allowing them to prove who they are, and safely store, share and sign important digital documents.

Discover the wallet >



Sign in with Google



Sign in with Apple



Login with Facebook



Sign in with EUDI

EUDI | eIDAS Regulation → Wallet in 2026



- EU regulation eIDAS 2.0 entered into force in May 2024
- All EU member states must provide a EUDI Wallet by end of 2026

- EU regulation eIDAS 2.0 entered into force in May 2024
- All EU member states must provide a EUDI Wallet by end of 2026
- Regulation mandates privacy & security properties

“securely [..] authenticate to relying parties [..] while ensuring **selective disclosure of data** [..]
enable privacy-preserving techniques which ensure **unlinkability** [..]
possibility of users to access services through the use of **pseudonyms** [..]
providers should ensure **unobservability** by not collecting data and not having insight into the
transactions of the users [..]

- EU regulation eIDAS 2.0 entered into force in May 2024
- All EU member states must provide a EUDI Wallet by end of 2026
- Regulation mandates privacy & security properties

“securely [...] authenticate to relying parties [...] while ensuring **selective disclosure of data** [...] enable privacy-preserving techniques which ensure **unlinkability** [...]

~~possibility of users to access services through the use of pseudonyms [...]~~

§ 16. The technical framework of the European Digital Identity Wallet shall:

(a) **not allow providers** of electronic attestations of attributes or any other party, after the issuance of the attestation of attributes, **to obtain data that allows transactions or user behaviour to be tracked, linked or correlated**, or knowledge of transactions or user behaviour to be otherwise obtained, unless explicitly authorised by the user;

(b) enable privacy preserving techniques which ensure unlinkability



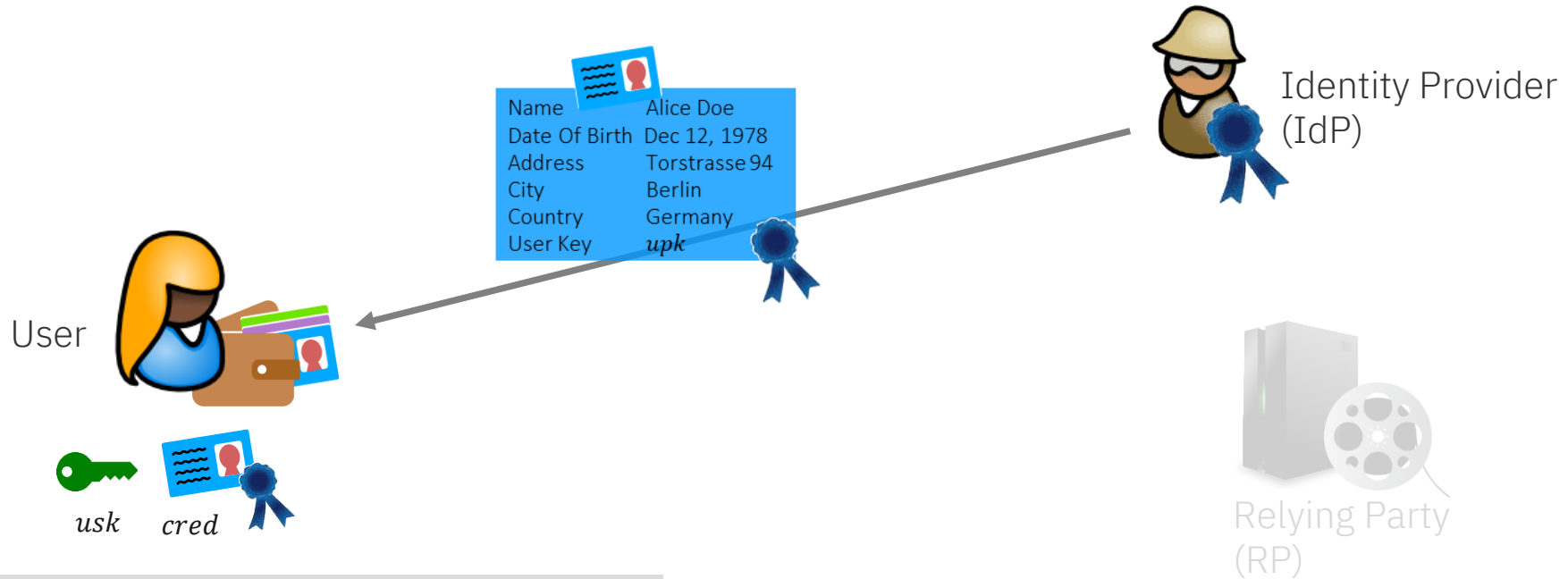
- Architecture Reference Framework (ARF 1.7, March '25) & Implementing Acts:

- Architecture Reference Framework (ARF 1.7, March '25) & Implementing Acts:

ECDSA

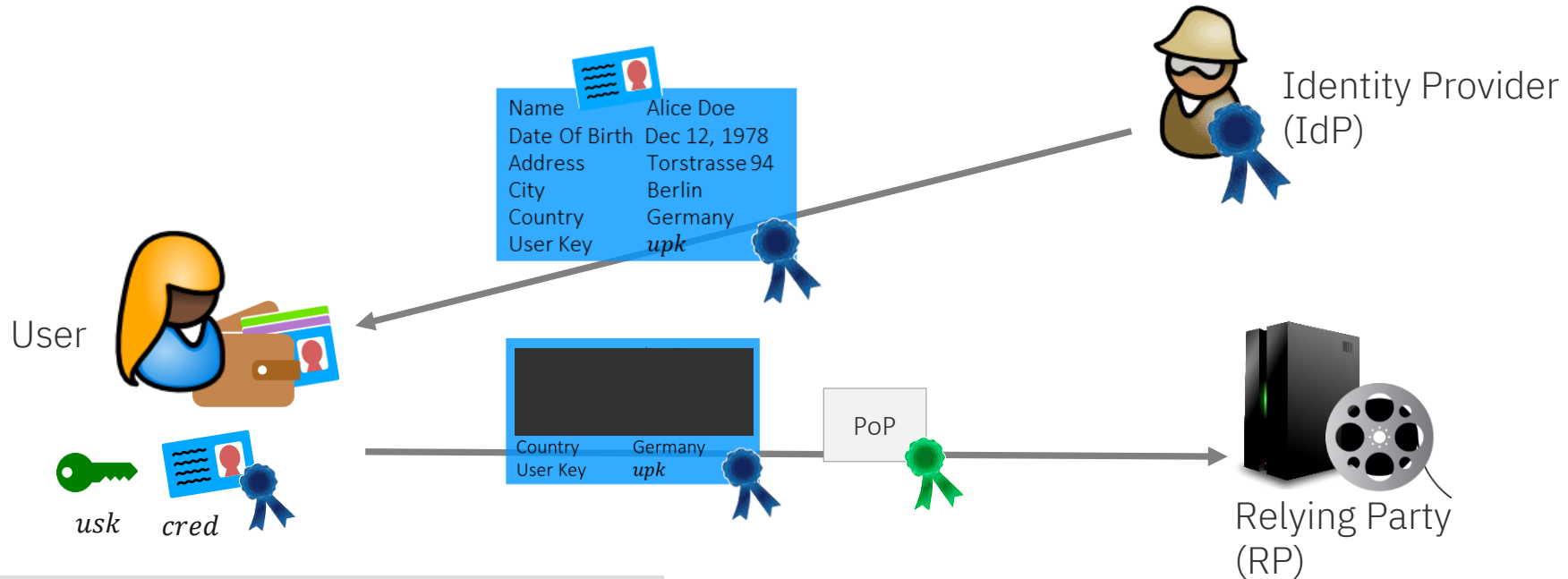
... maybe they did mean “unlikeability” ...

EUDI ARF | Selective Disclosure via Salted Hashes



Random salt $s_1, s_2, \dots, s_\ell$
Attributes $a_1, a_2, \dots, a_\ell$
 $cred = \text{Sign}(isk, (h_1, h_2, \dots, h_\ell))$

EUDI ARF | Selective Disclosure via Salted Hashes

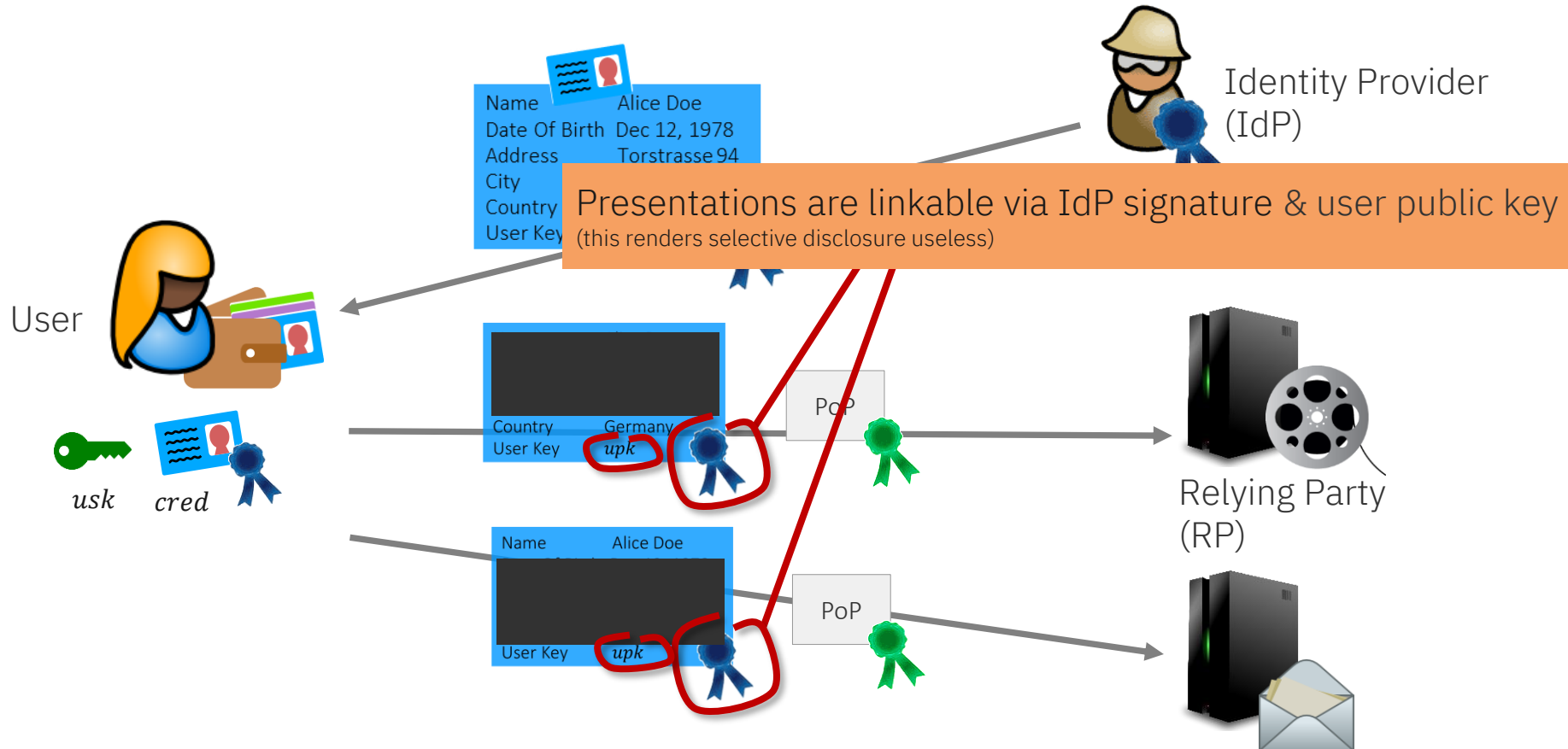


Random salt $s_1, s_2, \dots, s_\ell$
Attributes $a_1, a_2, \dots, a_\ell$

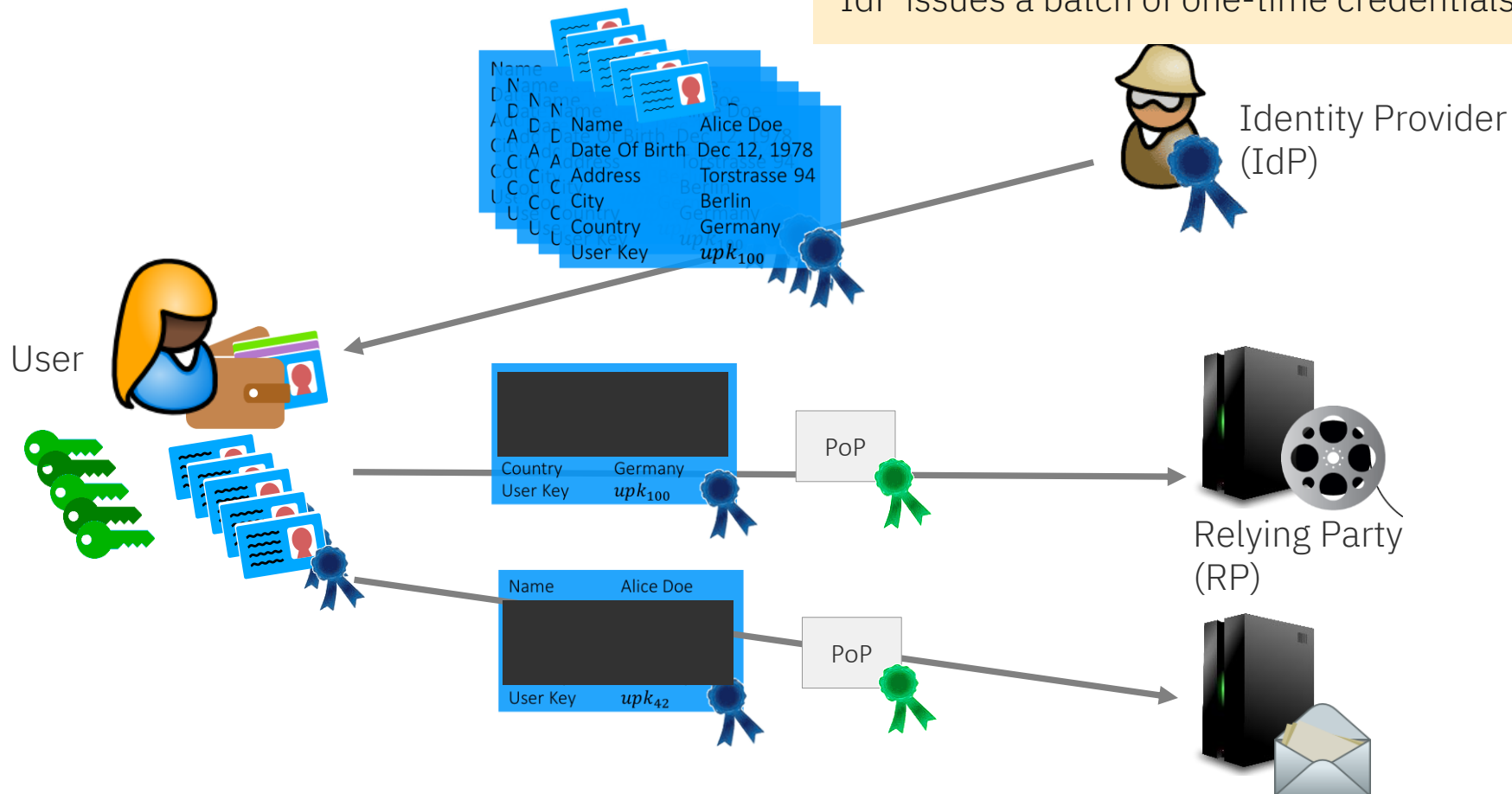
$$cred = Sign(usk, (h_1, h_2, \dots, h_\ell))$$

Selective disclosure

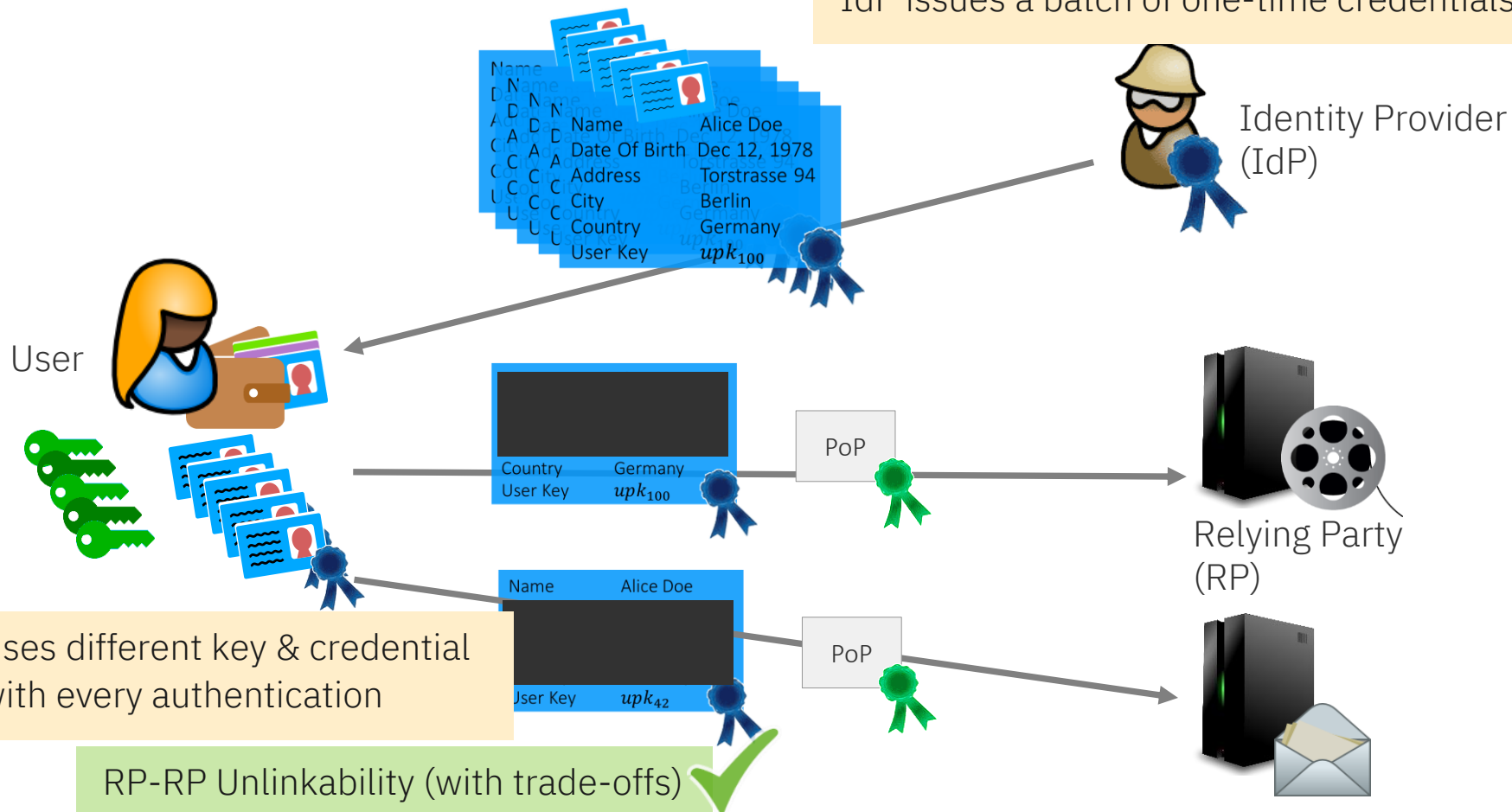




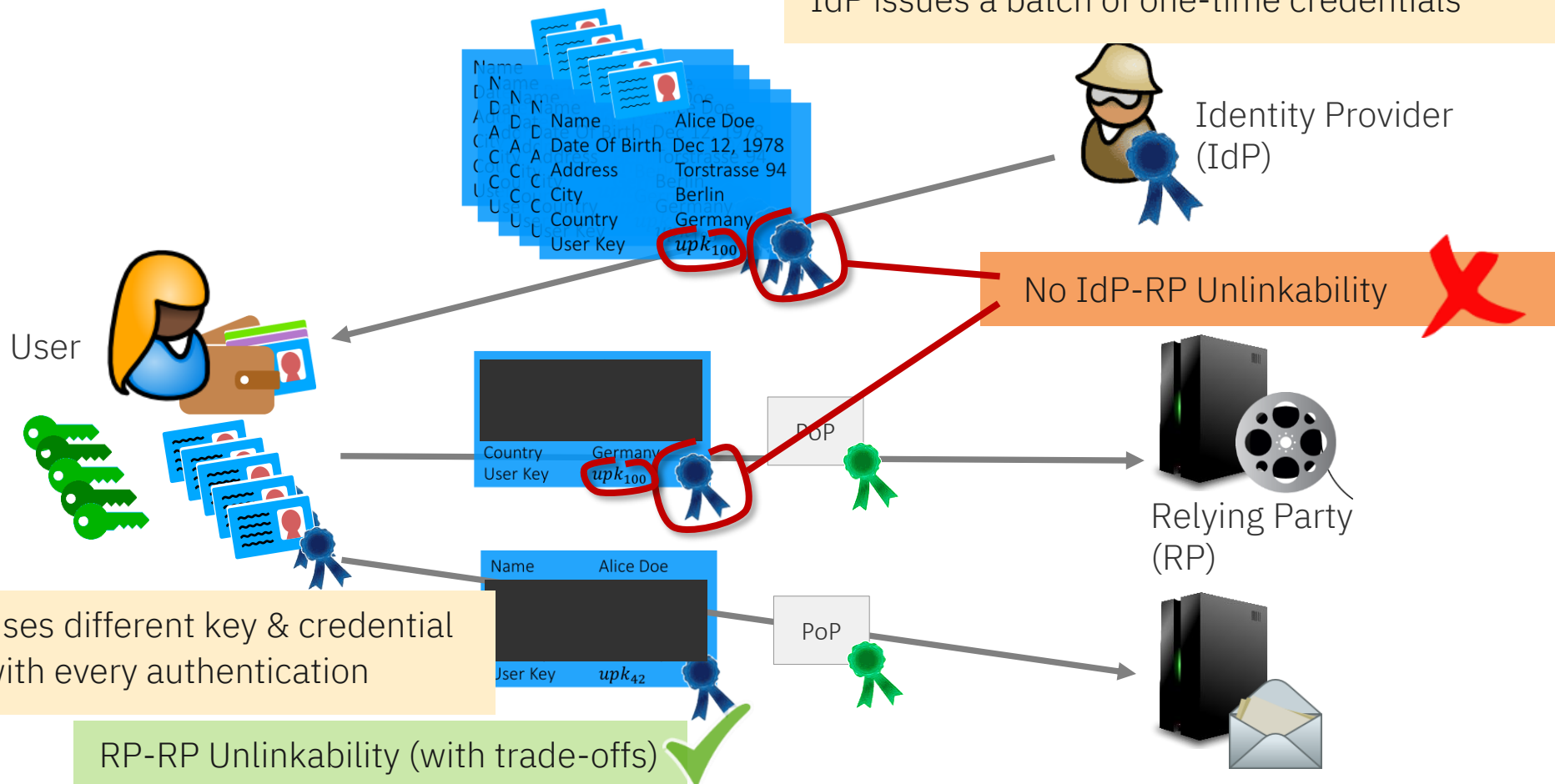
IdP issues a batch of one-time credentials



IdP issues a batch of one-time credentials



IdP issues a batch of one-time credentials



- Current solution does not satisfy unlinkability requirement mandated by eIDAS

Properties	Classic Signatures	„Patched“ Signatures
Unobservability	✓	✓
Selective Disclosure	✗	Salted hashes ✓
RP ↔ RP Unlinkability	✗	Batch issuance ✓
IdP ↔ RP Unlinkability	✗	Impossible ✗

Cryptographers' Feedback on the EUDI ARF

- Current solution does not satisfy unlinkability requirement mandated by eIDAS

... But we have solutions with build-in privacy & unlinkability

Properties	Requirements	Anonymous Credentials
Unobservability		✓
Selective Disclosure		✓
RP ↔ RP Unlinkability		✓
IdP ↔ RP Unlinkability		✓

Cryptographers' Feedback on the EU Digital Identity's ARF

Carsten Baum
Technical University of Denmark

Jaap-Henk Hoepman
Karlstad University
& Radboud University

Anna Lysyanskaya
Brown University

Ngoc Khanh Nguyen
King's College London

Daniel Slamanig
Universität der Bundeswehr München

Søren Eller Thomsen
Partisia

Olivier Blazy
École Polytechnique

Eysa Lee
Brown University

René Mayrhofer
Johannes Kepler University Linz

Bart Preneel
KU Leuven

abhi shelat
Northeastern University

Stefano Tessaro
University of Washington

Carmela Troncoso
EPFL

Jan Camenisch
Dfinity

Anja Lehmann
Hasso-Plattner-Institute,
University of Potsdam

Hart Montgomery*

June 2024

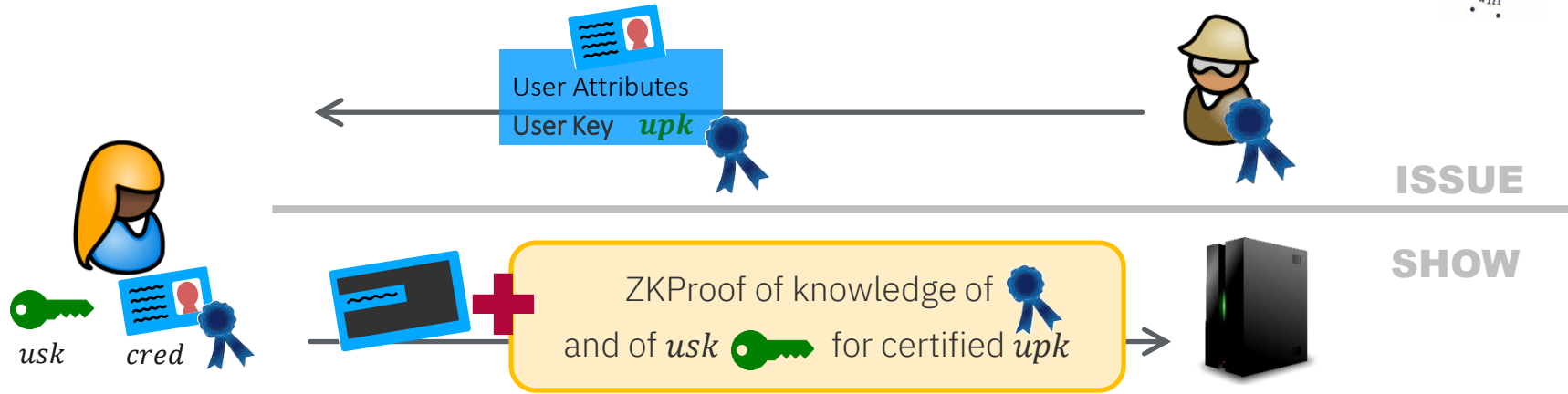
Executive Summary

The eIDAS 2.0 regulation (electronic identification and trust services) that defines the new EU Digital Identity Wallet (EUDIW) is an important step towards developing interoperable digital identities in Europe for the public and private sectors. The regulation, if realized with the right technology, can make Europe the front runner in private and secure identification mechanisms in the digital space, and act as a template for future digital identity systems in other regions.

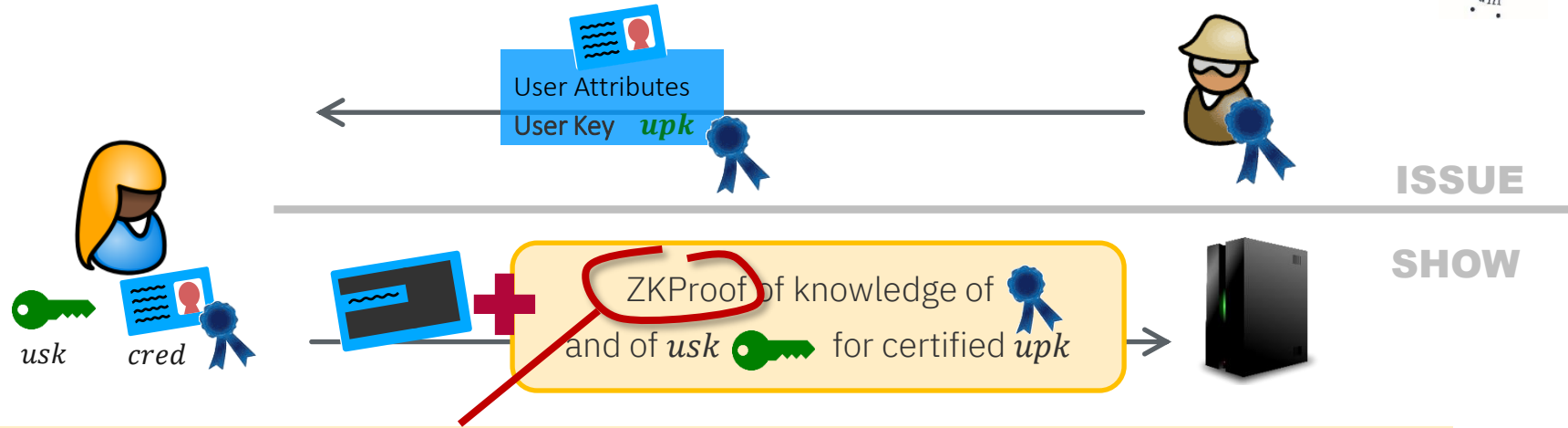
Unfortunately, we believe that some of the currently suggested design aspects of the EUDI and its debate in the Digital Identity regulation. The main reason for this shortcoming in the current proposal is that it relies on cryptographic methods that were never designed for such requirements. We propose a way to fix the proposed solution to meet all the privacy features that a larger redesign is in order.

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

Anonymous Credentials | Privacy through ZKPs



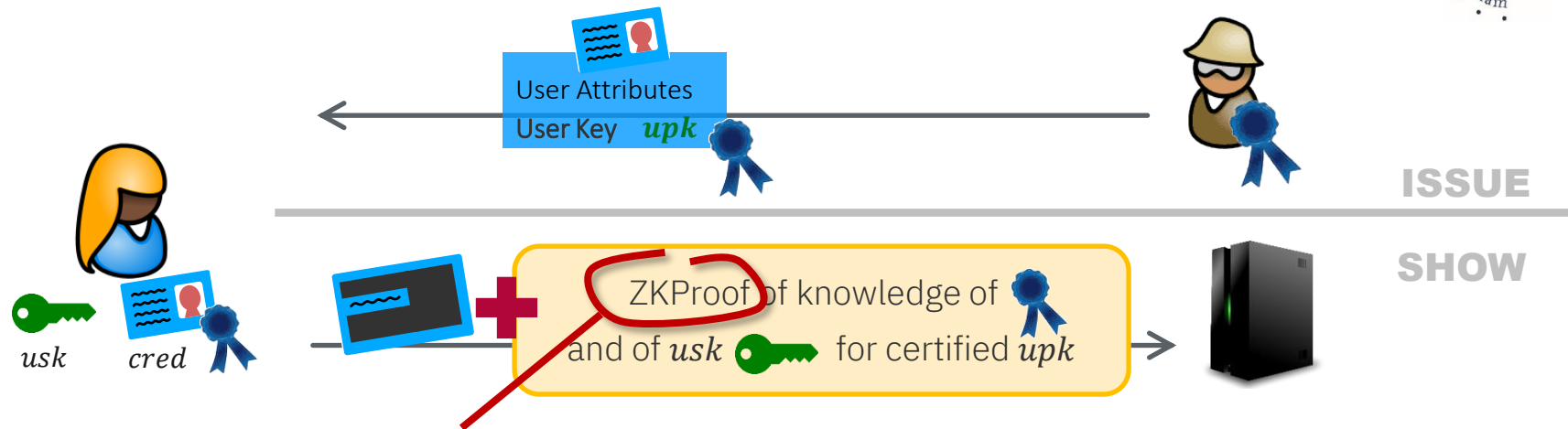
Anonymous Credentials | Privacy through ZKPs



Zero-Knowledge Proof (ZKP)

Proof of a statement that reveals *nothing* beyond validity

Anonymous Credentials | Privacy through ZKPs



Zero-Knowledge Proof (ZKP)

Proof of a statement that reveals *nothing* beyond validity

Here: user proves she owns *cred* from IdP on the revealed attributes & knows *usk* but reveals nothing about IdP's signature, her *usk* or *upk* (!)

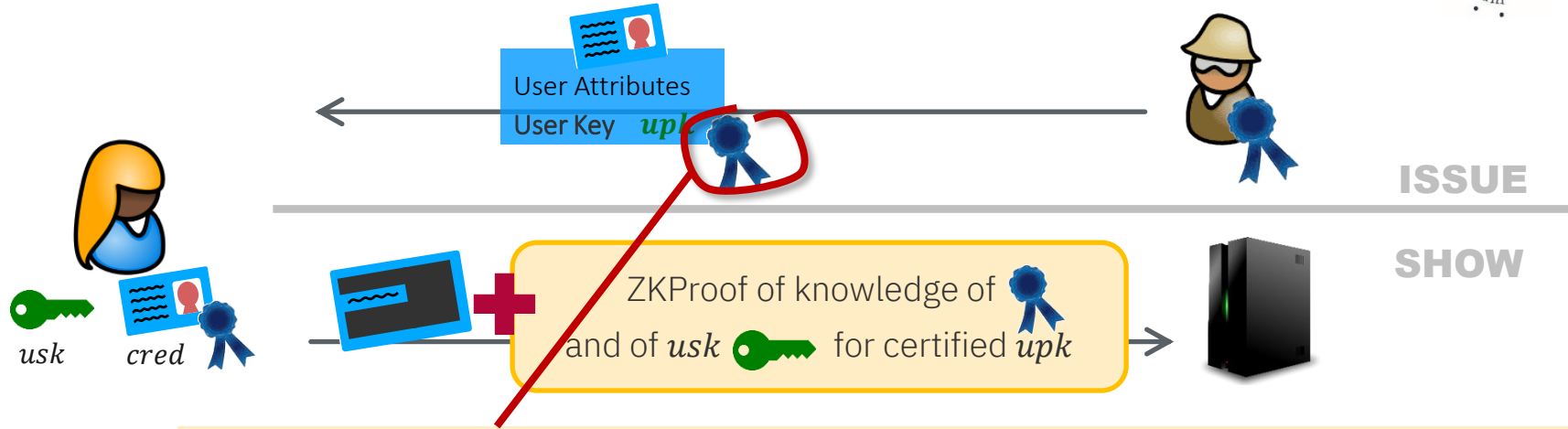
Multi-Show RP-RP & IdP-RP Unlinkability



Selective disclosure

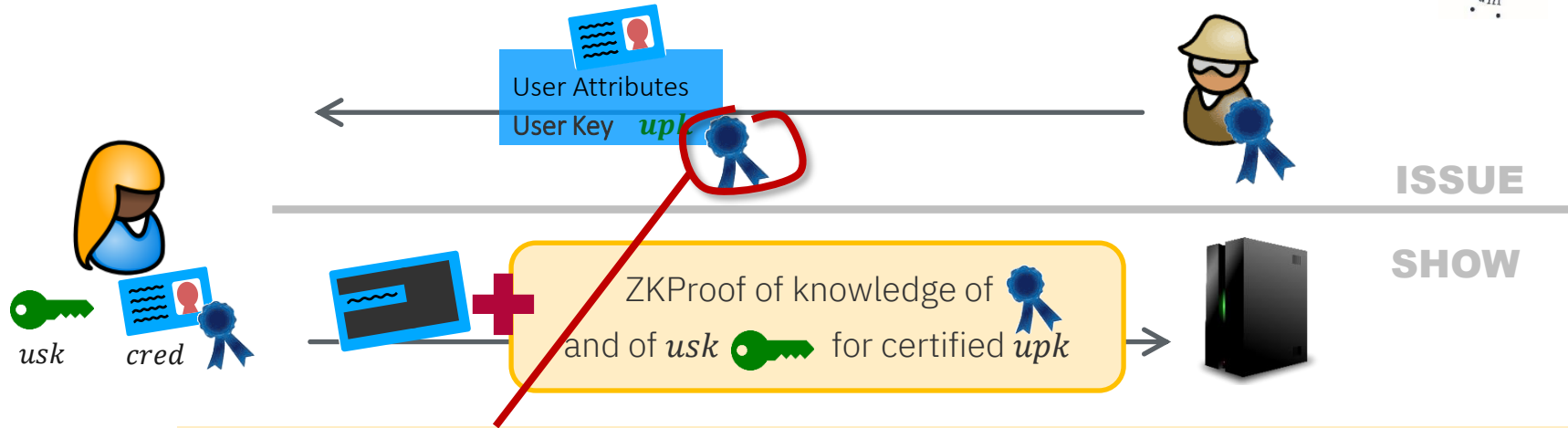


Anonymous Credentials | Signatures with ZKPs



Needs signature scheme (for IdP) that allows for efficient ZKP of a signature

Anonymous Credentials | Signatures with ZKPs

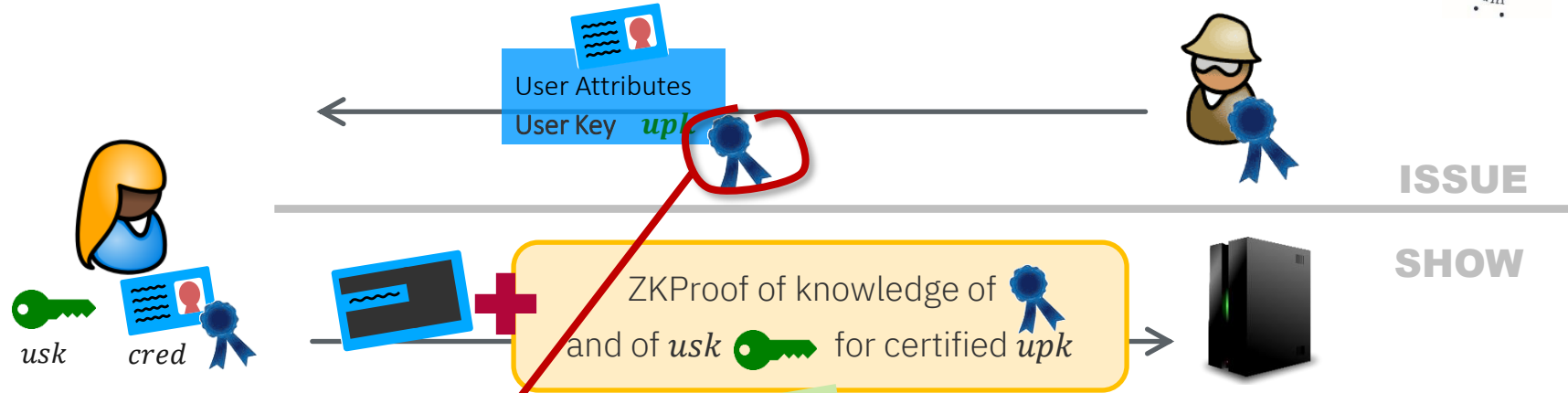


Needs signature scheme (for IdP) that allows for efficient ZKP of a signature

Option 1 | Dedicated signature scheme with „build-in“ ZKP-capabilities
E.g., CL/BBS/PS-signatures

Option 2 | Use any signature scheme (e.g., ECDSA) & generic (circuit-based) ZKP
Legacy-compatible, but less efficient & more complex

Anonymous Credentials | Signatures with ZKPs



Needs signature scheme that allows for efficient ZKP of a signature

Most mature (20 years), complete & efficient

Option 1 | Dedicated signature scheme with „build-in“ ZKP-capabilities

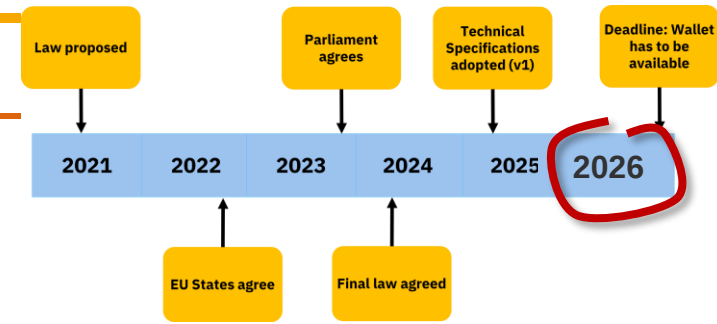
E.g., CL(BBS)PS-signatures

Option 2 | Use any signature scheme (e.g., ECDSA) & generic (circuit-based) ZKP

Legacy-compatible, but less efficient & more complex

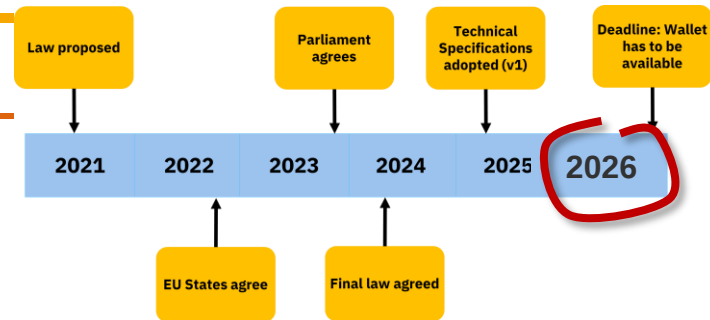
Why was BBS (or alike) not used?

- EUDI Wallet must be ready for 500 Mio users by 2026!
- Gets built from what is available today



Why was BBS (or alike) not used?

- EUDI Wallet must be ready for 500 Mio users by 2026!
- Gets built from what is available today



1) Crypto must be in SOG-IS catalogue

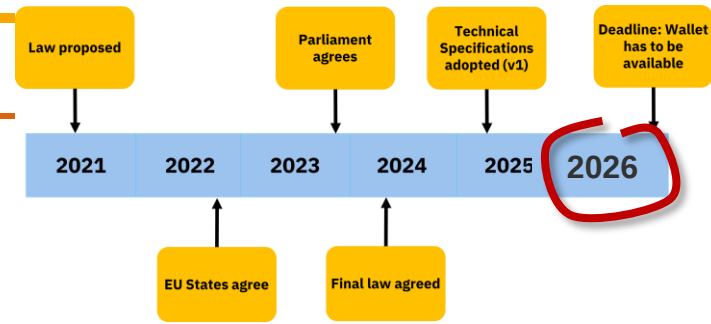
Set of approved crypto algorithms in Europe

ECDSA, Schnorr, RSA

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

Why was BBS (or alike) not used?

- EUDI Wallet must be ready for 500 Mio users by 2026!
- Gets built from what is available today



1) Crypto must be in SOG-IS catalogue

Set of approved crypto algorithms in Europe

ECDSA, Schnorr, RSA

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

2) Credential must be bound to hardware-protected device key

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

Secure Elements/OS provide ECDSA APIs



How to get Anonymous Credentials into EUDI

	BBS	ECDSA & zkSNARK
Research & Validation	Through test of time, 20 years of research 	
SOG-IS Approval & Standards		
Device Binding		No changes 

How to get Anonymous Credentials into EUDI

Next 4 talks

	BBS	ECDSA & zkSNARK
Research & Validation	Through test of time, 20 years of research 	Ongoing research Best protocol ?  Tooling support
SOG-IS Approval & Standards		
Device Binding		No changes 

How to get Anonymous Credentials into EUDI

	BBS	ECDSA & zkSNARK
Research & Validation	Through test of time, 20 years of research 	Ongoing research Best protocol ? Tooling support 
SOG-IS Approval & Standards	BBS IETF Drafts (core sign + nyms + blind issuance)  Update of ISO/IEC 20008-2 planned (2014, TPM DAA, contains BBS core signature) Pairing Curve Standard IETF draft expired in 2022! Main reference is a blog post by electriccoin.co for BLS12-381 	
Device Binding		No changes 

How to get Anonymous Credentials into EUDI

	BBS	ECDSA & zkSNARK
Research & Validation	Through test of time, 20 years of research 	Ongoing research  Best protocol ? Tooling support
SOG-IS Approval	BBS IETF Drafts (core sign + nyms + blind issuance)  Update of ISO/IEC 20008-2 planned (2014, TPM DAA, contains BBS core signature)	ECDSA 
& Standards	Pairing Curve Standard  IETF draft expired in 2022! Main reference is a blog post by electriccoin.co for BLS12-381	Standards for Circuits & zkSNARKs & Pairings? 
Device Binding		No changes 

How to get Anonymous Credentials into EUDI

Next 4 talks

	BBS	ECDSA & zkSNARK
Research & Validation	Through test of time, 20 years of research 	Ongoing research  Best protocol ? Tooling support
SOG-IS Approval	BBS IETF Drafts (core sign + nyms + blind issuance)  Update of ISO/IEC 20008-2 planned (2014, TPM DAA, contains BBS core signature)	ECDSA 
& Standards	Pairing Curve Standard  IETF draft expired in 2022! Main reference is a blog post by electriccoin.co for BLS12-381	Standards for Circuits & zkSNARKs & Pairings? 
Device Binding	API for Schnorr signature over $\mathbb{G}_1$, or Protocol that bridges ECDSA with BBS 	No changes 

How to get Anonymous Credentials into EUDI

	BBS	ECDSA & zkSNARK
Research & Validation	Through test of time, 20 years of research 	Ongoing research Best protocol ?  Tooling support
SOG-IS Approval	BBS IETF Drafts (core sign + nyms + blind issuance)  Update of ISO/IEC 20008-2 planned (2014, TPM DAA, contains BBS core signature)	ECDSA 
& Standards	Pairing Curve Standard IETF draft expired in 2022!  Main reference is a blog post by electriccoin.co for BLS12-381	Standards for Circuits & zkSNARKs & Pairings? 
Device Binding	API for Schnorr signature over $\mathbb{G}_1$, or Protocol that bridges ECDSA with BBS  Cloud HSM solution (e.g., used in Germany)	No changes 

How to get Anonymous Credentials into EUDI

	BBS	ECDSA & zkSNARK
Research & Validation	Through test of time, 20 years of research 	Ongoing research  Best protocol ? Tooling support
SOG-IS Approval & Standards	BBS IETF Drafts (core sign + nyms + blind issuance)  Update of ISO/IEC 20008-2 planned (2014, TPM DAA, contains BBS core signature) Pairing Curve Standard IETF draft expired in 2022! Main reference is a blog post by electriccoin.co for BLS12-381 Pairing-free variants (require interaction) BBS# (Orange) & SAAC 	ECDSA  Standards for Circuits & zkSNARKs & Pairings? 
Device Binding	API for Schnorr signature over $\mathbb{G}_1$, or Protocol that bridges ECDSA with BBS  Cloud HSM solution (e.g., used in Germany)	No changes 

How to get Anonymous Credentials into EUDI

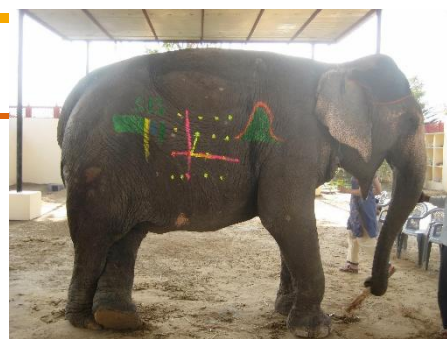
Next 4 talks

	BBS	ECDSA & zkSNARK
Research & Validation	Through test of time, 20 years of research 	Ongoing research  Best protocol ? Tooling support
SOG-IS Approval	BBS IETF Drafts (core sign + nyms + blind issuance)  Update of ISO/IEC 20008-2 planned (2014, TPM DAA)	ECDSA 
& Standards	Pairing Curve Standard Anyone interested in picking this up? Consensus on pairing curve with 192-bit security?	Standards for Circuits & zkSNARKs & Pairings?  BBS# (Orange) & SAAC 
Device Binding	API for Schnorr signature over $\mathbb{G}_1$, or Protocol that bridges ECDSA with BBS  Cloud HSM solution (e.g., used in Germany)	No changes 

Post-Quantum vs. Post-Privacy?

- Does it make sense to deploy new DL-based crypto? PQC!
 - But, PQC less time-critical for authentication than for encryption
 - NIST 2024 report on PQC transition

*"Authentication systems may continue to use quantum-vulnerable algorithms **until quantum computers** that are capable of breaking current, quantum-vulnerable algorithms **become available.**"*

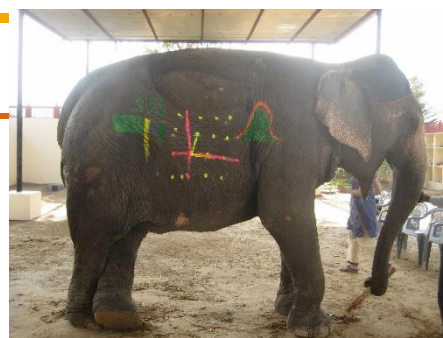


Post-Quantum vs. Post-Privacy?

- Does it make sense to deploy new DL-based crypto? PQC!
 - But, PQC less time-critical for authentication than for encryption
 - NIST 2024 report on PQC transition

*"Authentication systems may continue to use quantum-vulnerable algorithms **until quantum computers** that are capable of breaking current, quantum-vulnerable algorithms **become available**."*

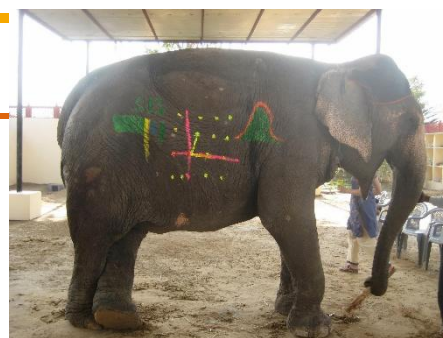
- If real-world focus is solely on PQC transition for encryption and signatures:
Are we giving up deployment for (non-PQC) advanced and privacy-preserving crypto ?



Post-Quantum vs. Post-Privacy?

- Does it make sense to deploy new DL-based crypto? PQC!
 - But, PQC less time-critical for authentication than for encryption
 - NIST 2024 report on PQC transition

*"Authentication systems may continue to use quantum-vulnerable algorithms **until quantum computers** that are capable of breaking current, quantum-vulnerable algorithms **become available**."*



- If real-world focus is solely on PQC transition for encryption and signatures:
Are we giving up deployment for (non-PQC) advanced and privacy-preserving crypto ?
- Identity infrastructure is being built now! Based on „ECDSA mindset“
If we don't propose a viable solution now → lack of privacy will manifest

Short/Midterm (non-PQC)

- Show feasibility and benefits
- Shape requirements and use cases



Know-Your-Customer (KYC)
e.g., opening bank account

Age Proofs

Digital Identity with Privacy

There is no need for privacy!

Short/Midterm (non-PQC)

- Show feasibility and benefits
- Shape requirements and use cases

Security

Know-Your-Customer (KYC)
e.g., opening bank account

Privacy

Age Proofs

Does this really have to be LoA high and come with 24h revocation guarantees?

Digital Identity with Privacy

There is no need for privacy!

Short/Midterm (non-PQC)

- Show feasibility and benefits
- Shape requirements and use cases

Security

Know-Your-Customer (KYC)
e.g., opening bank account

This is where anonymous
credentials can have most
impact

Privacy

Age Proofs

Does this really have to be LoA high and come
with 24h revocation guarantees?

There is no need for privacy!

Short/Midterm (non-PQC)

- Show feasibility and benefits
- Shape requirements and use cases
- ZKP-compatible protocols (OIDC4Vx) & data formats

Ensure application layer support e.g., for:

- Presentation $\neq$ Credential
- Conditional disclosure
- Composite proofs
- Blind issuance
- Pseudonyms

→ Provides concrete target for PQC research

Security
Privacy

Know-Your-Customer (KYC)
e.g., opening bank account

This is where anonymous
credentials can have most
impact

Age Proofs

Does this really have to be LoA high and come
with 24h revocation guarantees?

There is hope for a ZKP-based EUDI

- EU opened discussion on ZKP
- ZKP integration planned for ARF 2.0

<https://github.com/eu-digital-identity-wallet/eudi-doc-architecture-and-reference-framework/blob/main/docs/discussion-topics/g-zero-knowledge-proof.md>

This is all public and open for cryptographers' input

Technical Specifications

The initial drafts of the following technical specifications will be developed from **March 7, 2025, to August 15, 2025**. Each specification includes links to its corresponding GitHub discussion area and roadmap issue.

Id	Title	Discussion area	Roadmap issue
TS01	EUDI Wallet Trust Mark	Discussion area	Roadmap issue
TS02	Notification and Publication of Provider Information	Discussion area	Roadmap issue
TS03	Specification of Wallet Unit Attestation (WUA)	Discussion area	Roadmap issue
TS04	Zero-Knowledge Proof (ZKP) Implementation in EUDI Wallet	Discussion area	Roadmap issue

There is hope for a ZKP-based EUDI

- EU opened discussion on ZKP
- ZKP integration planned for ARF 2.0

<https://github.com/eu-digital-identity-wallet/eudi-doc-architecture-and-reference-framework/blob/main/docs/discussion-topics/g-zero-knowledge-proof.md>

This is all public and open for cryptographers' input

Technical Specifications

The initial drafts of the following technical specifications will be developed from **March 7, 2025, to August 15, 2025**. Each specification includes links to its corresponding GitHub discussion area and roadmap issue.

Id	Title	Discussion area	Roadmap issue
TS01	EUDI Wallet Trust Mark	Discussion area	Roadmap issue
TS02	Notification and Publication of Provider Information	Discussion area	Roadmap issue
TS03	Specification of Wallet Unit Attestation (WUA)	Discussion area	Roadmap issue
TS04	Zero-Knowledge Proof (ZKP) Implementation in EUDI Wallet	Discussion area	Roadmap issue

- Wallet attestation must be unlinkable too!
- Many more interesting topics, e.g., key blinding, key derivation (for batch issuance)
- Interested in getting involved? Postdoc position available ☺

Contact: anja.lehmann@hpi.de

Further References

SOG-IS catalogue:

<https://sogis.eu/documents/cc/crypto/SOGIS-Agreed-Cryptographic-Mechanisms-1.3.pdf>

IETF BBS Drafts: need review and support

<https://datatracker.ietf.org/doc/draft-irtf-cfrg-bbs-signatures>

<https://datatracker.ietf.org/doc/draft-irtf-cfrg-bbs-blind-signatures/>

<https://datatracker.ietf.org/doc/draft-irtf-cfrg-bbs-per-verifier-linkability/>

IETF Pairing-friendly Curves: expired & needs revival

<https://datatracker.ietf.org/doc/draft-irtf-cfrg-pairing-friendly-curves/>

The BBS# Protocol (Orange)

Nicolas Desmoulins, Antoine Dumanois, Seyni Kane, and Jacques Traoré

https://github.com/user-attachments/files/19198669/The_BBS_Sharp_Protocol.pdf

Server-Aided Anonymous Credentials

Rutchathon Chairattana-Apirom, Franklin Harding, Anna Lysyanskaya, and Stefano Tessaro

<https://ia.cr/2025/513>