Anonymous Credentials for the EUDI Wallet: Closing the Gaps

EUDI ON – 25.6.2026

Andrea Flamini Anja Lehmann Alexandros Zacharakis

HPI Hasso Plattner Institut
Digital Engineering · Universität Potsdam

EUDI Wallet | Privacy Requirements in eIDAS

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

(a) **not allow providers** of electronic attestations of attributes [..], after the issuance of the attestation of attributes, **to obtain data that allows transactions or user behaviour** to be **tracked, linked or correlated**, [..]

(b) enable privacy preserving techniques which ensure ~~unlikeability~~

Corrigendum 9.4.25: unlinkability! ☺

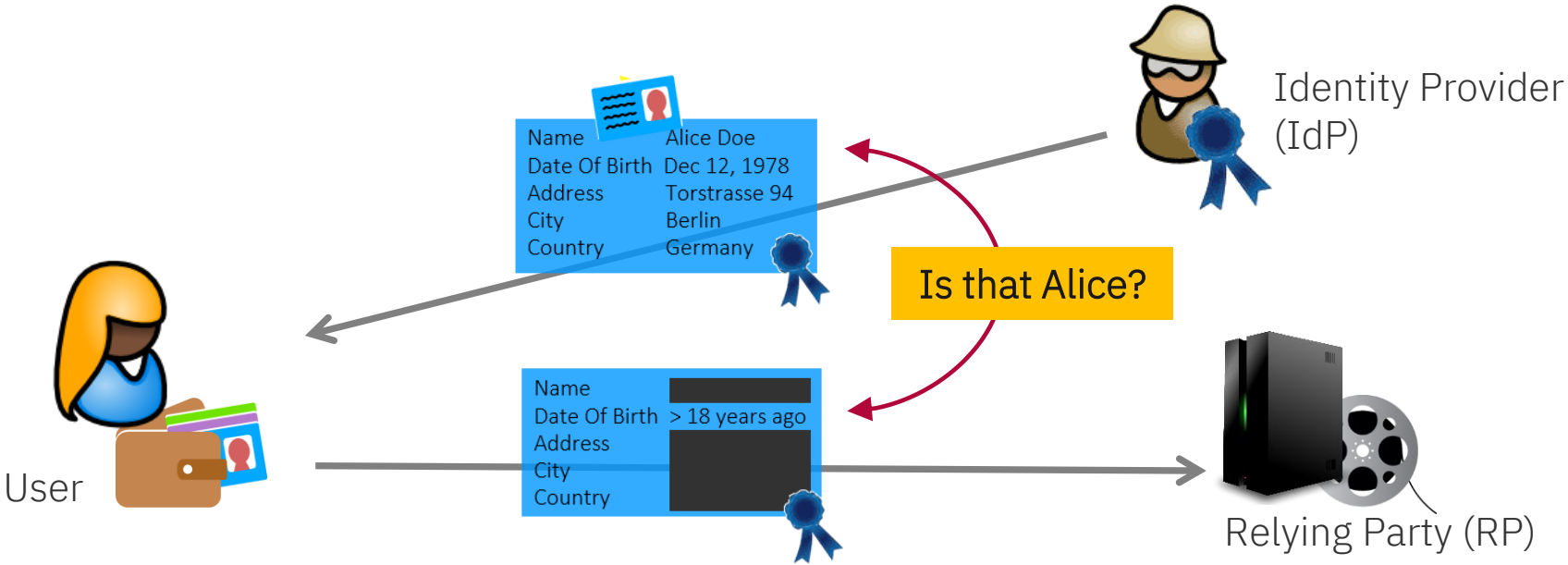
EUDI Wallet | Privacy Requirements in eIDAS

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

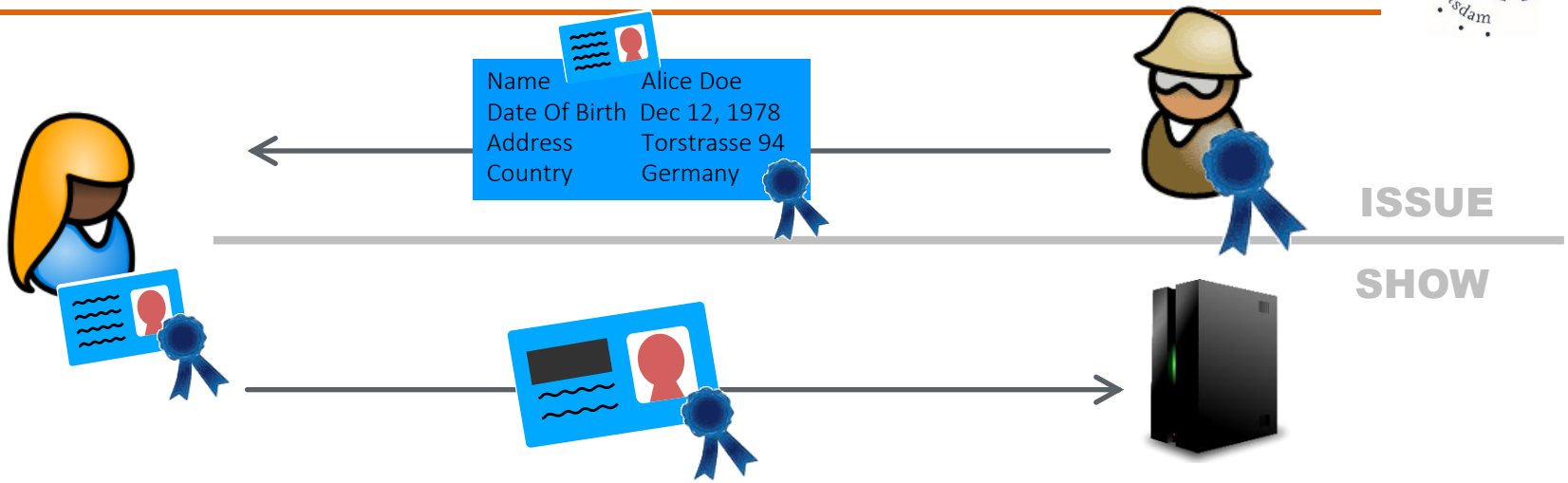
(a) **not allow providers** of electronic attestations of attributes [..], after the issuance of the attestation of attributes, **to obtain data that allows transactions or user behaviour** to be **tracked, linked or correlated**, [..]

(b) enable privacy preserving techniques which ensure ~~unlikeability~~

Corrigendum 9.4.25: **unlinkability**! ☺

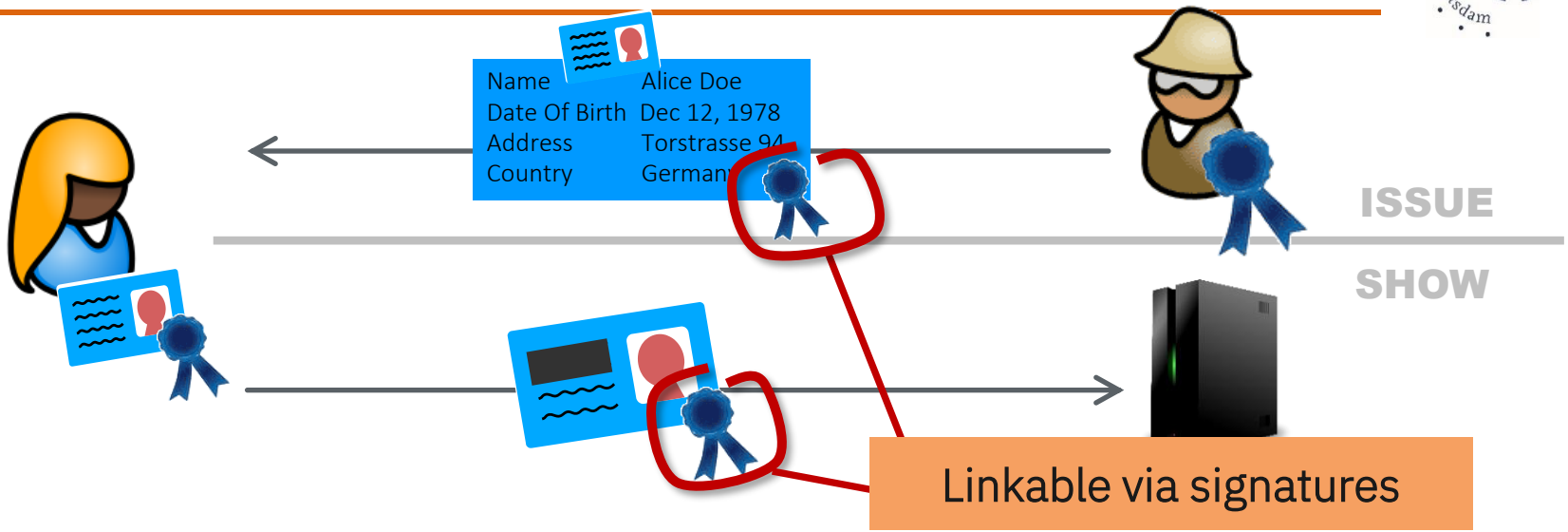


EUDI | Solution with Classical Signatures



- Digital identity credentials based on cryptographic signatures

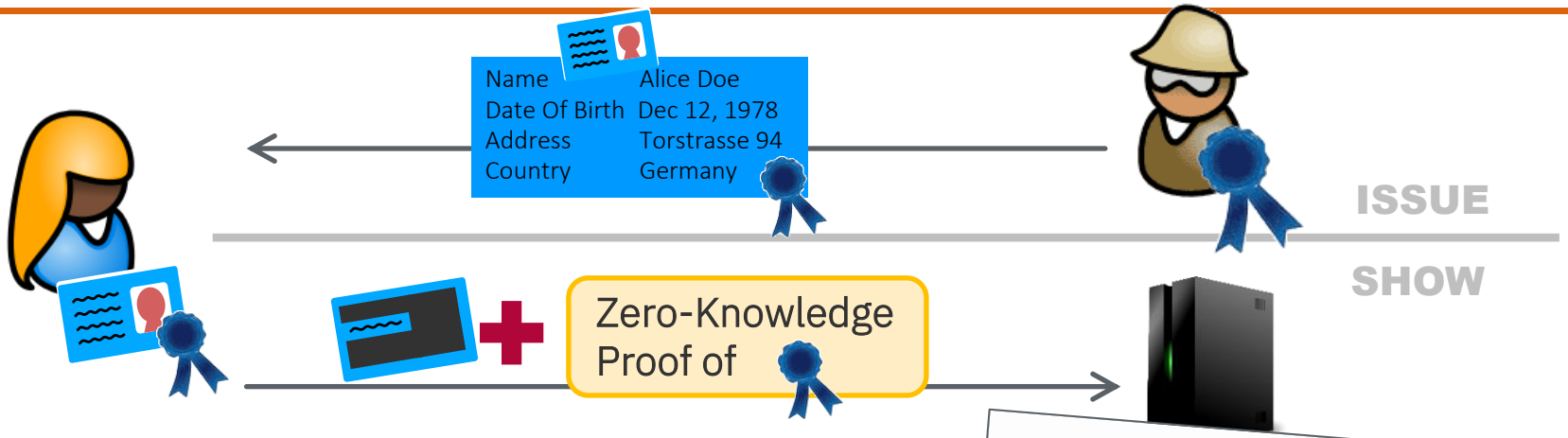
EUDI | Solution with Classical Signatures

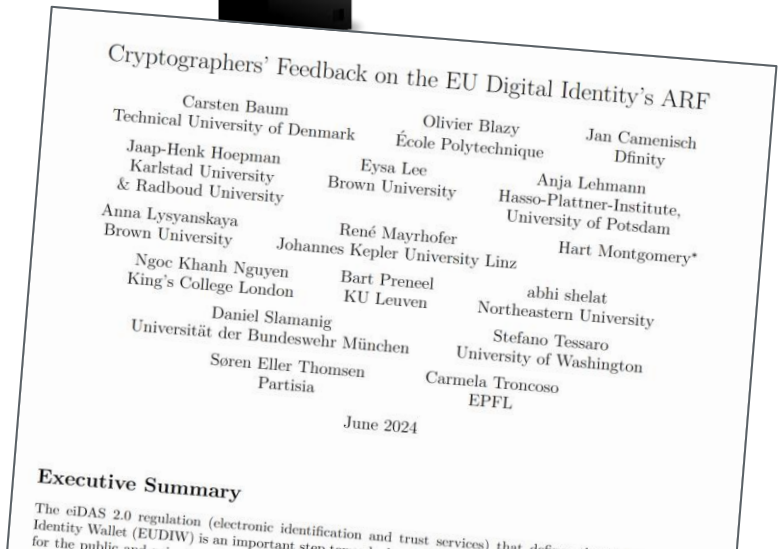


- Digital identity credentials based on cryptographic signatures
- Digital Signatures are great for security, but bad for privacy → unique identifier
- Batch issuance helps for unlinkability towards RPs (but is rather costly)

  & does **not achieve** unlinkability/untraceability if IdP and RP collude

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

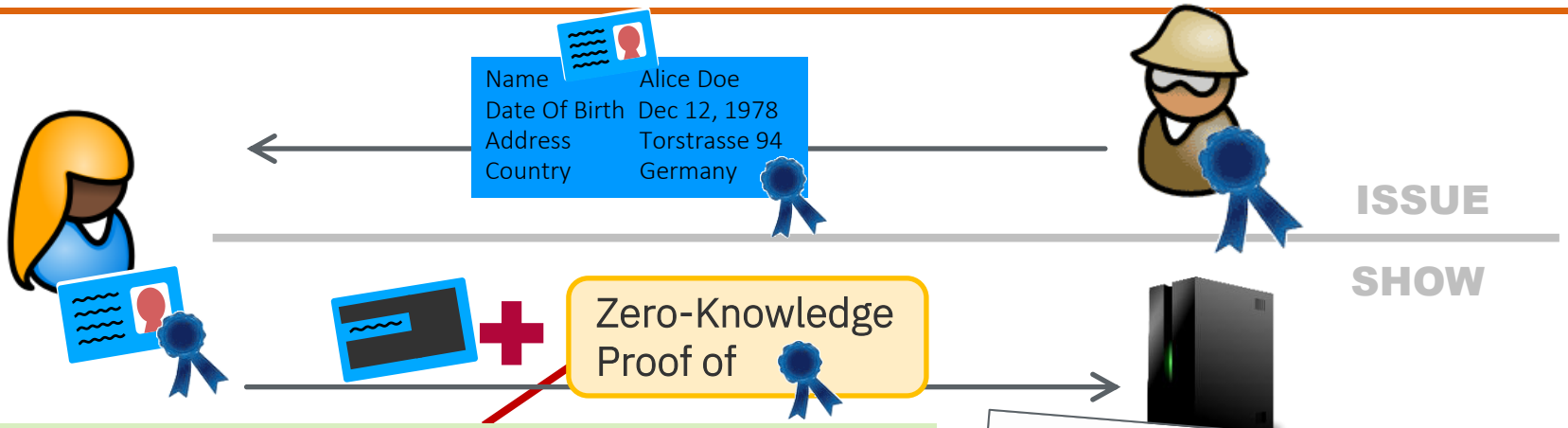
June 2024

Executive Summary

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

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

Anonymous Credentials & Zero-Knowledge Proofs

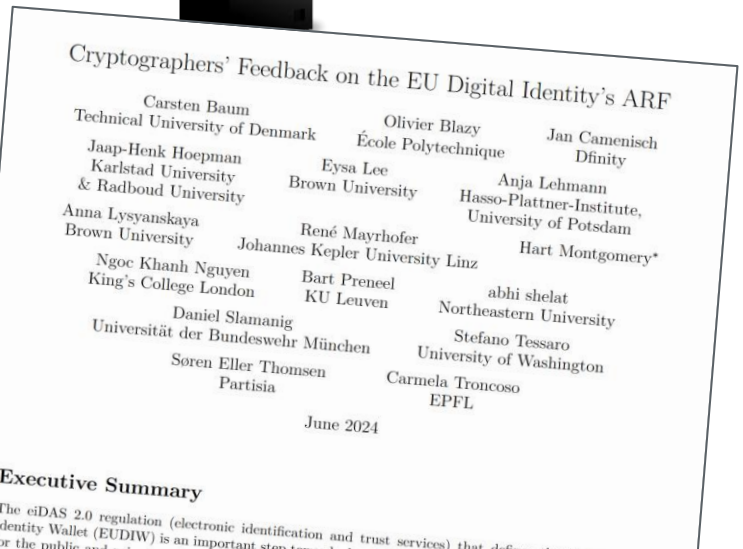


Zero-Knowledge Proof (ZKP)

Proof that reveals nothing beyond validity

→ multi-show unlinkability & no trust on IdP needed

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

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

Why does EUDI not use Anonymous Credentials (yet) ?

- Main focus so far: PID, i.e., national identity card

This comes with strong security requirements:

1) Must only use “Agreed Cryptographic Mechanisms”
2) Security on Level of Assurance High

→ ZKP not included in ACM or supported by secure hardware

KYC e.g., opening bank account

Why does EUDI not use Anonymous Credentials (yet) ?

- Main focus so far: PID, i.e., national identity card

This comes with strong security requirements:

1) Must only use “Agreed Cryptographic Mechanisms”
2) Security on Level of Assurance High

→ ZKP not included in ACM or supported by secure hardware

- Most high-security PID-based use cases don't need strong privacy

  Adding lightweight ZKPs would still offer better privacy and security though

KYC e.g., opening bank account

Why does EUDI not use Anonymous Credentials (yet) ?

- Main focus so far: PID, i.e., national identity card

This comes with strong security requirements:

1) Must only use “Agreed Cryptographic Mechanisms”
2) Security on Level of Assurance High

→ ZKP not included in ACM or supported by secure hardware

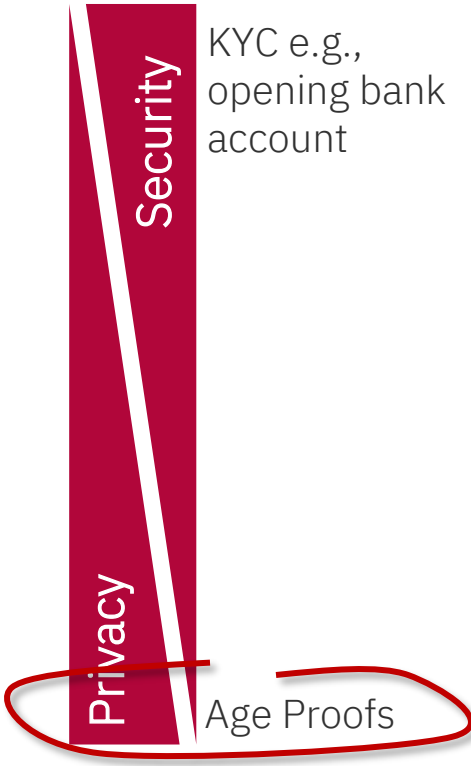
- Most high-security PID-based use cases don't need strong privacy

  Adding lightweight ZKPs would still offer better privacy and security though

- Current attention: age verification online (from age credential ≠ PID)

  High privacy needs, but lower security requirements than KYC

  Right setting to deploy anonymous credentials

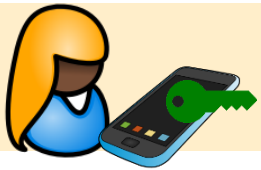


Towards Deploying Anonymous Credentials

1 | Standardisation of all required cryptographic protocols → interoperability

IETF: ongoing standards for all core crypto primitives (e.g., BBS)
ETSI: dedicated standard for ZKP-based EUDI Wallet under development

2 | Realize cloning-prevention for anonymous credentials
Usually done through device binding



→ Challenge: Secure Elements only support non-ZKP friendly signatures (ECDSA)

3 | Ensure that privacy is strong enough for real-world use case, e.g., for age proofs

→ Challenge: (Anonymous) Credentials usually reveal the issuer‘s identity

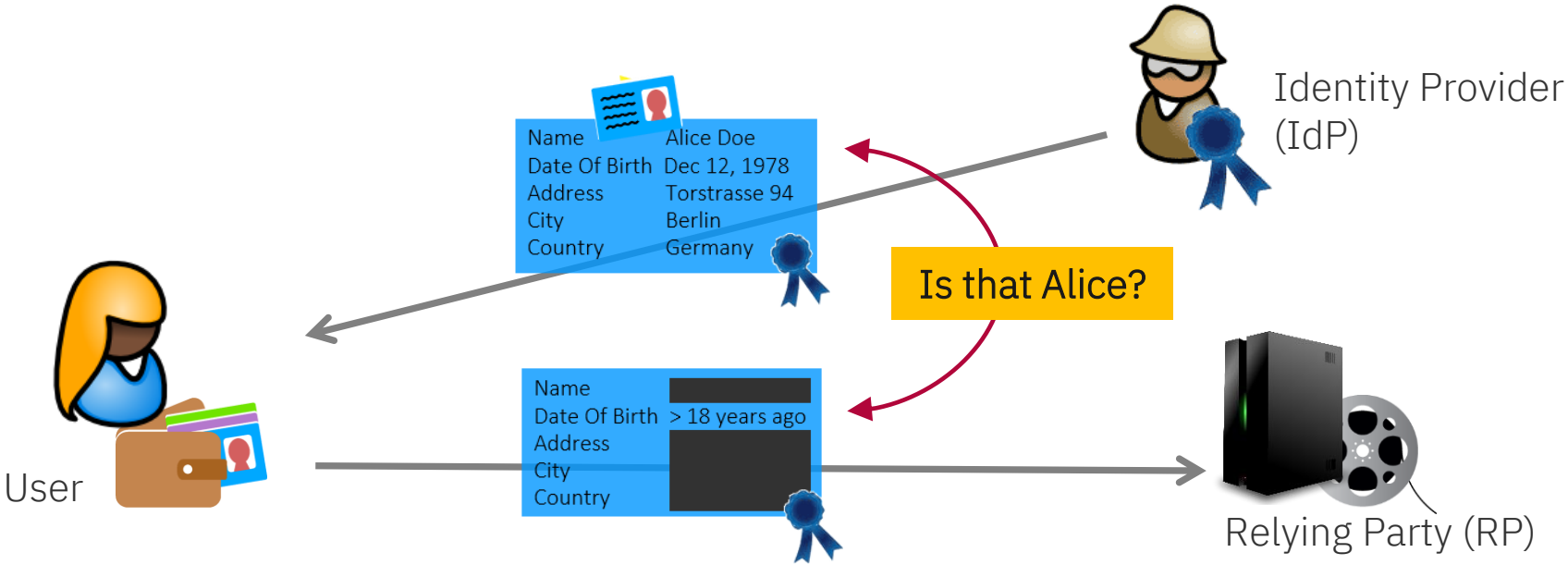
Device Binding for Anonymous Credentials

Alexandros Zacharakis

based on joint work with Sofia Celi, Anja Lehmann and Shai Levin

Recall Unlinkability

- Presentations cannot be traced back to a credential.
- Great for privacy! But...
- Makes misuse easier.



Credential Transfer/Cloning

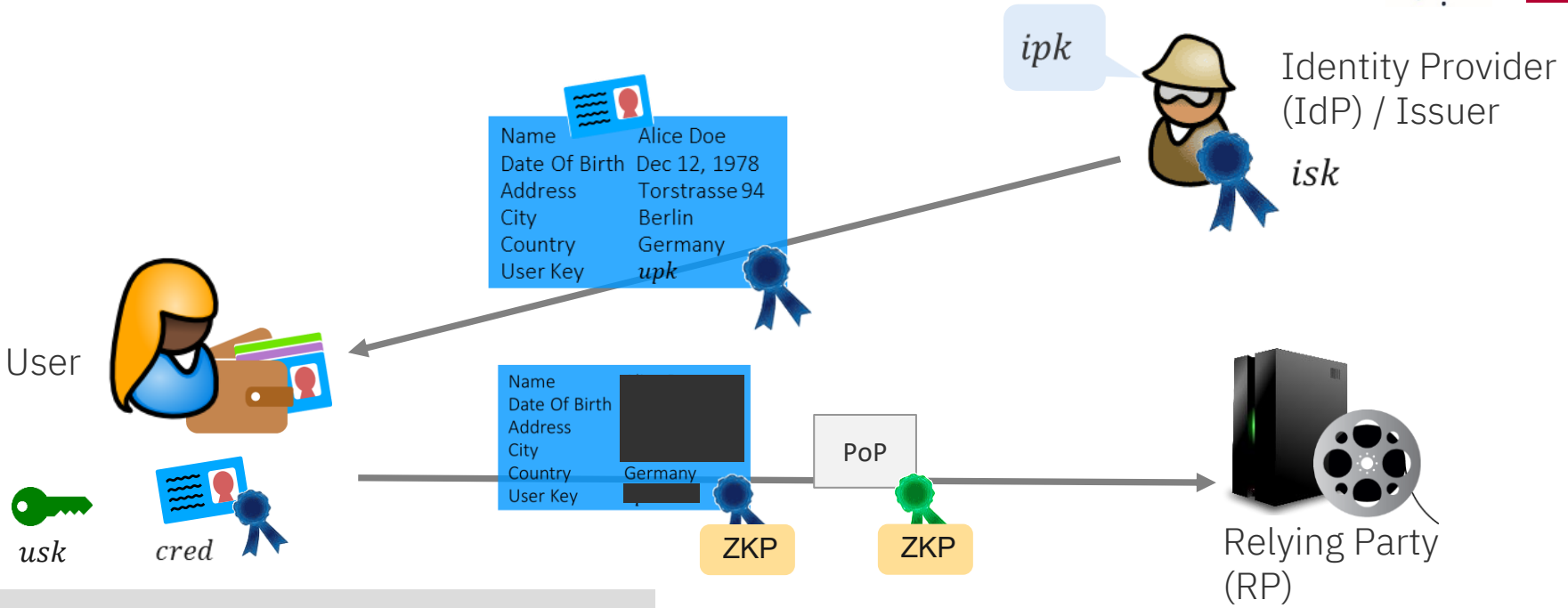
The core problem:

- Digital goods are easy to *clone*
- *Privacy vs Security:* misuse (e.g. sharing credentials) can happen *undetectably*
- Lack of security ⟶ reduced trust on the system: presentations are “vacant”

A (somewhat partial) solution

- Bind credentials to a device ⟶ harder to share “en masse”
- Valid presentation requires accessing the device
- Implemented via SE that stores an (inaccessible) secret signing key + *Proof-of-Possession*

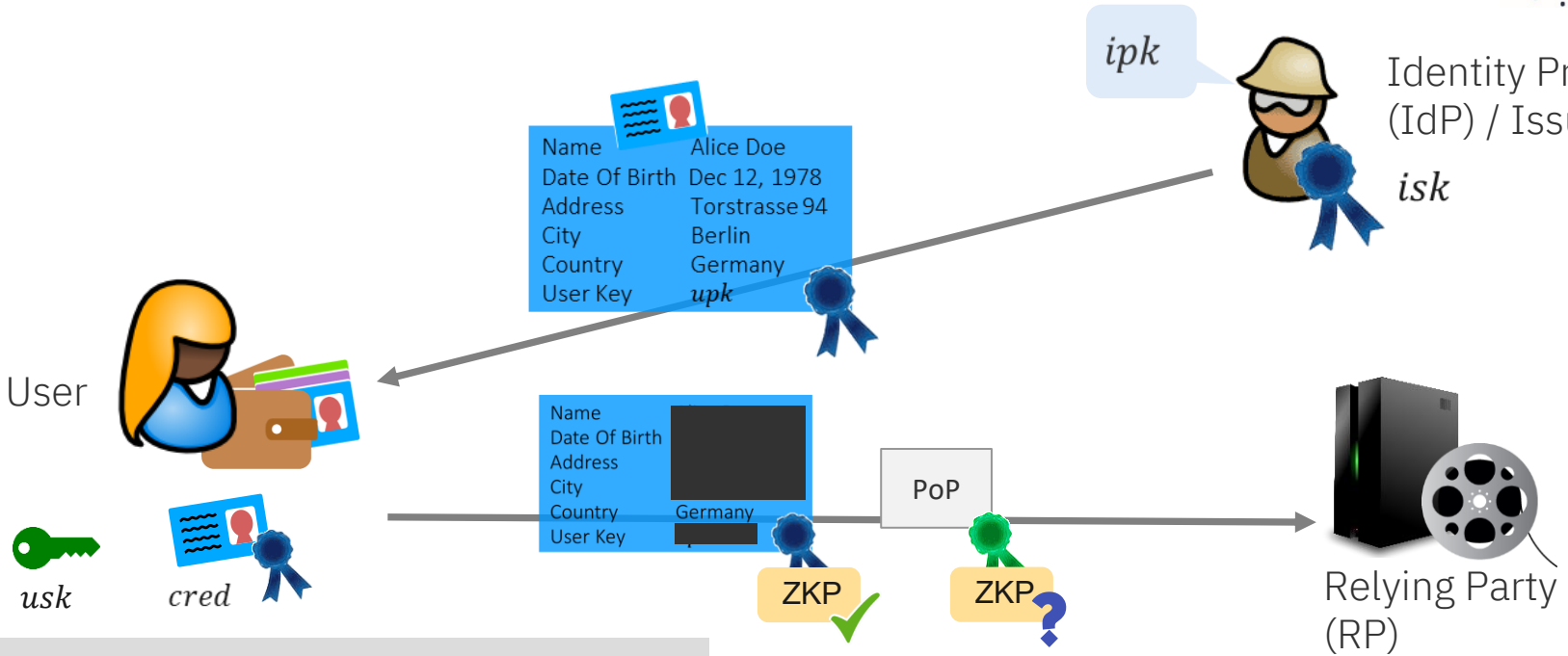
Device Bound Anonymous Credentials



$$cred := Sign(isk, (a_1, \ldots, a_\ell, upk))$$

$$\sigma_{PoP} := Sign(usk, nonce)$$

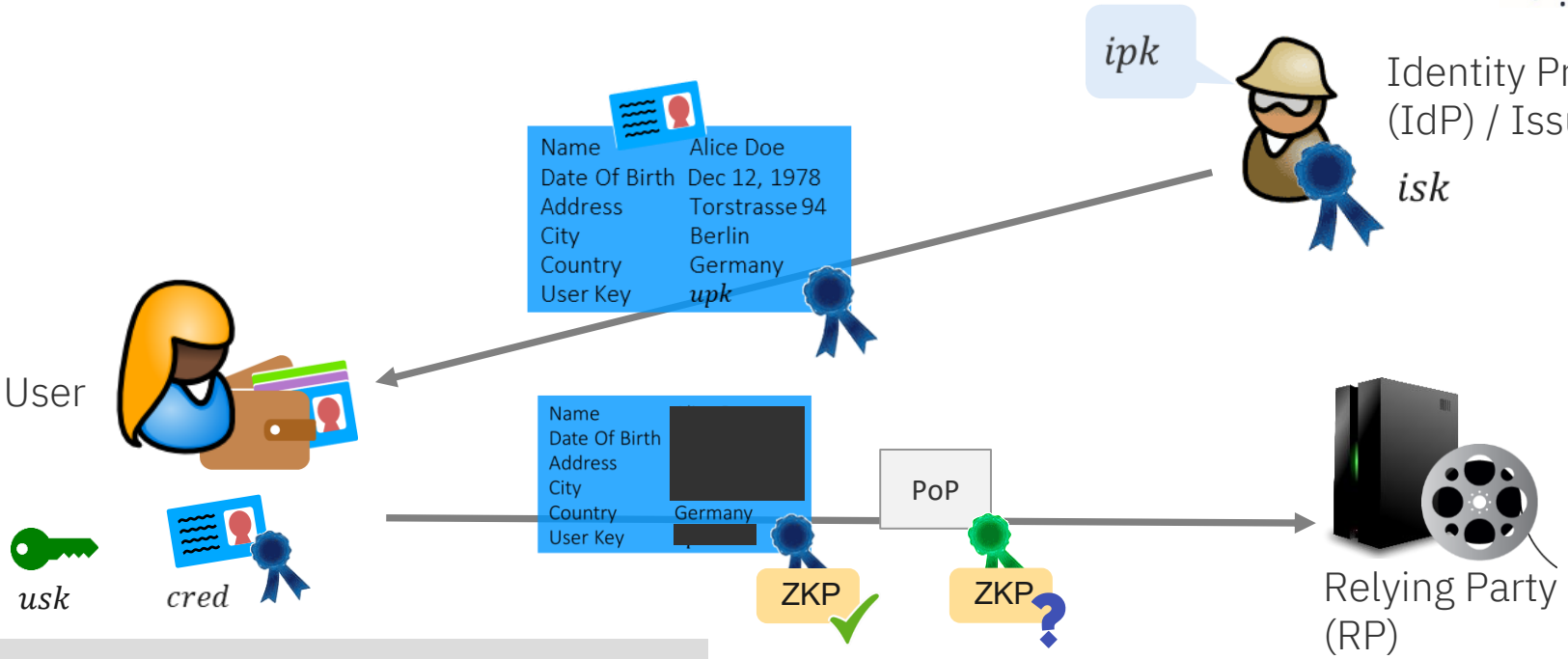
Device Bound Anonymous Credentials



$$cred := Sign(isk, (a_1, \ldots, a_\ell, upk))$$

$$\sigma_{PoP} := Sign(usk, nonce)$$

Device Bound Anonymous Credentials



$$cred := Sign(isk, (a_1, \ldots, a_\ell, upk))$$
$$\sigma_{PoP} := Sign(usk, nonce)$$

- **Goal**: efficient ZKP for cred and PoP
- **Constraints**: ECDSA for PoP (at least for the short term)

ZKPs for ECDSA

- ECDSA was *not* designed to support ZKP
- We can use generic ZKP techniques ⟶ complex*

* This is an understatement.

ZKPs for ECDSA

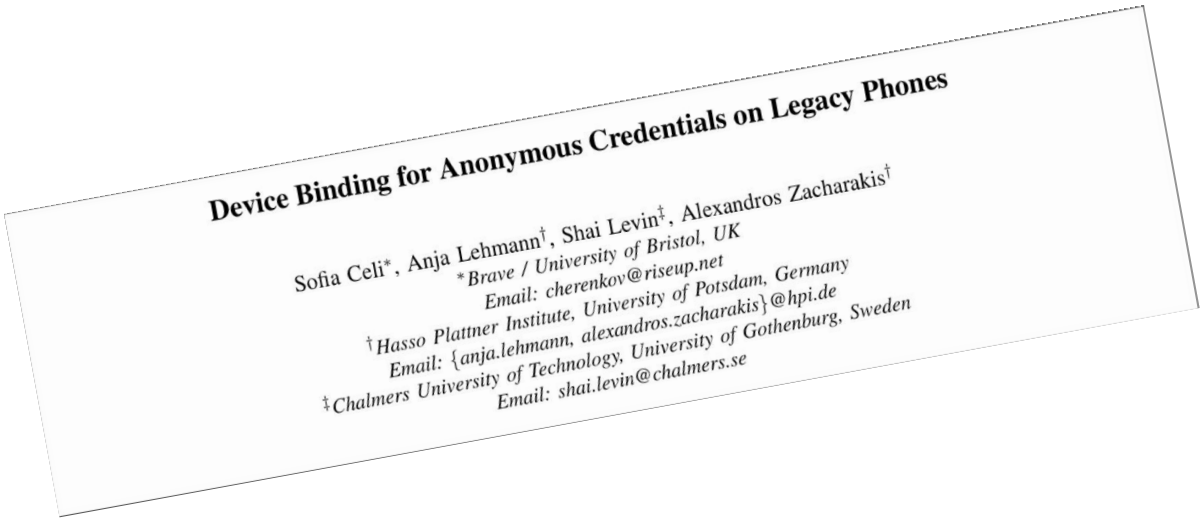
How can we improve?

- PoP is an easier problem since the nonce is public
- Leverage the “structure” of ECDSA to get *specialized ZKPs* for PoP

ZKPs for ECDSA

How can we improve?

- PoP is an easier problem since the nonce is public
- Leverage the “structure” of ECDSA to get *specialized ZKPs* for PoP



Device Binding for Anonymous Credentials on Legacy Phones

Sofia Celi*, Anja Lehmann†, Shai Levin‡, Alexandros Zacharakis†
*Brave / University of Bristol, UK
Email: cherenkov@riseup.net
†Hasso Plattner Institute, University of Potsdam, Germany
Email: {anja.lehmann, alexandros.zacharakis}@hpi.de
‡Chalmers University of Technology, University of Gothenburg, Sweden
Email: shai.levin@chalmers.se

https://eprint.iacr.org/2026/965.pdf

The Current Landscape

Issuer	User	ZKP	Efficiency (rough guestimates)	Advantages

The Current Landscape

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

The Current Landscape

Issuer	User	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

The Current Landscape

Issuer	User	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)	~350ms, ~125kB	Relatively simple. No circuit Easy to extend & standardize
ECDSA	ECDSA	Circuit (complex)	~400ms, ~300kB	No changes to issuer

The Current Landscape

Issuer	User	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)	~350ms, ~125kB	Relatively simple. No circuit Easy to extend & standardize
BBS	**ECDSA** 	Circuit (simple)	~350ms, ~1.5kB	Easy to extend & standardize Short proofs
ECDSA 	ECDSA 	Circuit (complex)	~400ms, ~300kB	No changes to issuer

Conclusion

Can we achieve efficient, privacy preserving device binding?

Can we do that now under the existing restrictions?

Are we done?

Conclusion

Can we achieve efficient, privacy preserving device binding? ***YES!***

Can we do that now under the existing restrictions? ***YES!***

- Various solutions for ECDSA with a *broad trade-off* spectrum

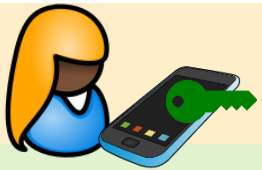
Are we done? ***YES*** *and* ***NO***

- Efficient (and simple) solutions already exist!
- The remaining challenge: *standardization*

Towards Deploying Anonymous Credentials

1 | Standardisation of all required cryptographic protocols → interoperability

IETF: ongoing standards for all core crypto primitives (e.g., BBS)
ETSI: dedicated standard for ZKP-based EUDI Wallet under development



2 | Realize cloning-prevention for anonymous credentials
Usually done through device binding

→ Solved: Device-binding from ECDSA Secure Elements

3 | Ensure that privacy strong enough for real-world use case, e.g., for age proofs?

→ Challenge: (Anonymous) Credentials usually reveal the issuer‘s identity

Anonymous Credentials with Issuer Hiding

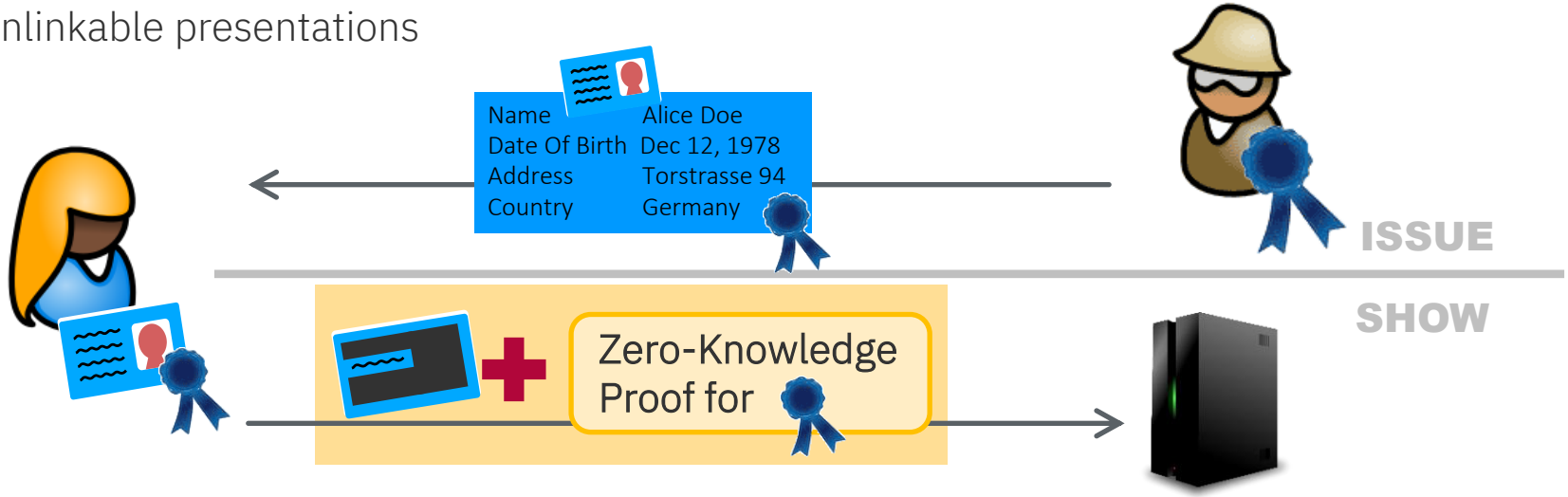
Andrea Flamini

based on joint works with Karla Friedrichs, Jonathan Katz, Watson Ladd, Anja Lehmann and Marek Sefranek

Do anonymous credentials really enable minimal disclosure?

We have verifiable credentials supporting

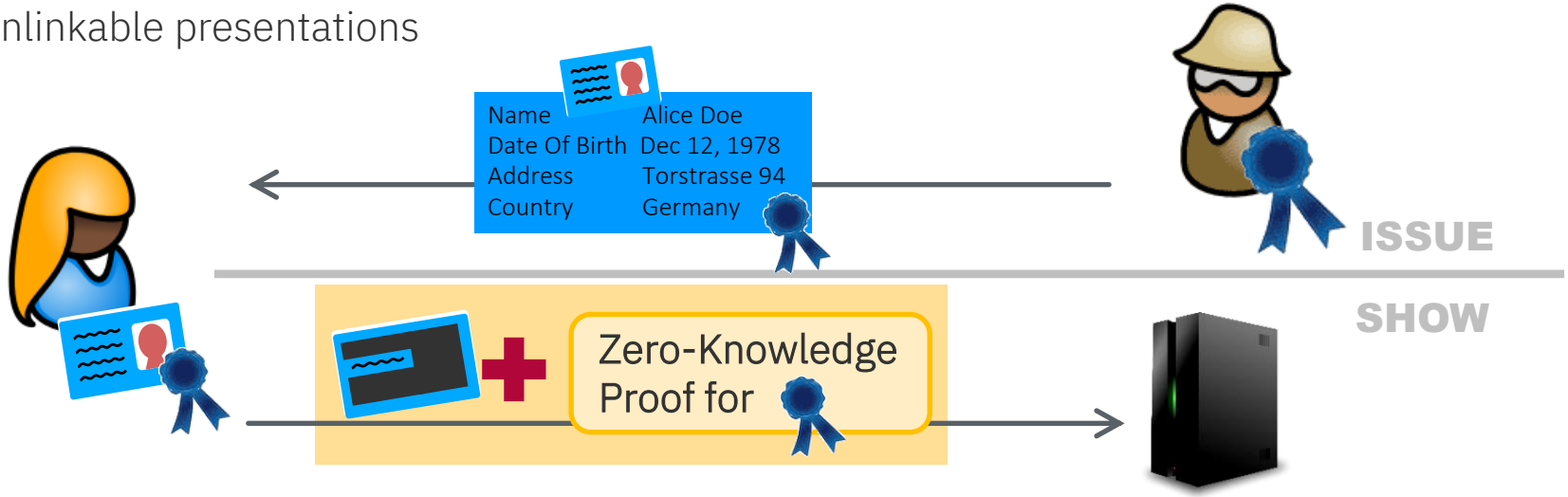
1. selective disclosure
2. unlinkable presentations



Do anonymous credentials really enable minimal disclosure?

We have verifiable credentials supporting

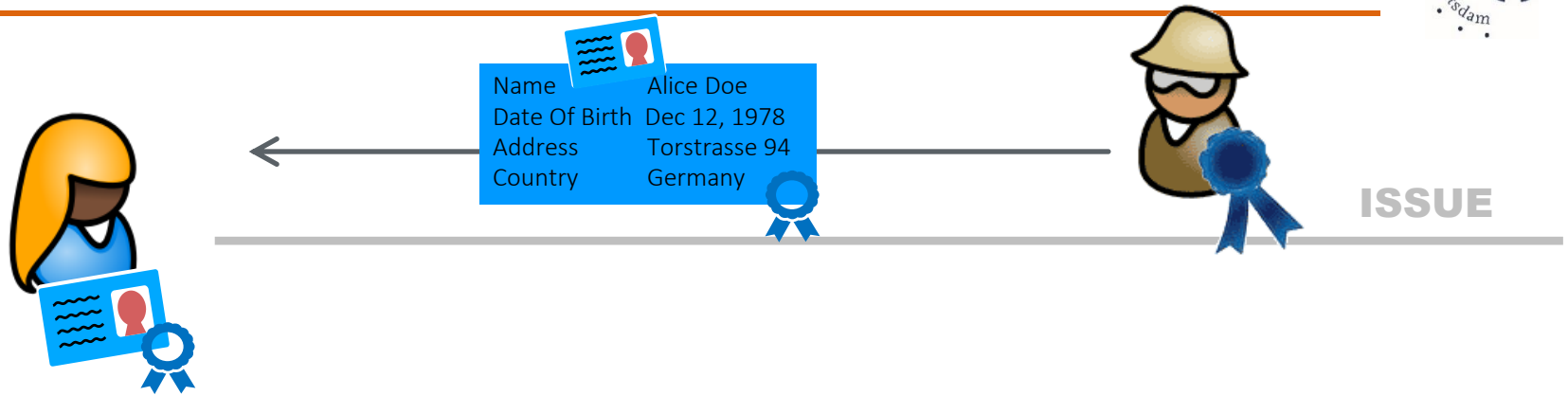
1. selective disclosure
2. unlinkable presentations



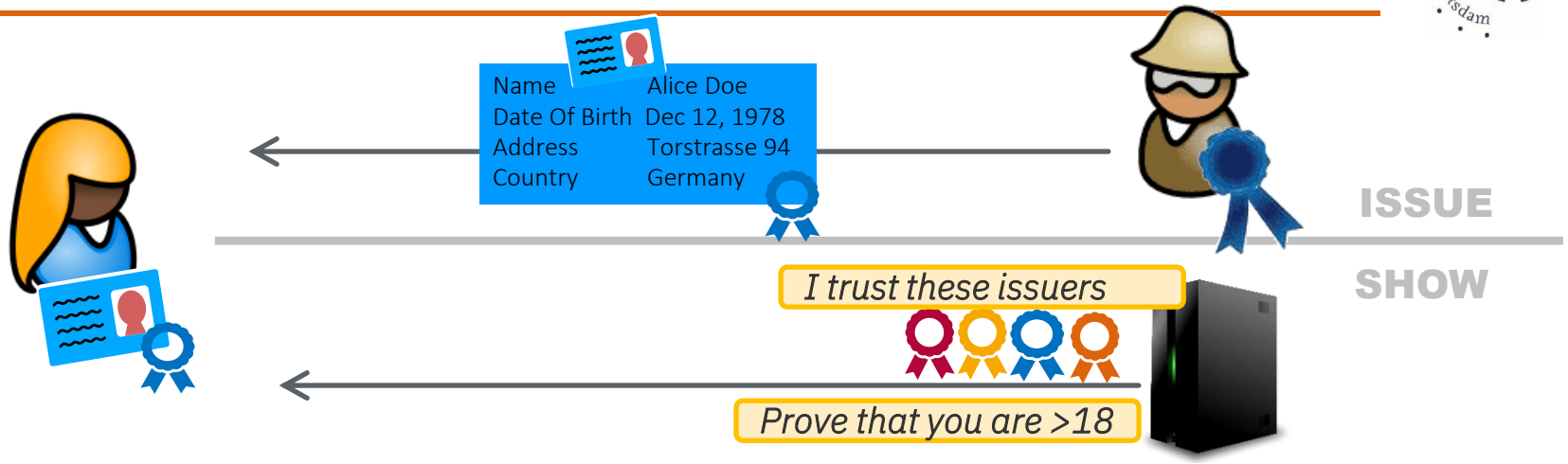
Presentations **always reveal the issuer** to enable public verifiability

This can reveal your **citizenship**, your **university**, your **device's manufacturer**...

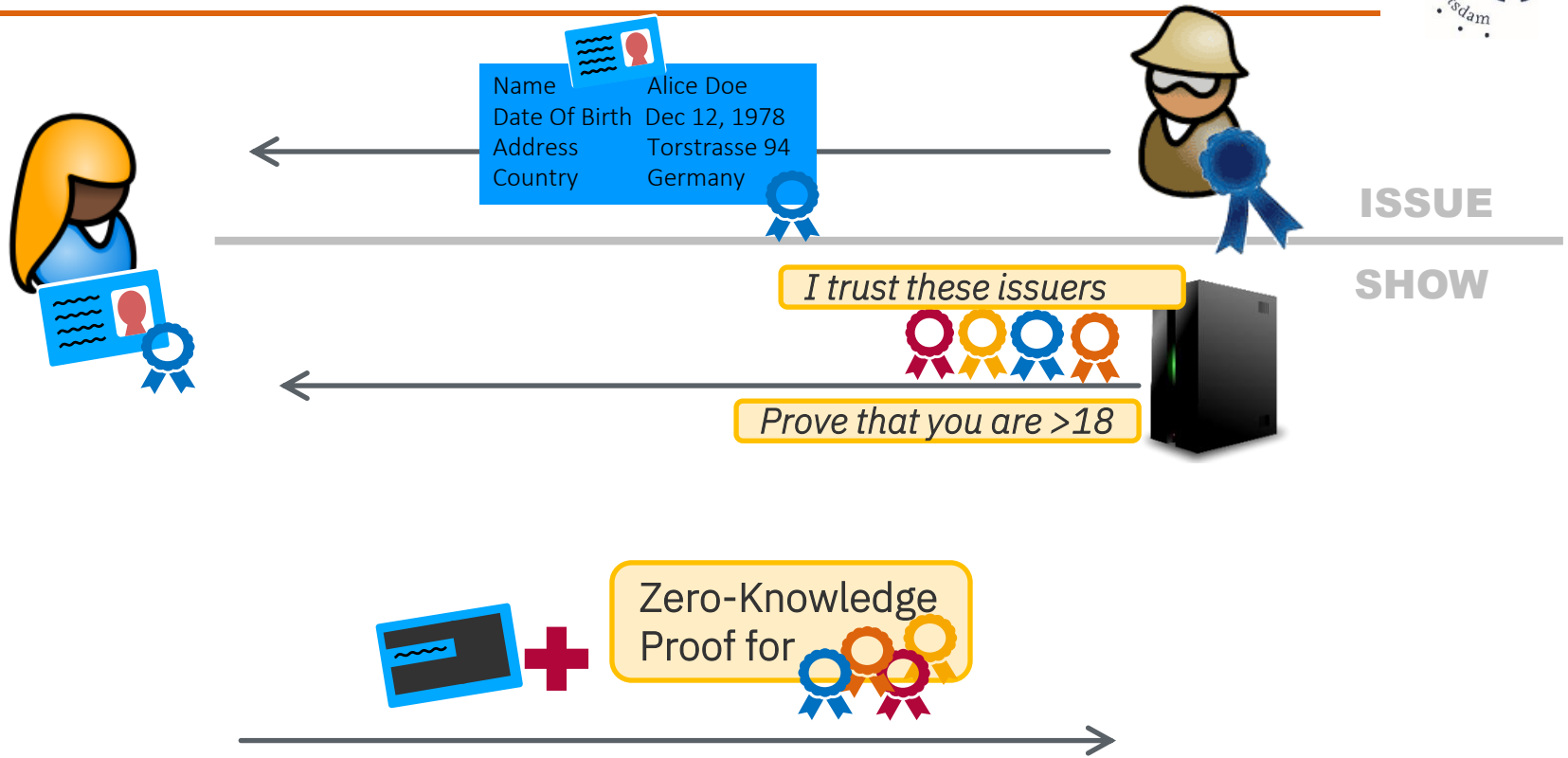
What we want to have



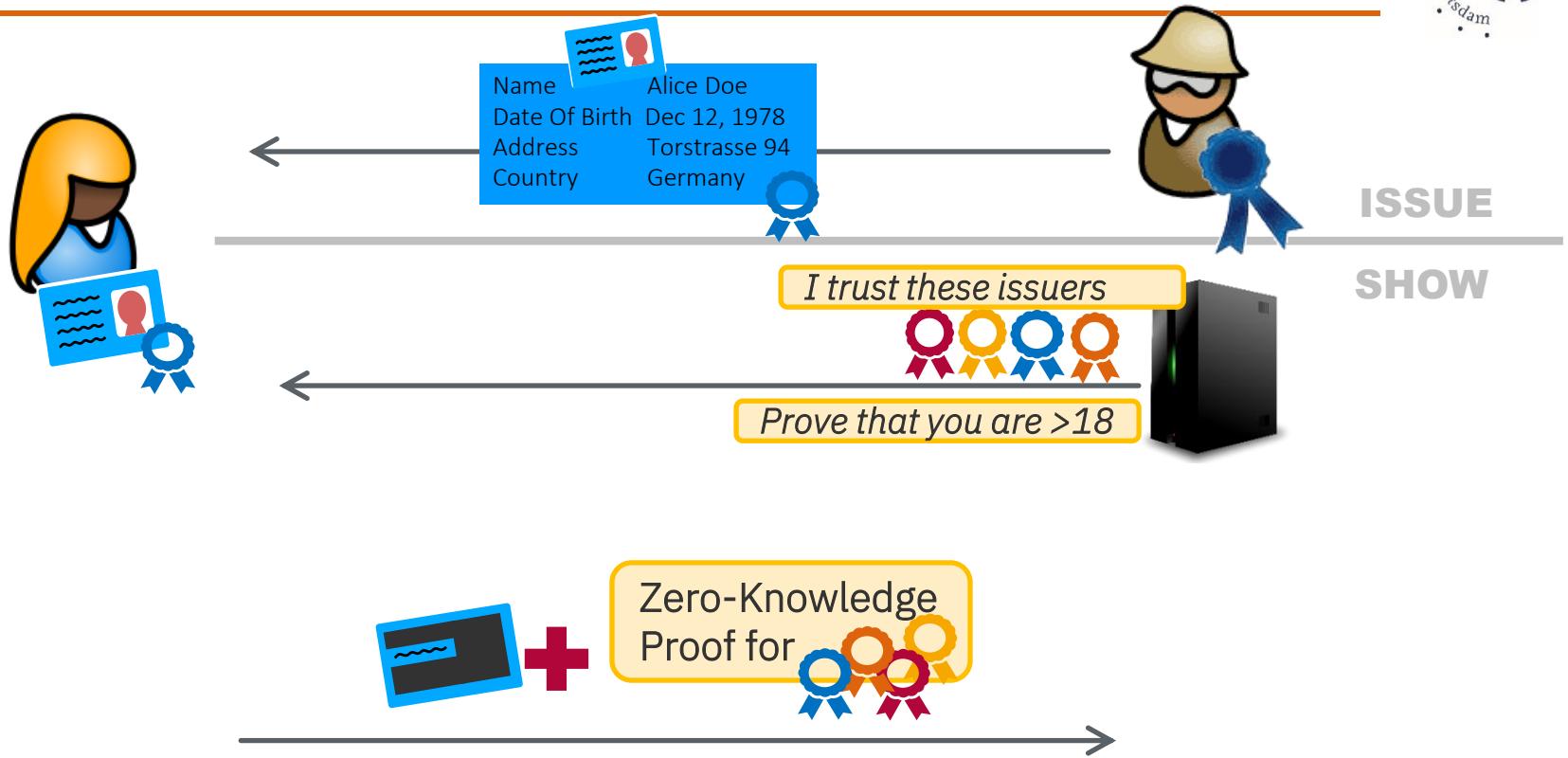
What we want to have



What we want to have



What we want to have



GOOD NEWS:

WE KNOW HOW TO DO IT!

A useful property of BBS signatures

Given a BBS credential issued by 

Name	Alice Doe
Date Of Birth	Dec 12, 1978
Address	Torstrasse 94
Country	Germany

We know how to transform it into a credential for the same attributes that verifies under a **random public key**

Name	Alice Doe
Date Of Birth	Dec 12, 1978
Address	Torstrasse 94
Country	Germany

A useful property of BBS signatures

Given a BBS credential issued by 

Name	Alice Doe
Date Of Birth	Dec 12, 1978
Address	Torstrasse 94
Country	Germany

We know how to transform it into a credential for the same attributes that verifies under a **random public key**

Name	Alice Doe
Date Of Birth	Dec 12, 1978
Address	Torstrasse 94
Country	Germany

This might look irrelevant, but it is actually very useful!

Our Solutions

We have designed two solutions that match two use cases:

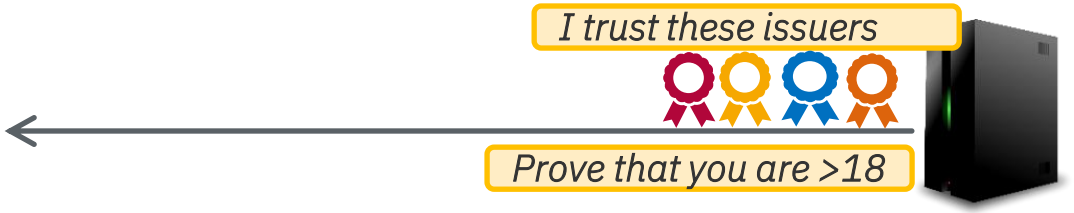
	Small sets of issuers	Large sets of issuers
Use case	Issuers are EU member states	Issuers are EU Universities
Trust	Trust only the issuers	Trust the **issuers** and **a third party** who certifies the public keys of the issuers in a set
Presentation size	overhead logarithmic in the number of issuers	Constant presentation size
Compatibility with BBS	✓	✓

Simple construction for small policies

When the set of trusted issuers is small (e.g. <64) we have an efficient construction

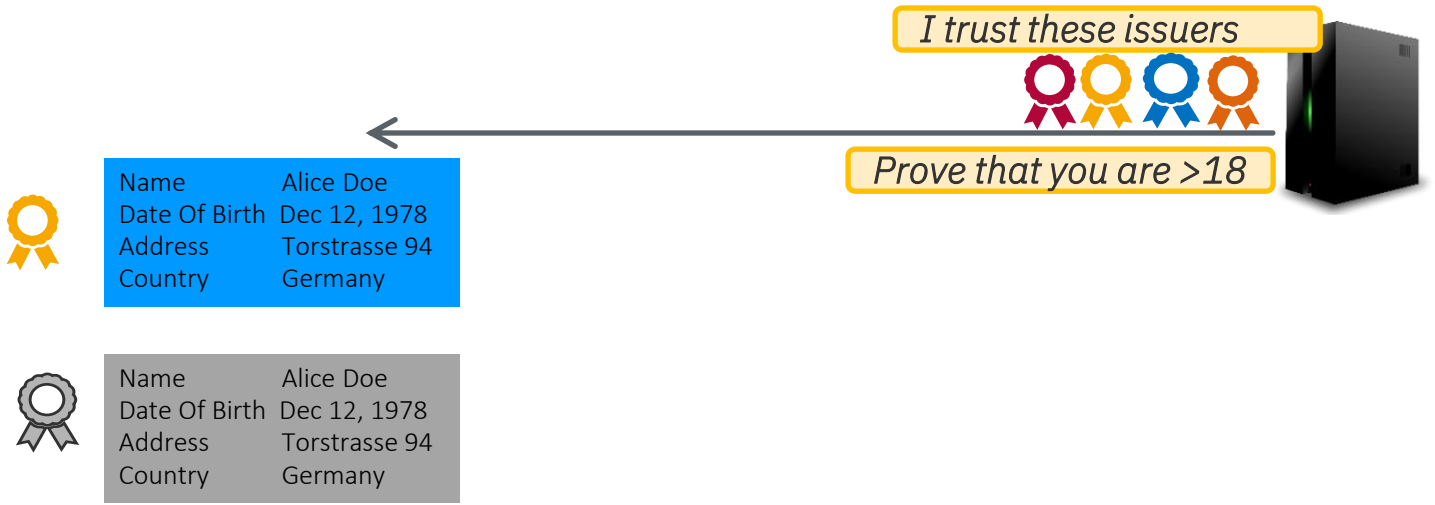
Simple construction for small policies

When the set of trusted issuers is small (e.g. <64) we have an efficient construction



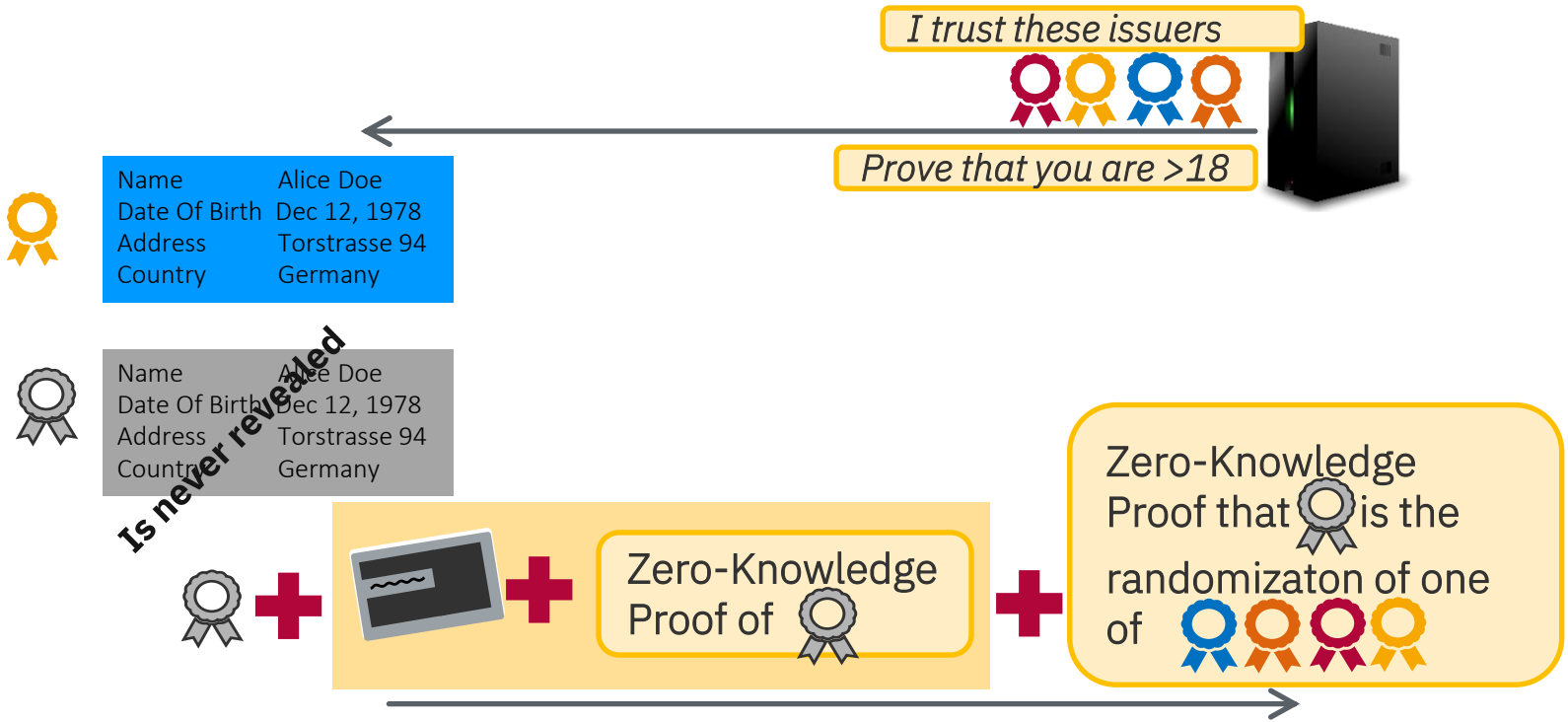
Simple construction for small policies

When the set of trusted issuers is small (e.g. <64) we have an efficient construction



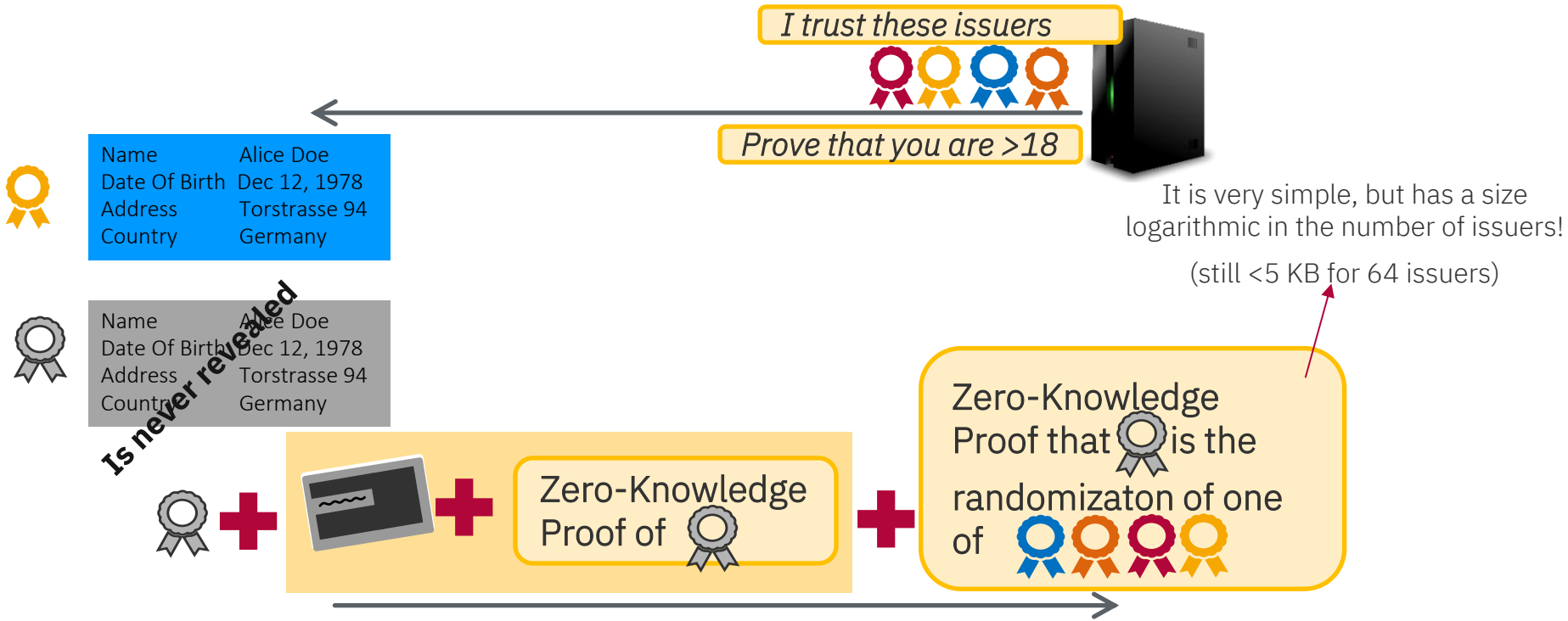
Simple construction for small policies

When the set of trusted issuers is small (e.g. <64) we have an efficient construction



Simple construction for small policies

When the set of trusted issuers is small (e.g. <64) we have an efficient construction



Simple construction for small policies

When the set of trusted issuers is small (e.g. <64) we have an efficient construction

It is very simple, but has a size logarithmic in the number of issuers!

(still <5 KB for 64 issuers)

- https://ia.cr/2026/870

Simple construction for larger policies

When the set of trusted issuers is large (e.g. >1000) we have an efficient construction

Simple construction for larger policies

When the set of trusted issuers is large (e.g. >1000) we have an efficient construction

Trusted party certifies

EU-Uni

Simple construction for larger policies

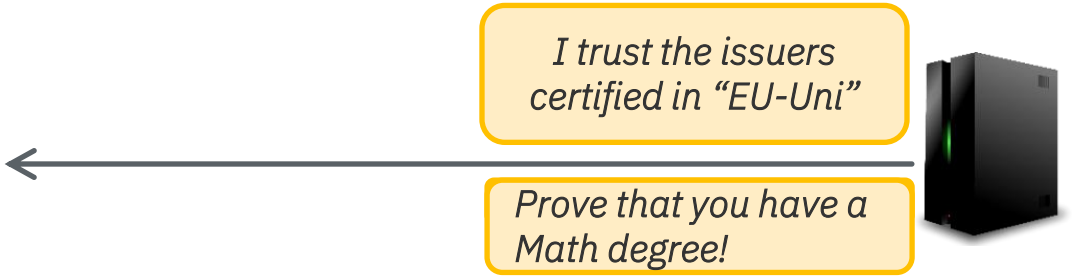
When the set of trusted issuers is large (e.g. >1000) we have an efficient construction

Trusted party certifies

EU-Uni

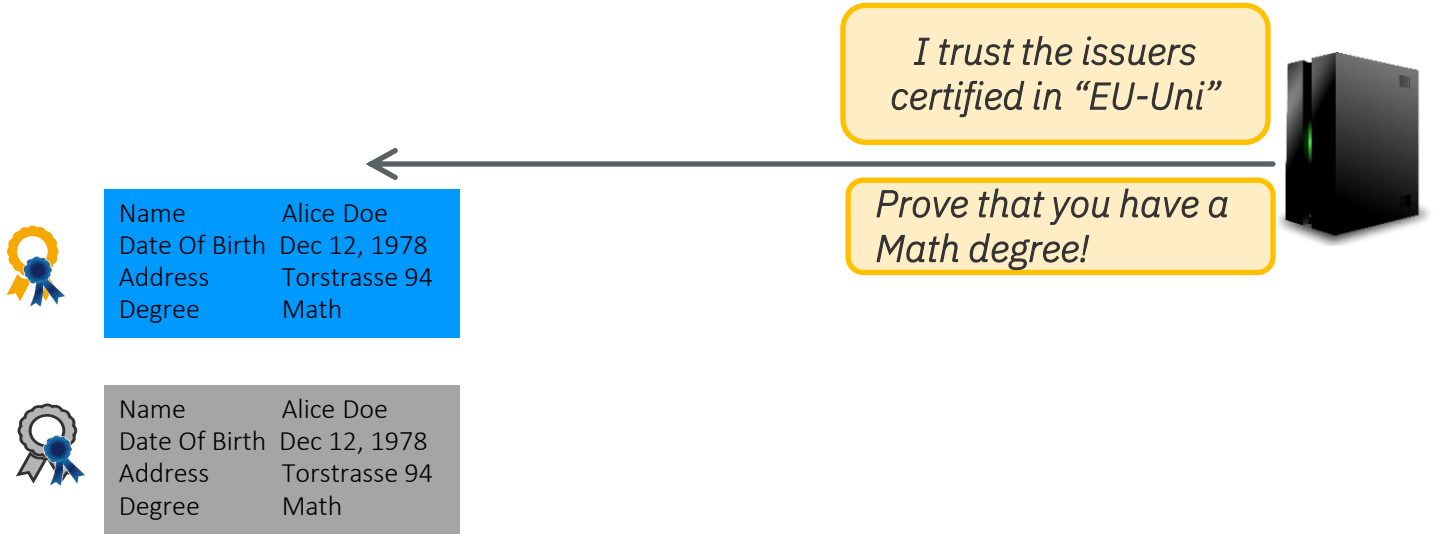
Simple construction for larger policies

When the set of trusted issuers is large (e.g. >1000) we have an efficient construction



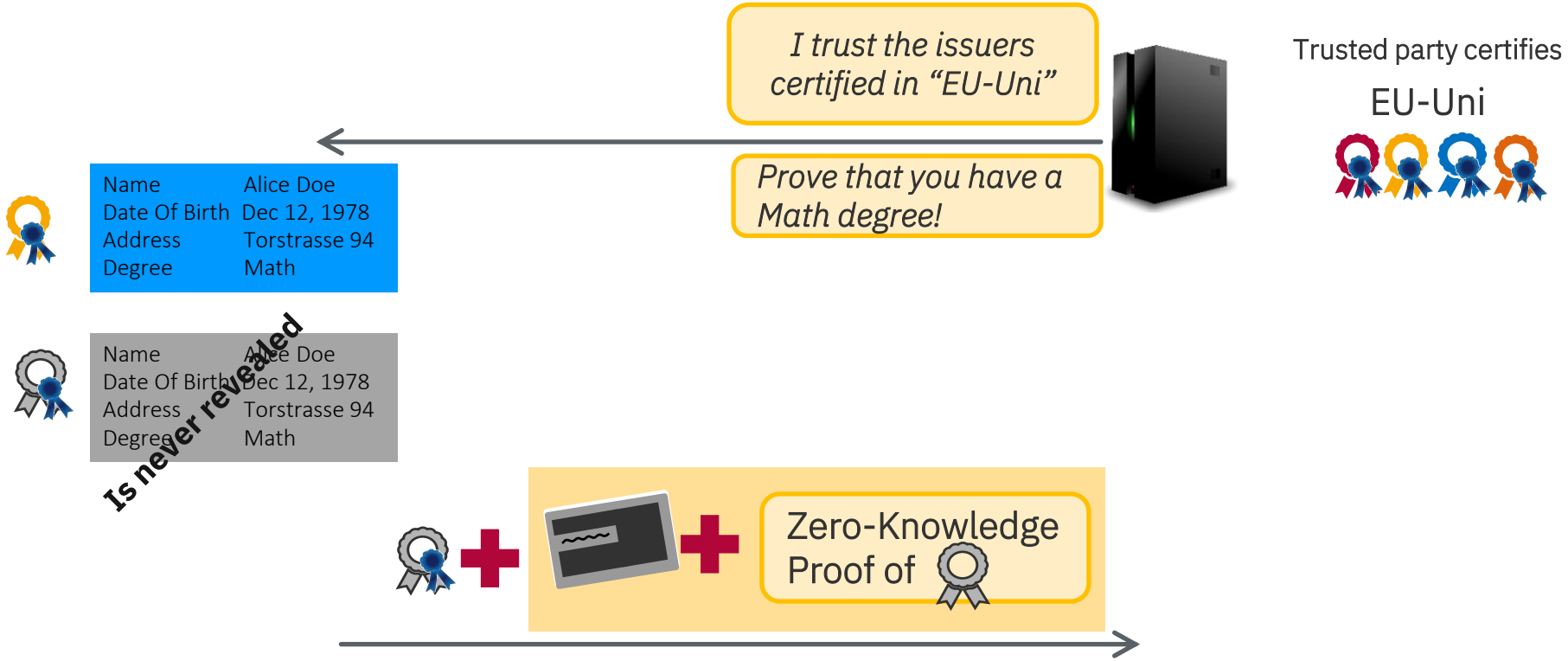
Simple construction for larger policies

When the set of trusted issuers is large (e.g. >1000) we have an efficient construction



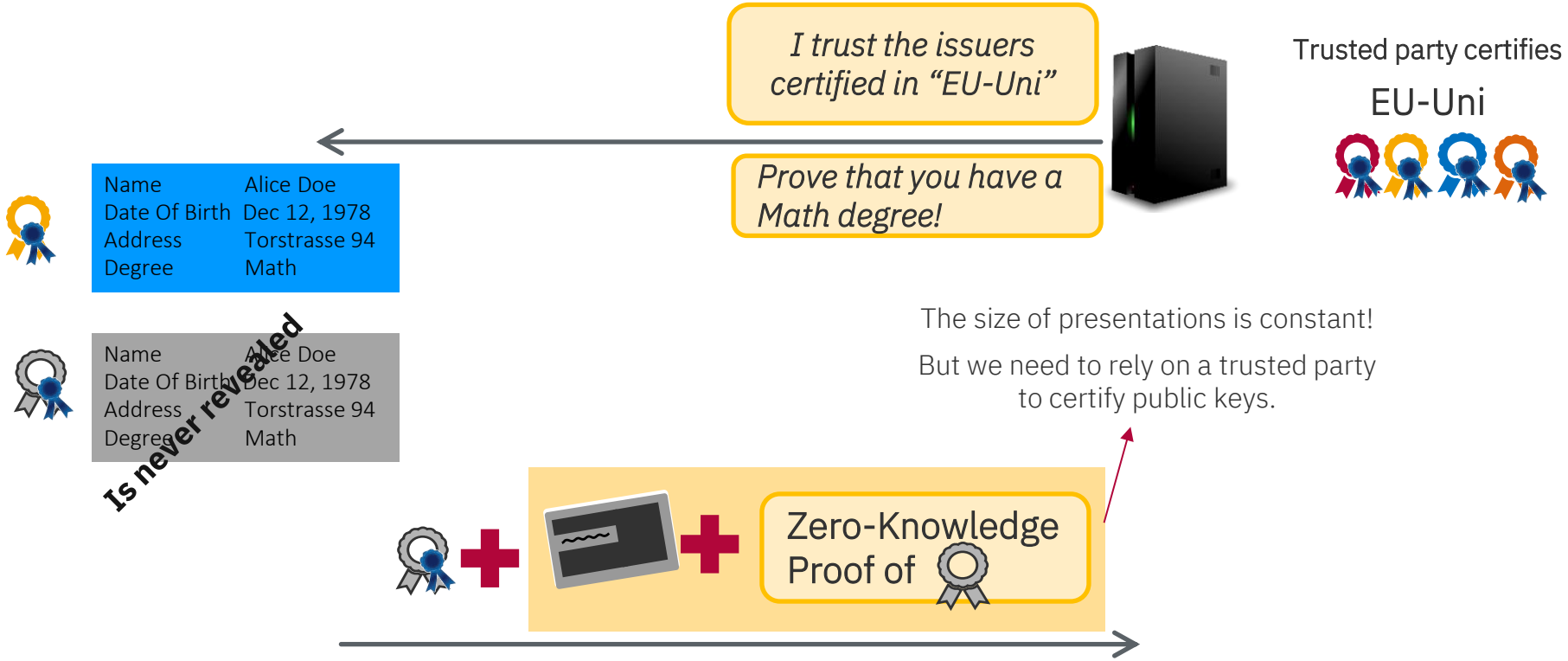
Simple construction for larger policies

When the set of trusted issuers is large (e.g. >1000) we have an efficient construction



Simple construction for larger policies

When the set of trusted issuers is large (e.g. >1000) we have an efficient construction

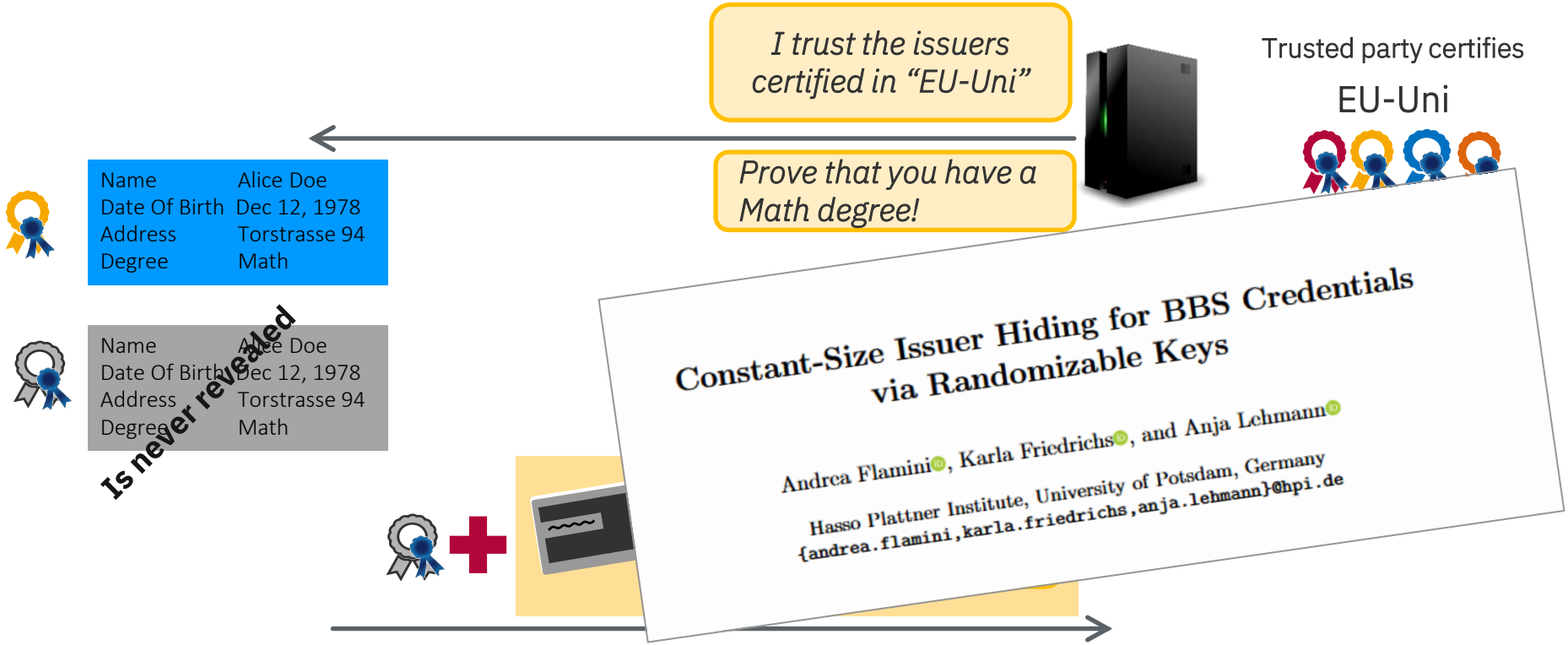


The size of presentations is constant!

But we need to rely on a trusted party to certify public keys.

Simple construction for larger policies

When the set of trusted issuers is large (e.g. >1000) we have an efficient construction



- https://ia.cr/2026/369

Conclusion

The tricks we have shown do not work also for single-show credentials (due to salted hashes)

But we have shown that this is possible for BBS credentials!

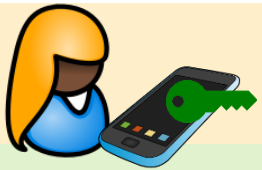
- We know how to build Issuer-Hiding presentations efficiently.
- The protocols are very simple.
- The constructions do not require updating the issuance of BBS credentials.
- Issuer-Hiding presentations use standard BBS presentations as building blocks, and require only a few additional operations.

Towards Deploying Anonymous Credentials

1 | Standardisation of all required cryptographic protocols → interoperability

IETF: ongoing standards for all core crypto primitives (e.g., BBS)
ETSI: dedicated standard for ZKP-based EUDI Wallet under development

2 | Realize cloning-prevention for anonymous credentials
Usually done through device binding



→ Solved: Device-binding from ECDSA Secure Elements

3 | Ensure that privacy strong enough for real-world use case, e.g., for age proofs?

→ Solved: Issuer-hiding protocols, e.g. for BBS

ZKP-EUDI Roadmap | Next Steps

Short/Mid-term: show feasibility and benefits

- Use ZKP for use cases with high privacy demands
- ZKP-compatible protocols (OID4VC) & data formats
- Many additional features: pseudonyms, blind issuance, …
  → Build modular & crypto-agile protocols

ZKP-EUDI Roadmap | Next Steps

Short/Mid-term: show feasibility and benefits

- Use ZKP for use cases with high privacy demands
- ZKP-compatible protocols (OID4VC) & data formats
- Many additional features: pseudonyms, blind issuance, …
  → Build modular & crypto-agile protocols

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 = only path to strong & multi-show unlinkability

  Can even provide issuer hiding
- Start where privacy matters most, e.g., age proofs

  (but whether we want age proofs is a different story …)
- Main deployment blockers are solved: device binding & standards underway
- Cryptography for transitional phase is ready!

Summary

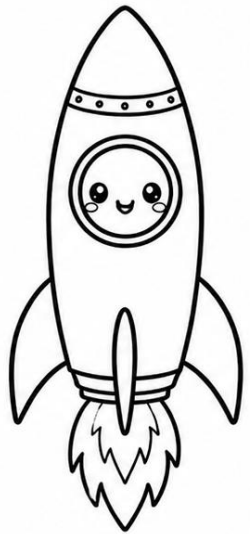
- Anonymous credentials = only path to strong & multi-show unlinkability
  Can even provide issuer hiding
- Start where privacy matters most, e.g., age proofs
  (but whether we want age proofs is a different story …)
- Main deployment blockers are solved: device binding & standards underway
- Cryptography for transitional phase is ready!

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

eIDAS: privacy-preserving eID

ARF: ECDSA

Ready to use & built for this: anonymous credentials



Summary

- Anonymous credentials = only path to strong & multi-show unlinkability
  Can even provide issuer hiding
- Start where privacy matters most, e.g., age proofs
  (but whether we want age proofs is a different story …)
- Main deployment blockers are solved: device binding & standards underway
- Cryptography for transitional phase is ready!

eIDAS: privacy-preserving eID

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

Interested in using ZKP? Please reach out:
https://hpi.de/lehmann/eudi

ARF: ECDSA

Ready to use & built for this: anonymous credentials