Finanziato
dall'Unione europea
NextGenerationEU

Ministero
dell'Università
e della Ricerca

Italiadomani
PIANO NAZIONALE
DI RIPRESA E RESILIENZA

SERICS
SECURITY AND RIGHTS IN THE CYBERSPACE

CrypTO CONFERENCE

1859
Politecnico
di Torino

Telsy
A TIM
ENTERPRISE
BRAND

DISMA

FONDAZIONE BRUNO KESSLER | CENTER FOR CYBERSECURITY

ST SECURITY & TRUST

Research Challenges of the Digital Identity Wallet

Roberto Carbone

Center for Cybersecurity, Fondazione Bruno Kessler (FBK)

carbone@fbk.eu

CrypTO CONFERENCE
POLITECNICO DI TORINO 2025
Torino, 23 May 2025

Who are we?
Fondazione Bruno Kessler (FBK)

- Research and Innovation institute in Trento, Italy
- 12 research centers: from technology to humanities and social sciences

FBK at a glance

450+
researchers

136
PhD students from 25 different Countries

200+
thesis students, visiting professor, visitors

700+
students involved in the FBK activities

4.645 sq m
labs for scientific research

230.000
and more titles in a special library

Center for Cybersecurity
Fondazione Bruno Kessler (FBK)

Digital Identity

Applied Cryptography

Threat and Anomaly Detection

...

ST SECURITY & TRUST

ALEPH APPLIED CRYPTOGRAPHY

...

Digital identity wallet
Outline

EU
European Digital Identity Wallet
Obtain and present your documents
Enter

EUDI Wallet Overview

Evolution of the eIDAS ecosystem and our research activities

Trust Framework

Overview

Selective Disclosure and Revocation Mechanisms

Overview and comparison of different approaches

Secure elements

Overview and comparison

Threat Model and Risk Analysis for the Wallet Ecosystem

Discussion on overall security and privacy aspects of digital identity wallets

Digital identity wallet

Outline

EU
European Digital Identity Wallet
Obtain and present your documents
Enter

EUDI Wallet Overview

Evolution of the eIDAS ecosystem and our research activities

Trust Framework

Overview

Selective Disclosure and Revocation Mechanisms

Overview and comparison of different approaches

Secure elements

Overview and comparison

Threat Model and Risk Analysis for the Wallet Ecosystem

Discussion on overall security and privacy aspects of digital identity wallets

EU
European Digital Identity Wallet
Obtain and present your documents
Enter

European Digital Identity Wallet (EUDIW)

allows users to be in **control of their personal data**

Document storage
Of **different types** (identity, driving license, passport…)

Enabler of transactions
Both **physical** and **digital** world

Signature
by means of **qualified electronic signatures**

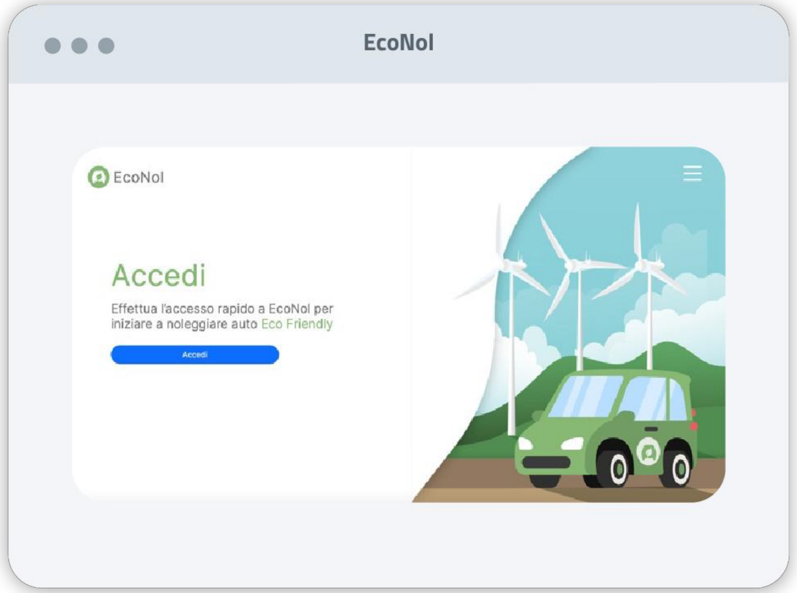
Revision June, 2021 – Final Act signed 2024

eID.AS electronic IDentification Authentication and Signature

EUDI Wallet
Remote flow

EcoNol is a rental car company

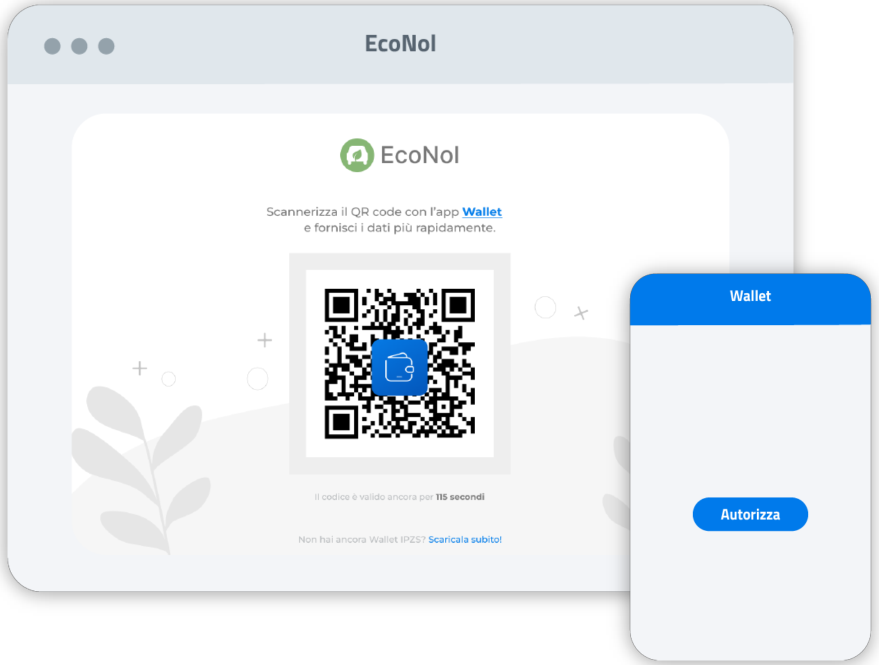
which allows online booking after checking the validity of the driver's license.


EcoNol

EcoNol

Accedi

Effettua l'accesso rapido a EcoNol per iniziare a noleggiare auto Eco Friendly

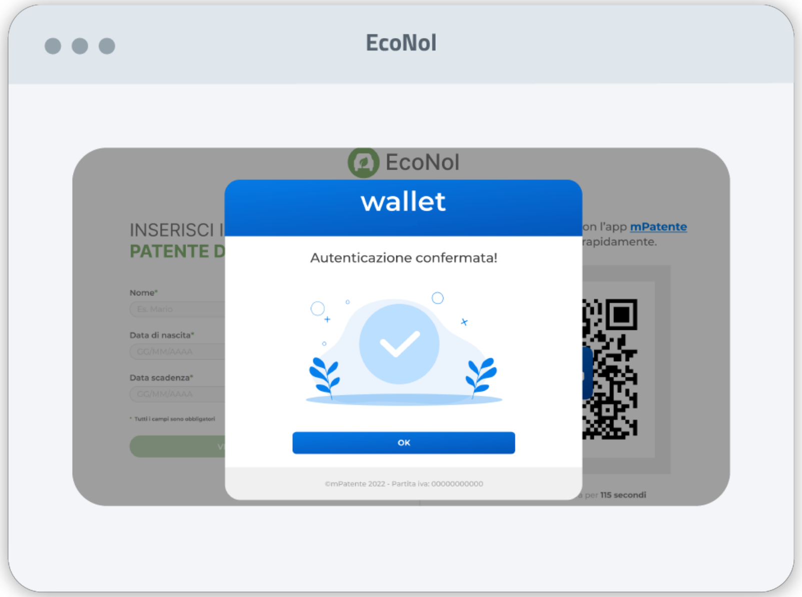

EcoNol

EcoNol

Scannerizza il QR code con l'app Wallet e fornisci i dati più rapidamente.

Il codice è valido ancora per **115 secondi**

Non hai ancora Wallet IPZS? Scaricala subito!


EcoNol

EcoNol

INSERISCI I
PATENTE D

Nome*

Es. Mario

Data di nascita*

GG/MM/AAAA

Data scadenza*

GG/MM/AAAA

* Tutti i campi sono obbligatori

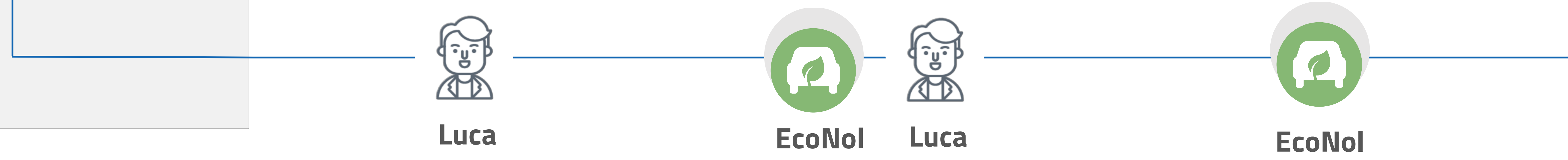
on l'app mPatente
rapidamente.

a per **115 secondi**

wallet

Autenticazione confermata!

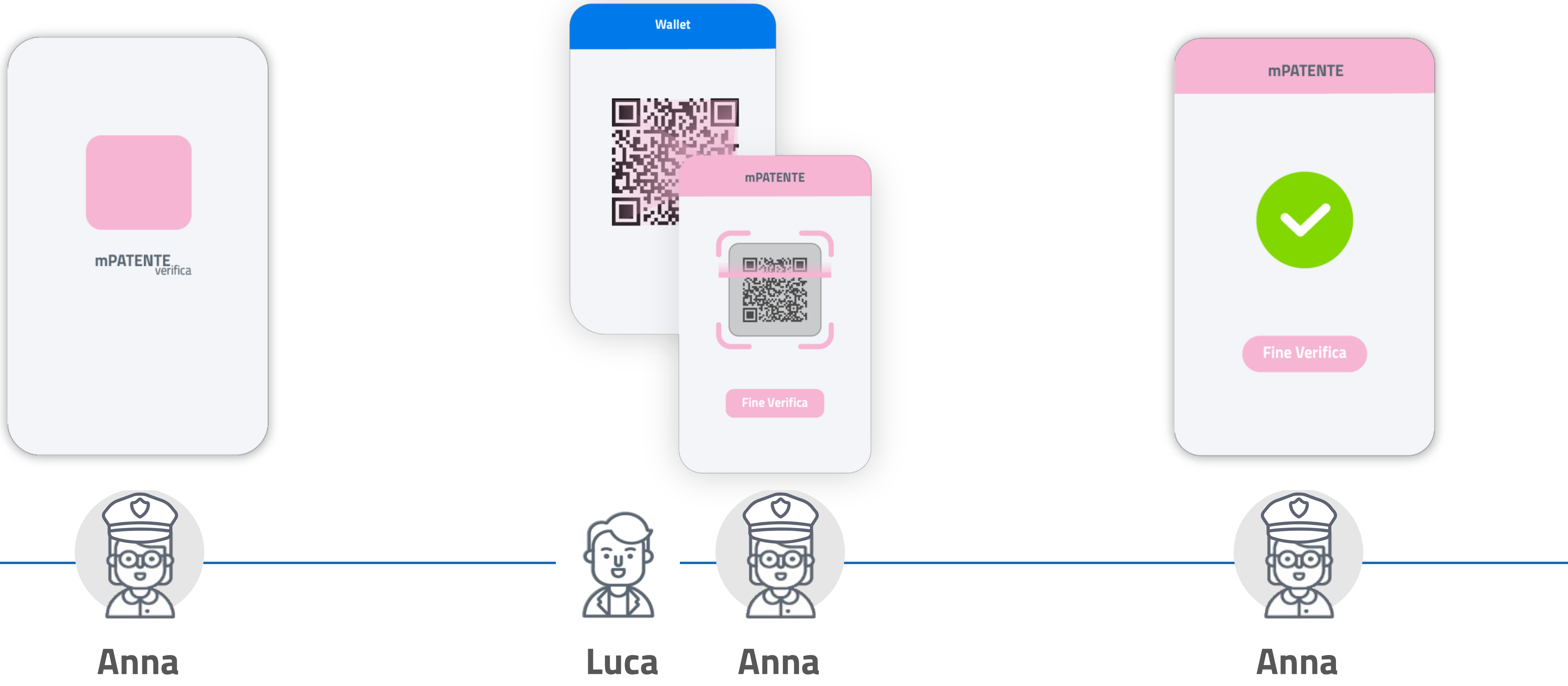
©mPatente 2022 - Partita iva: 00000000000



EUDI Wallet
Proximity flow

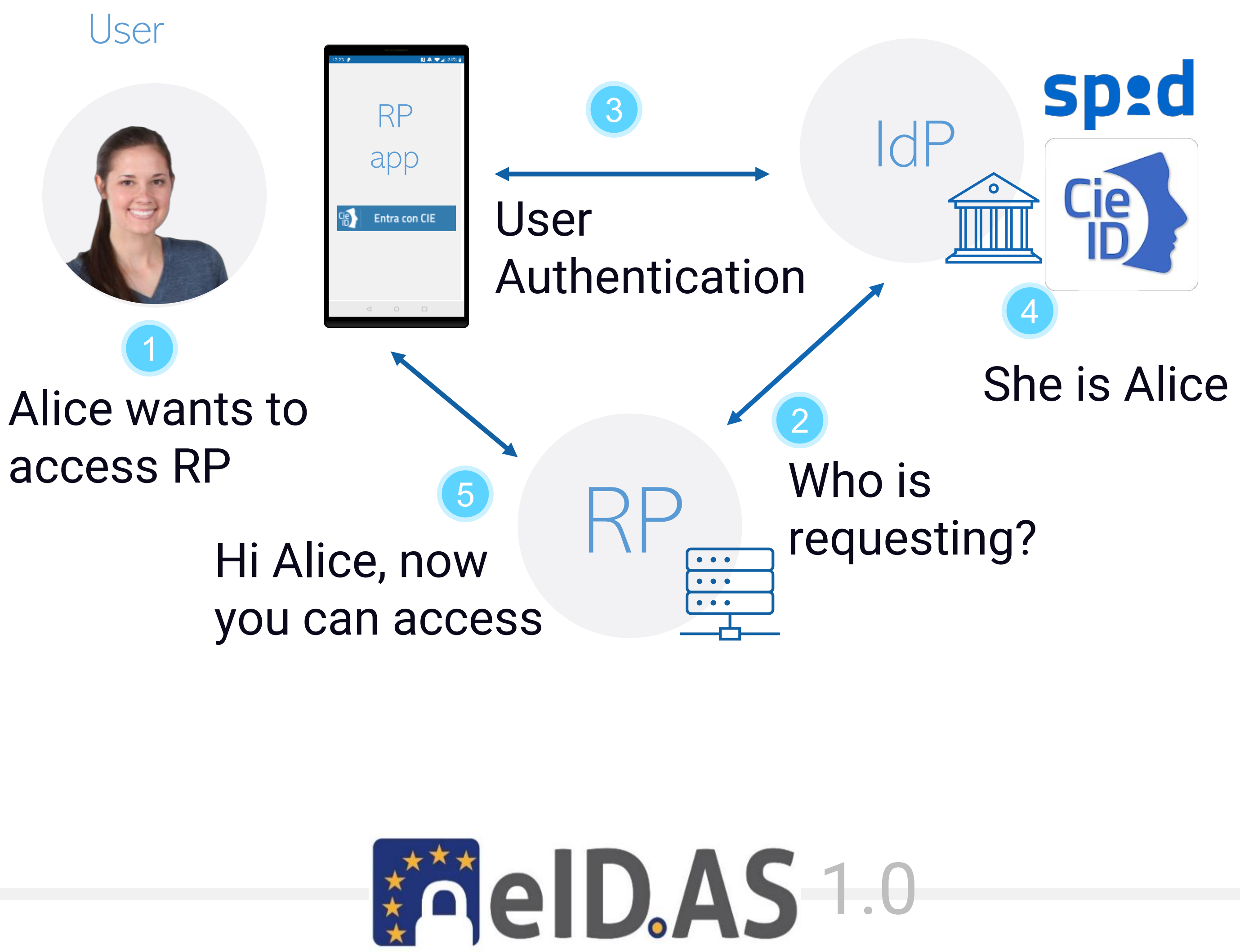
Anna is a police officer

conducting driver's
license validity checks.



EUDI Wallet Ecosystem
Different Paradigm

The IdP is involved at each user login attempt

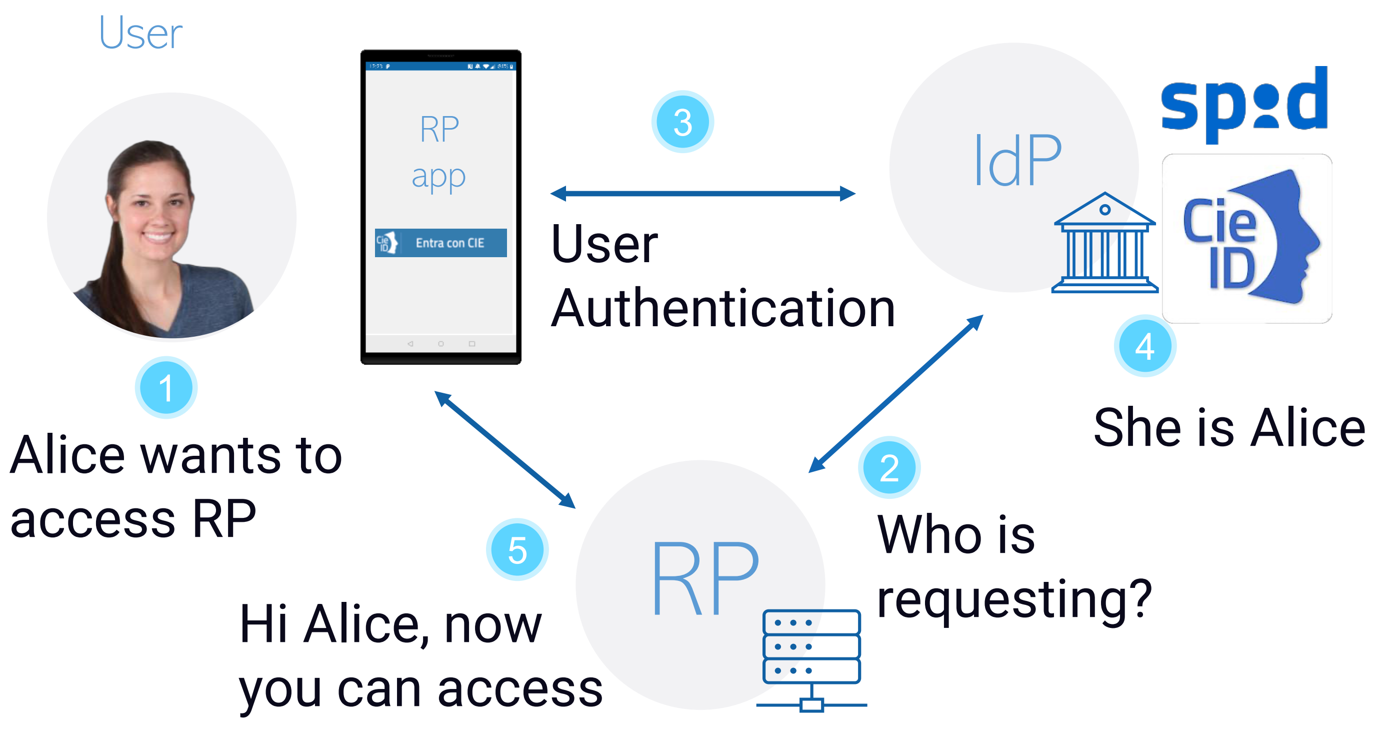


- + Reduce the number of credentials users need to remember
- + Security best current practice in place

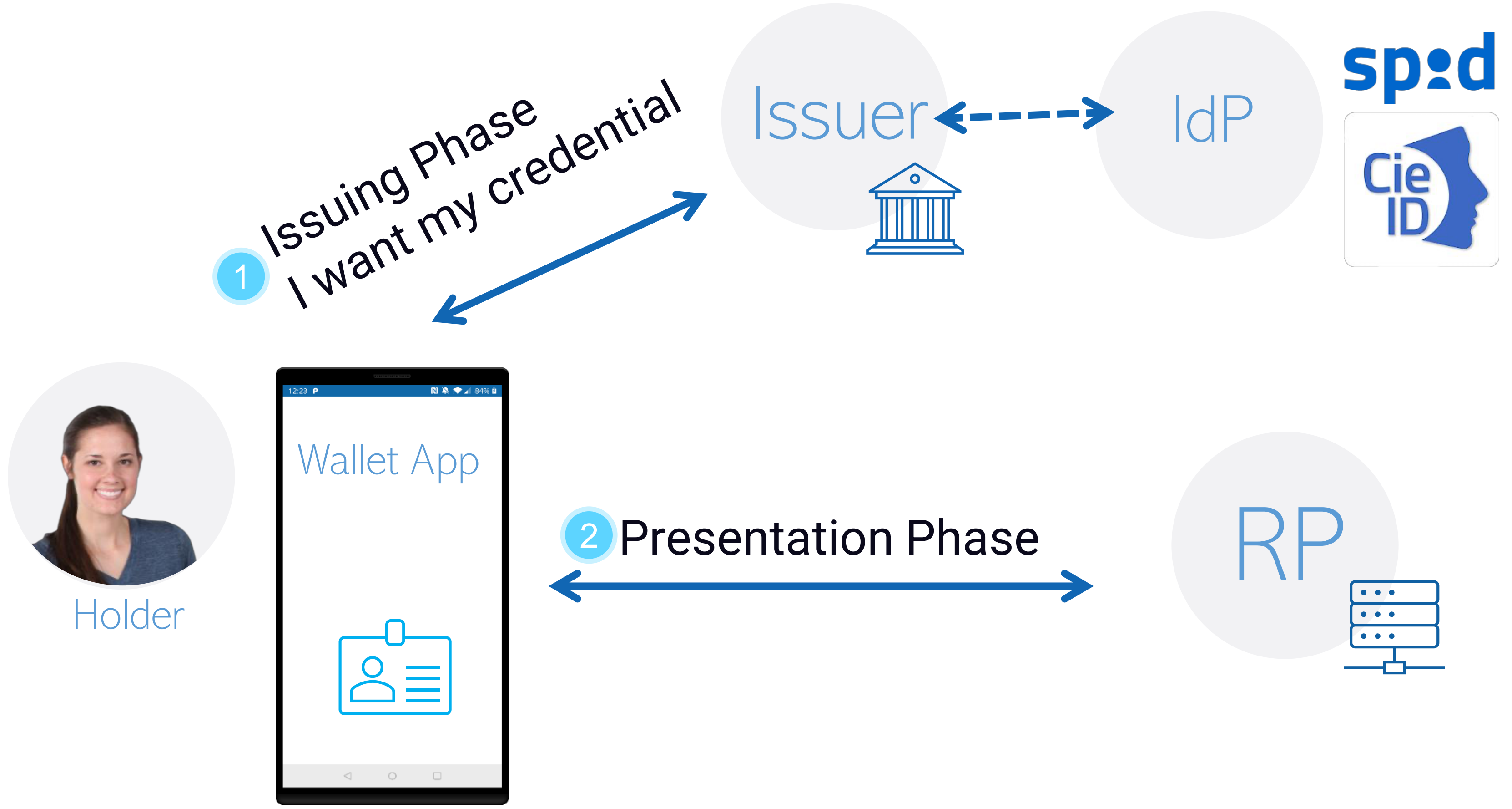
- – centralized providers may track user activity across services
- – central data storage increases breach risks
- – excessive sharing of personal information can lead to tracking and data monetization by services
- – it requires connectivity, only online scenarios

EUDI Wallet Ecosystem
Different Paradigm

The IdP is involved at each user login attempt



eIDAS 1.0



- The User obtains a credential from the Issuer (e.g., after an authentication of level high with IdPs)
- The User presents the credential directly to the RP (no Issuer or IdPs involvement)

eIDAS 2.0

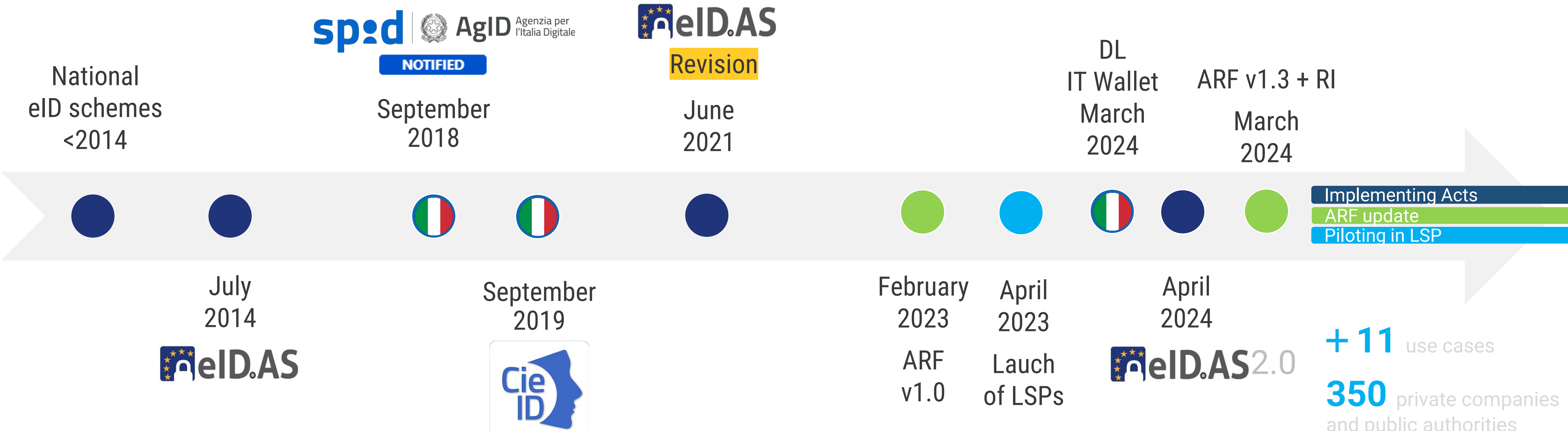
eIDAS Timeline

Legislative — Handled by the European Commission with co-legislators negotiations

Technical — The eIDAS Expert Groups are working on the Technical Specifications (**Architecture and Reference Framework - ARF** and **Reference Implementation**)

Large Scale Pilots — Grant under the Digital European Programme are started with the aim of testing functionalities and interoperability for cross border use cases

Provide feedback to



MINISTERO DELL'INTERNO | POLIGRAFICO E ZECCA DELLO STATO ITALIANO

NOBID CONSORTIUM — EWC — DC4EU — Potential For European Digital Identity

+11 use cases

350 private companies and public authorities

26+ Member States

EUDI Wallet
Our Involvement

Potential
For European Digital Identity

Co-funded by
the European Union

PROVINCIA AUTONOMA DI TRENTO

Trentino Digitale SpA

- PilOTs for EuropeaN digital Identity wALlet
- 6 use cases: eGov Services, Bank Account Opening, SIM Card Registration, Mobile Driving Licence, Qualified eSignature, ePrescription

IT Wallet technical specification

https://italia.github.io/eudi-wallet-it-docs/versione-corrente/

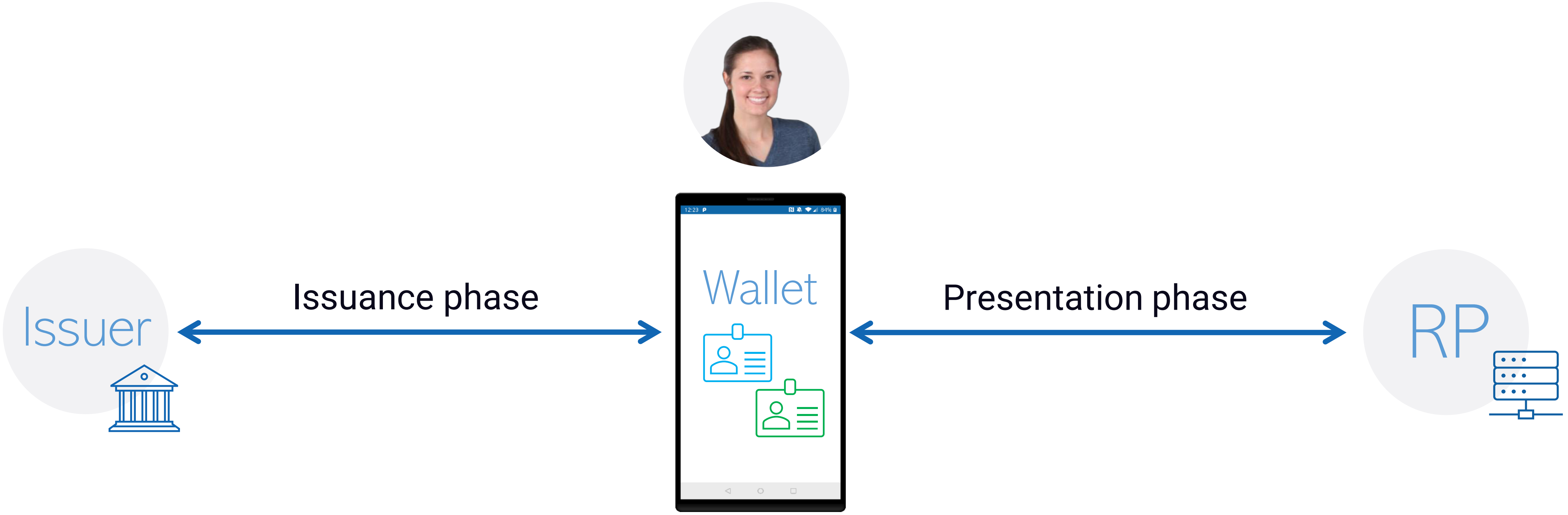
POLIGRAFICO
E ZECCA
DELLO STATO
ITALIANO

Issuer

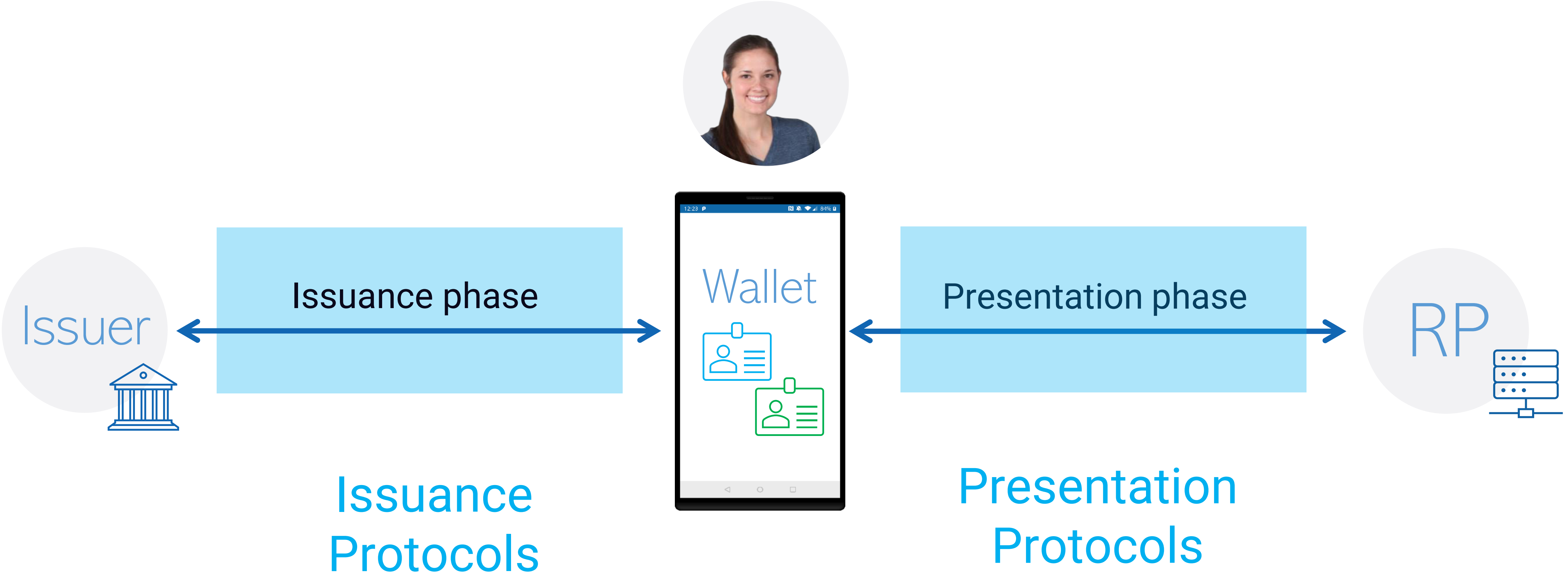
pagopa

Wallet Provider

EUDI Wallet
Challenges

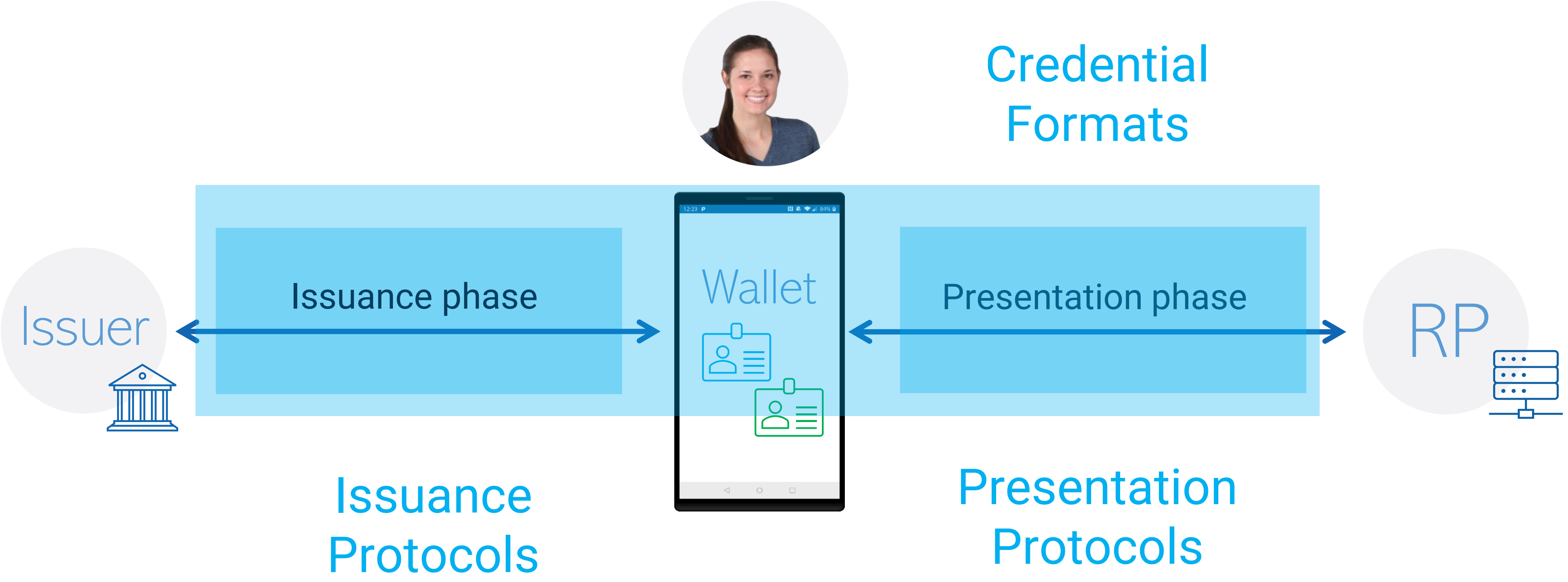


EUDI Wallet
Challenges



- New protocol flows (issuance, presentation, …)

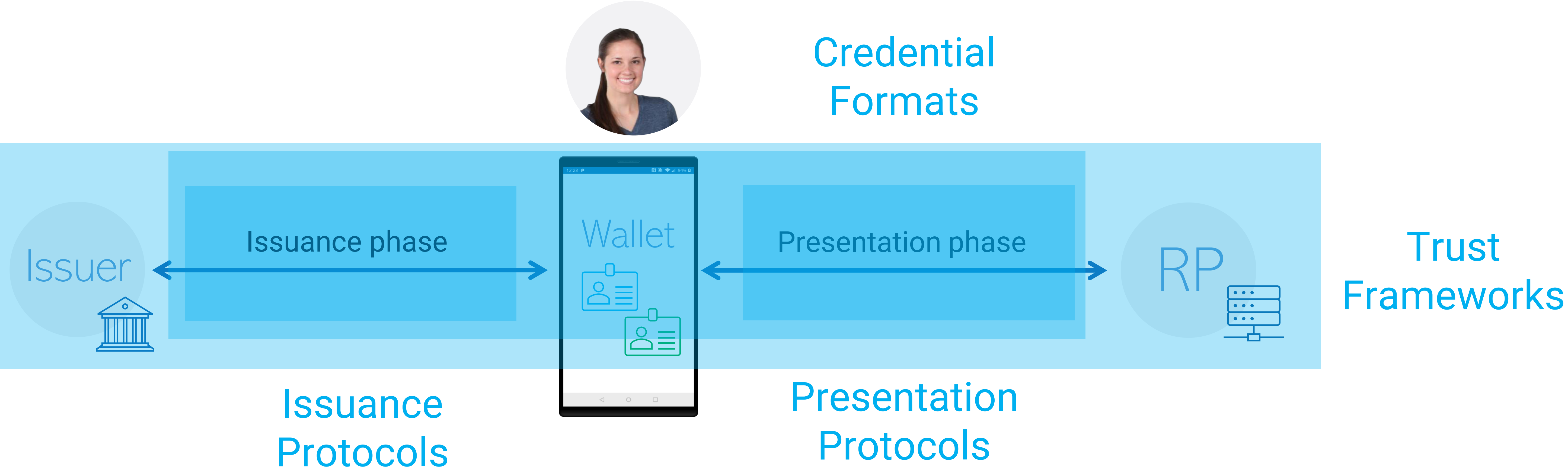
EUDI Wallet
Challenges



- New protocol flows (issuance, presentation, …)
- New credential formats, features (e.g., selective disclosure), and lifecycle (e.g., revocation)

EUDI Wallet Challenges

Privacy, security and interoperability



- New protocol flows (issuance, presentation, …)
- New credential formats, features (e.g., selective disclosure), and lifecycle (e.g., revocation)
- New way to manage the trust

Digital identity wallet
Outline

EU
European Digital Identity Wallet
Obtain and present your documents
Enter

EUDI Wallet Overview
Evolution of the eIDAS ecosystem and our research activities

Trust Framework
Overview

Selective Disclosure and Revocation Mechanisms
Overview and comparison of different approaches

Secure elements
Overview and comparison

Threat Model and Risk Analysis for the Wallet Ecosystem
Discussion on overall security and privacy aspects of digital identity wallets

Digital identity wallet

Outline

EU
European Digital Identity Wallet
Obtain and present your documents
Enter

EUDI Wallet Overview

Evolution of the eIDAS ecosystem and our research activities

Trust Framework

Overview

Selective Disclosure and Revocation Mechanisms

Overview and comparison of different approaches

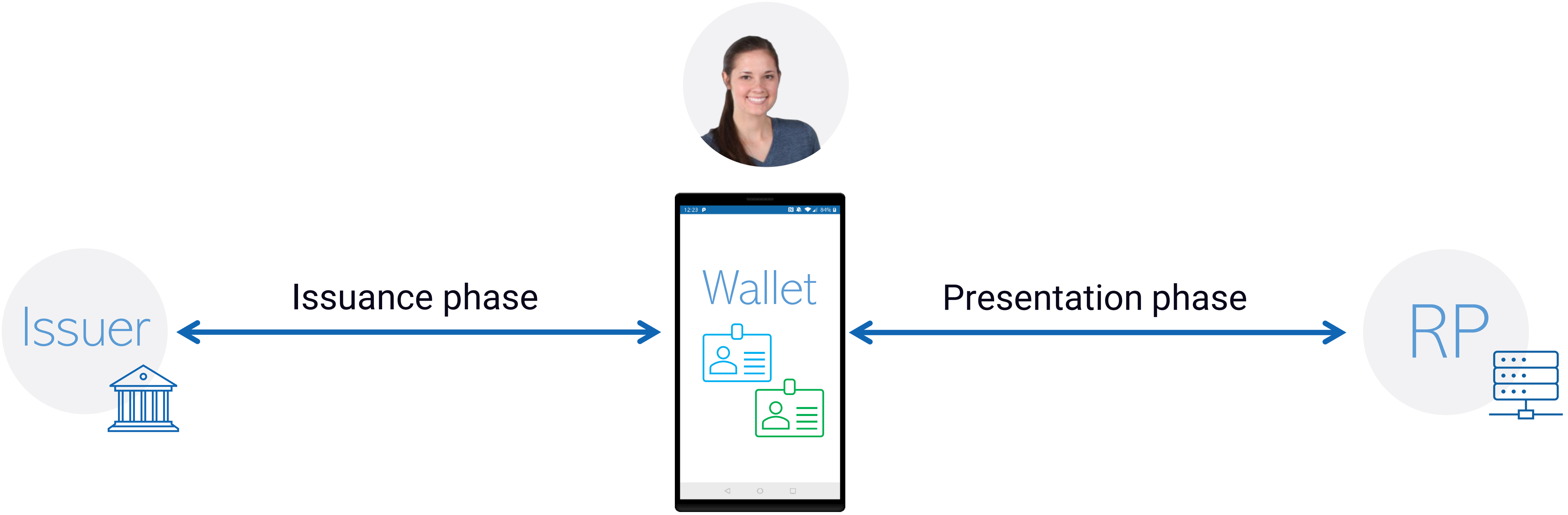
Secure elements

Overview and comparison

Threat Model and Risk Analysis for the Wallet Ecosystem

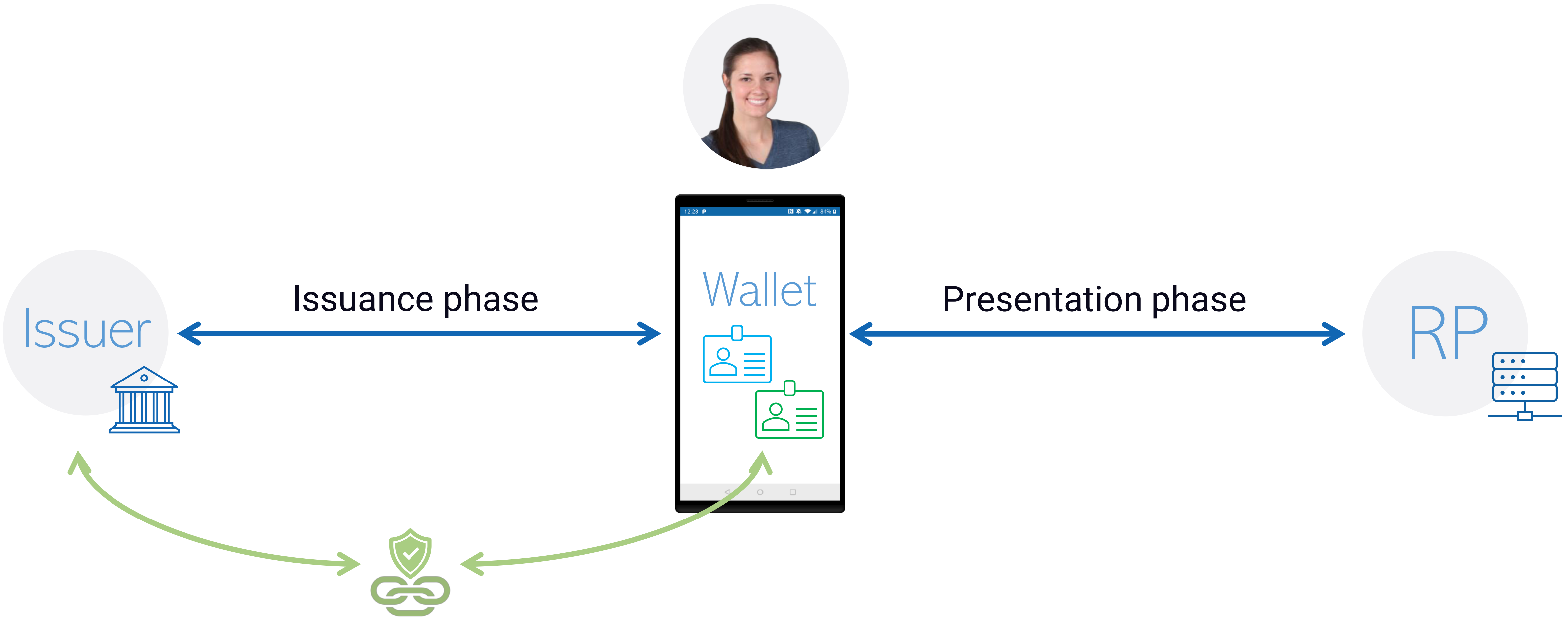
Discussion on overall security and privacy aspects of digital identity wallets

Trust in EUDIW
What exactly is meant by “TRUST”?



Trust in EUDIW

What exactly is meant by “TRUST”?

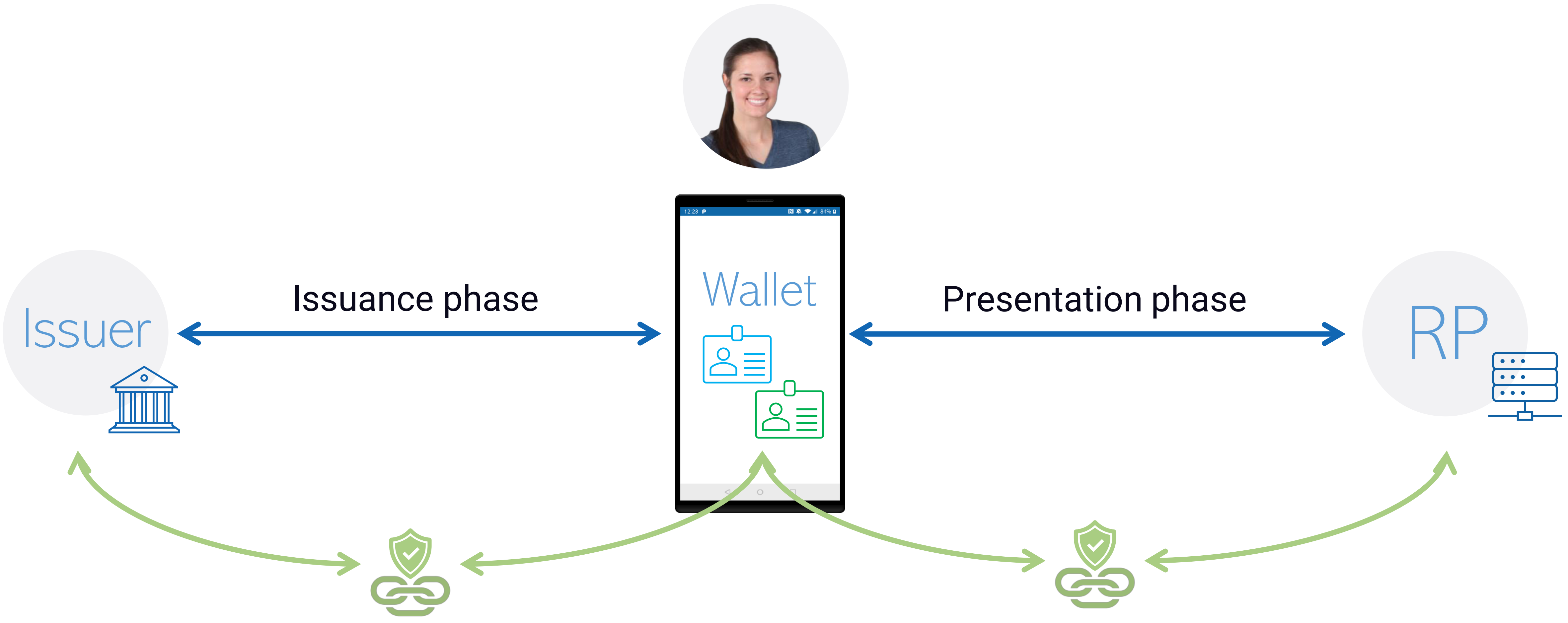


Establishes the trust

Wallet checks that the Issuer is trusted (i.e., eligible to issue that credential)

Issuer checks the integrity, genuinity, capabilities of the Wallet and that is provided by a trusted Wallet Provider

Trust in EUDIW
What exactly is meant by “TRUST”?



Establishes the trust

Wallet checks that the Issuer is trusted (i.e., eligible to issue that credential)

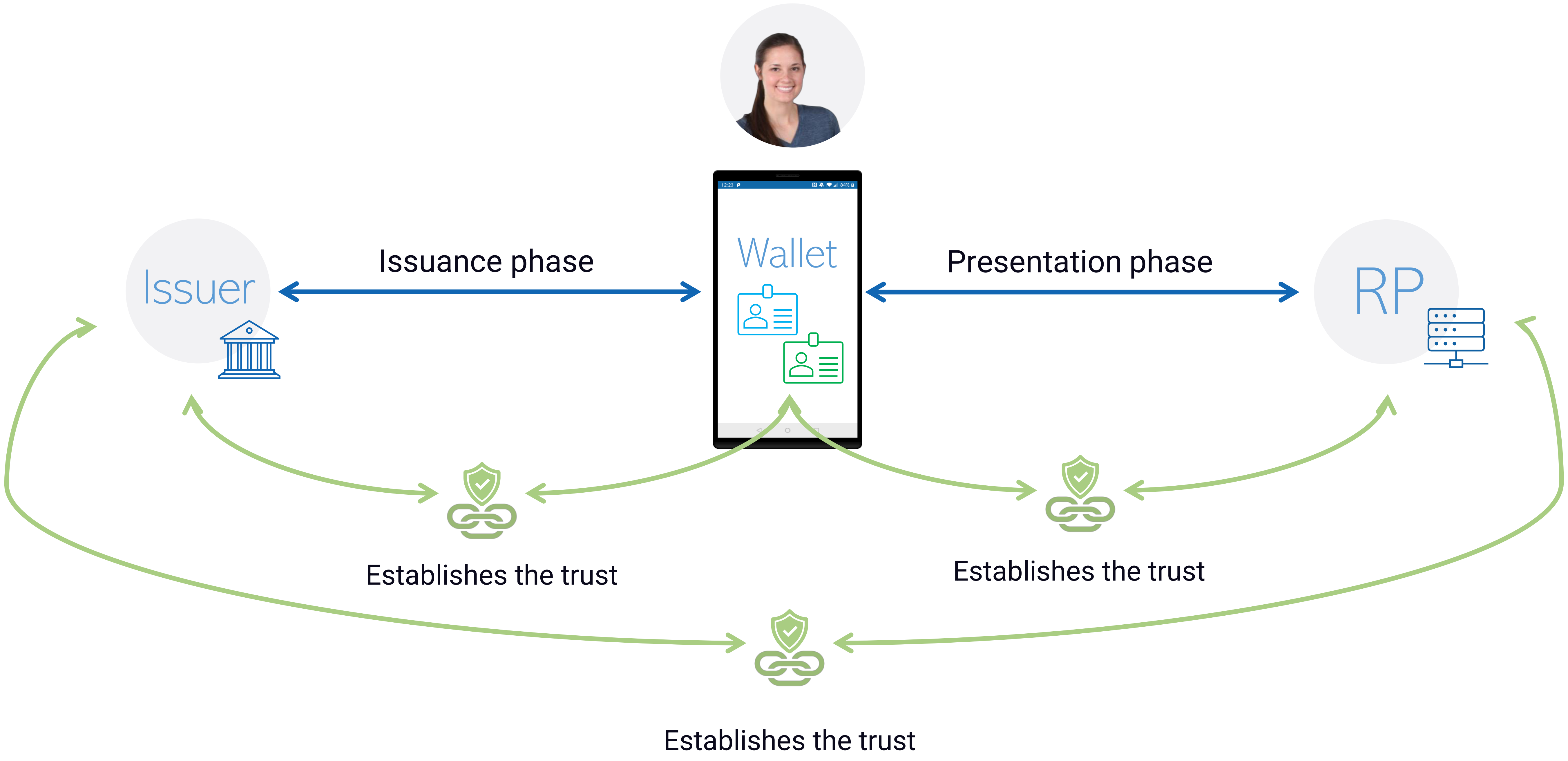
Issuer checks the integrity, genuinity, capabilities of the Wallet and that is provided by a trusted Wallet Provider

Establishes the trust

Wallet checks the trust of the RP (i.e., eligible to request that credential)

RP checks the integrity and genuity of the Wallet and that is provided by a trusted Wallet Provider

Trust in EUDIW
What exactly is meant by "TRUST"?



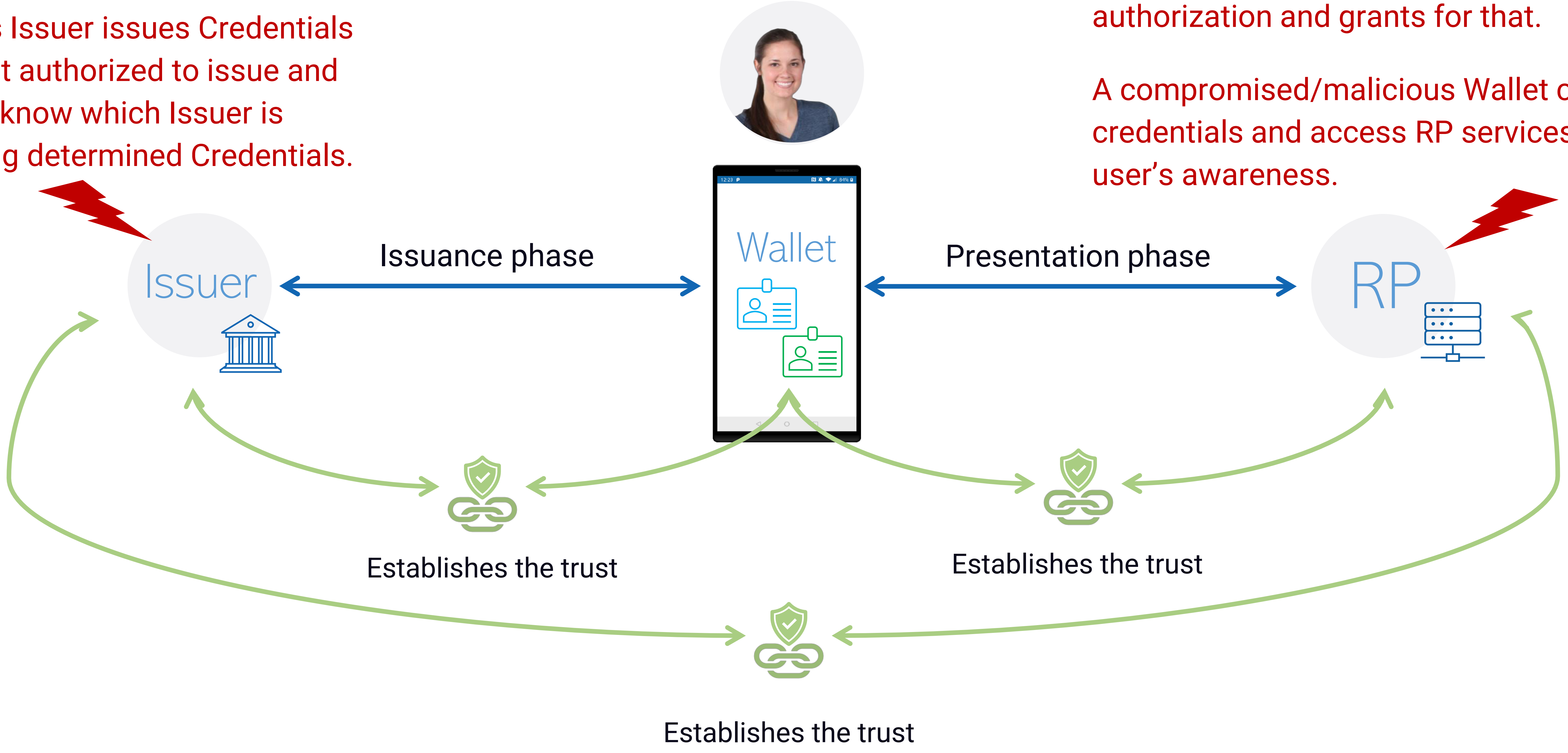
RP checks that the Issuer is trusted (i.e., eligible to issue that credential) and the status of the Credential

Trust in EUDIW
What exactly is meant by “TRUST”?

A fake/malicious Issuer issues Credentials for which is is not authorized to issue and an RP would not know which Issuer is eligible for issuing determined Credentials.

An RP would overask for user attributes without authorization and grants for that.

A compromised/malicious Wallet could obtain user credentials and access RP services without the user’s awareness.



Severe privacy and security issues

Trust in EUDIW
What exactly is meant by “TRUST”?

- Trustworthiness and reliability of Issuers, Relying Parties and Wallet Providers (as legal entities) and the technical components provided by them (e.g., Wallet app).
- Authenticity and integrity of Credentials and digital artefacts used in the Credential issuing and presentation phases.

Implementation of these principles involves the use of cryptography

→ use of one or more cryptographic keys uniquely associated to and for the exclusive use of the legitimate owner

→ need for digital certificates to be made available to third parties who need to establish trust with respect to certificate owners

Digital identity wallet
Outline

EU
European Digital Identity Wallet
Obtain and present your documents
Enter

EUDI Wallet Overview

Evolution of the eIDAS ecosystem and our research activities

Trust Framework

Overview

Selective Disclosure and Revocation Mechanisms

Overview and comparison of different approaches

Secure elements

Overview and comparison

Threat Model and Risk Analysis for the Wallet Ecosystem

Discussion on overall security and privacy aspects of digital identity wallets

Digital identity wallet
Outline

EU
European Digital Identity Wallet
Obtain and present your documents
Enter

EUDI Wallet Overview

Evolution of the eIDAS ecosystem and our research activities

Trust Framework

Overview

Selective Disclosure and Revocation Mechanisms

Overview and comparison of different approaches

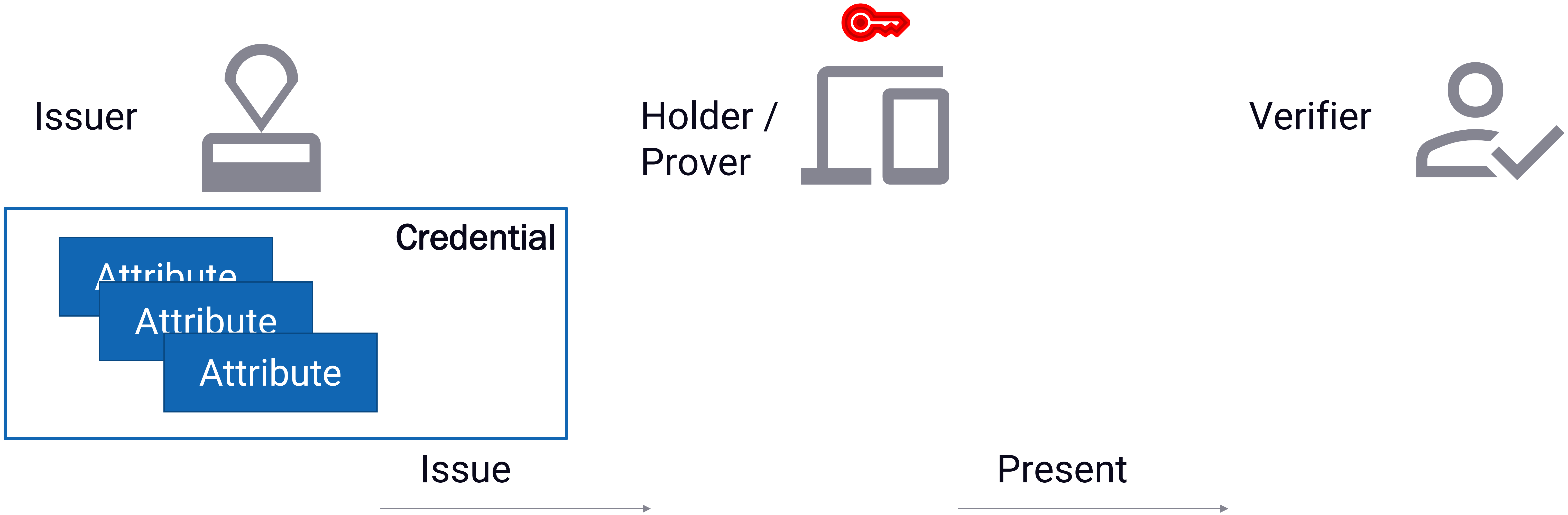
Secure elements

Overview and comparison

Threat Model and Risk Analysis for the Wallet Ecosystem

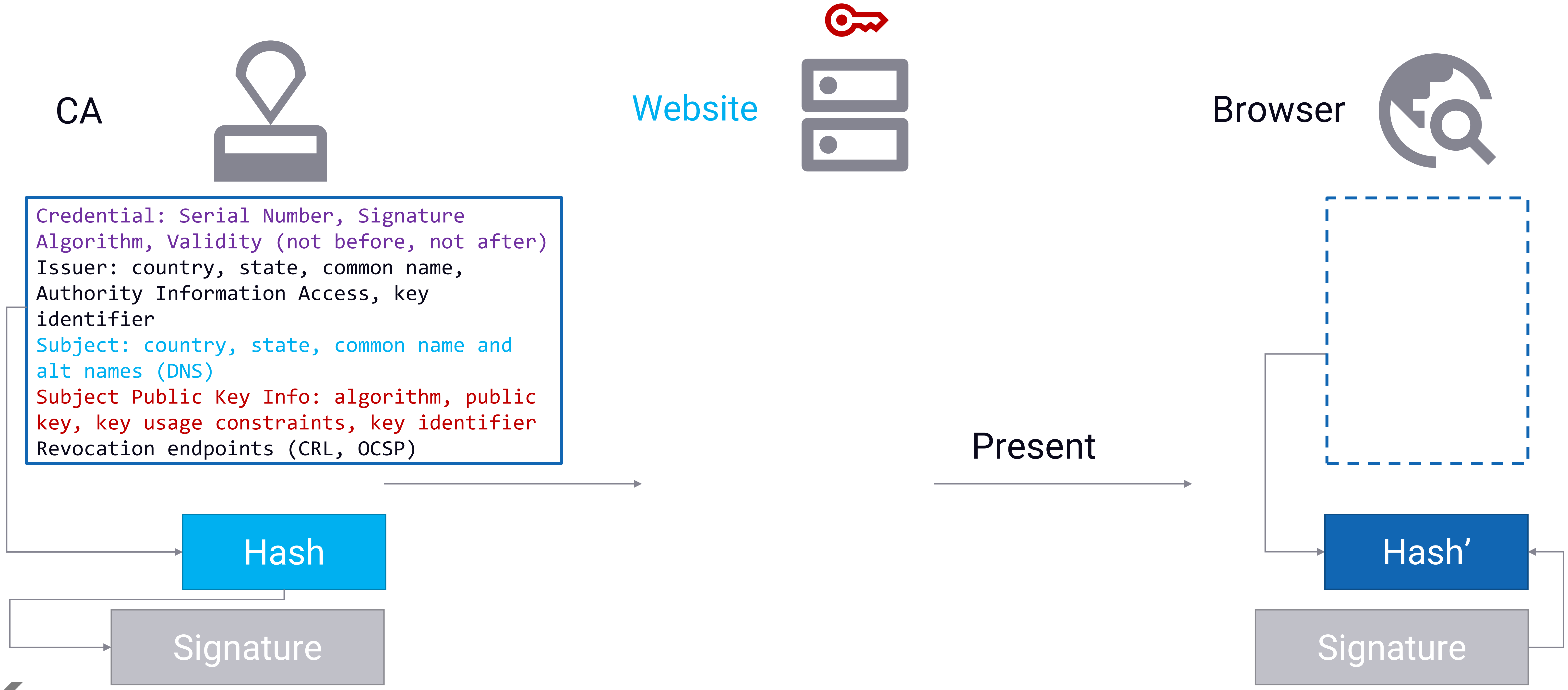
Discussion on overall security and privacy aspects of digital identity wallets

Credential
Definitions



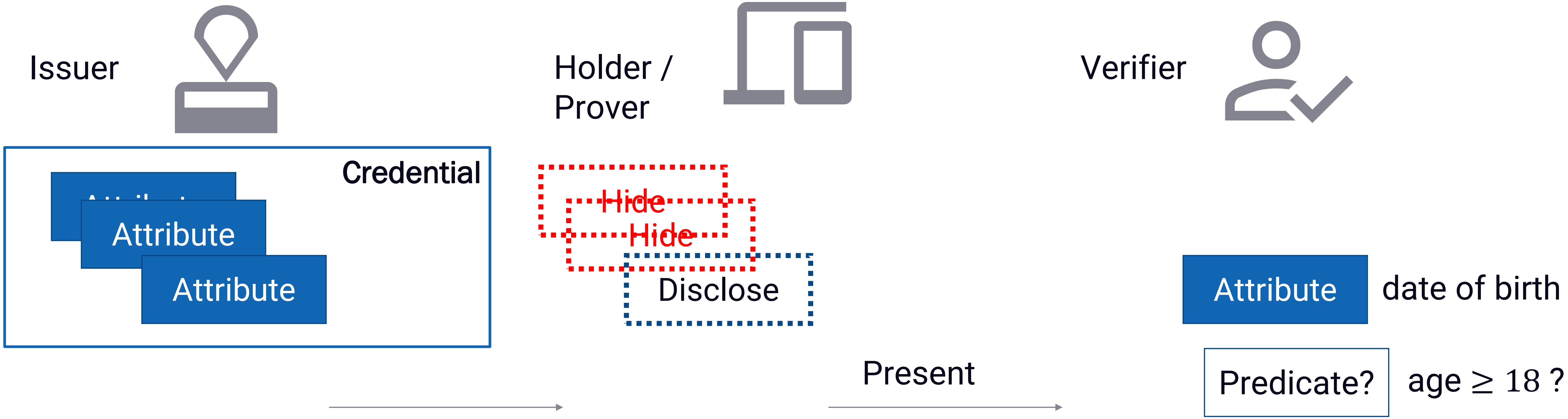
- Identity: “An attribute or set of attributes that uniquely describe a subject within a given context.”
- Credential: “An object or data structure that authoritatively binds an identity - via an identifier or identifiers - and (optionally) additional attributes, to at least one authenticator possessed and controlled by a subscriber.”

Credential example
X.509 certificate



Credential: Serial Number, Signature Algorithm, Validity (not before, not after)
Issuer: country, state, common name, Authority Information Access, key identifier
Subject: country, state, common name and alt names (DNS)
Subject Public Key Info: algorithm, public key, key usage constraints, key identifier
Revocation endpoints (CRL, OCSP)

Selective disclosure
Objective



Issuer

Credential

Attribute

Attribute

Attribute

Holder /
Prover

Hide

Hide

Disclose

Present

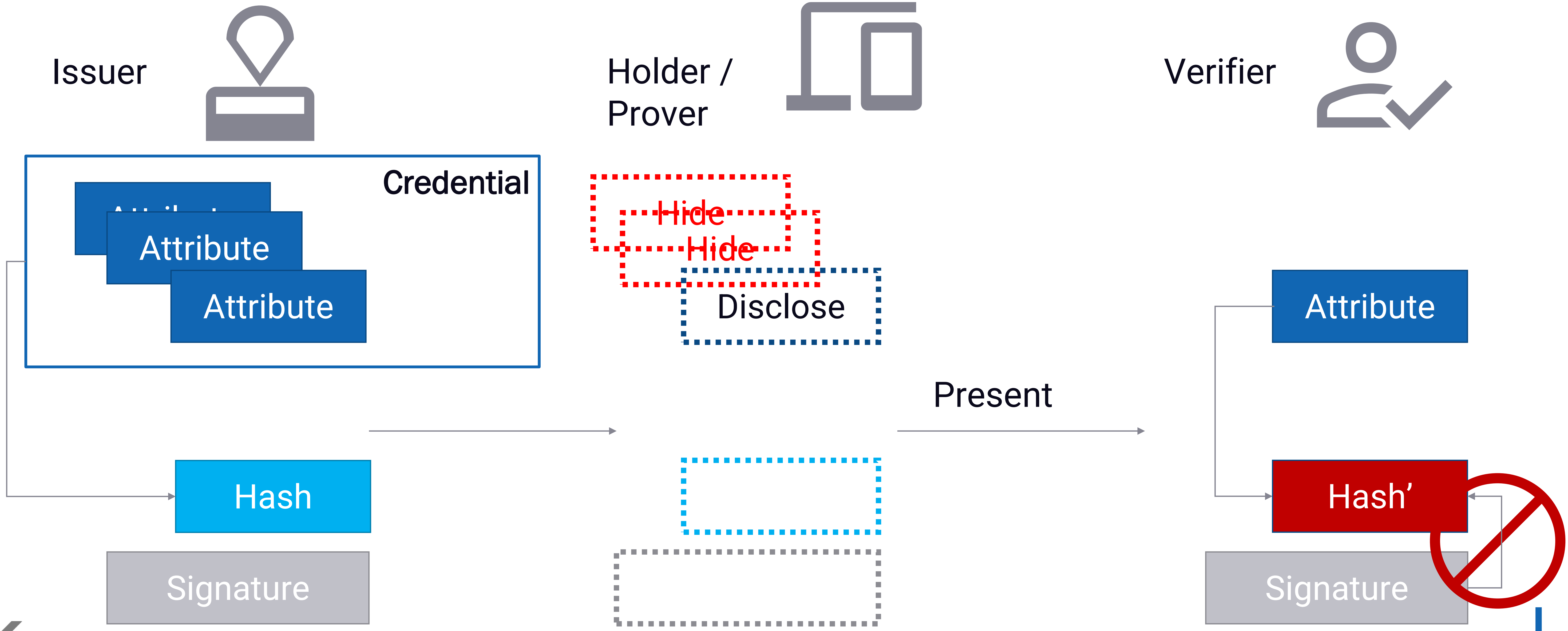
Verifier

Attribute date of birth

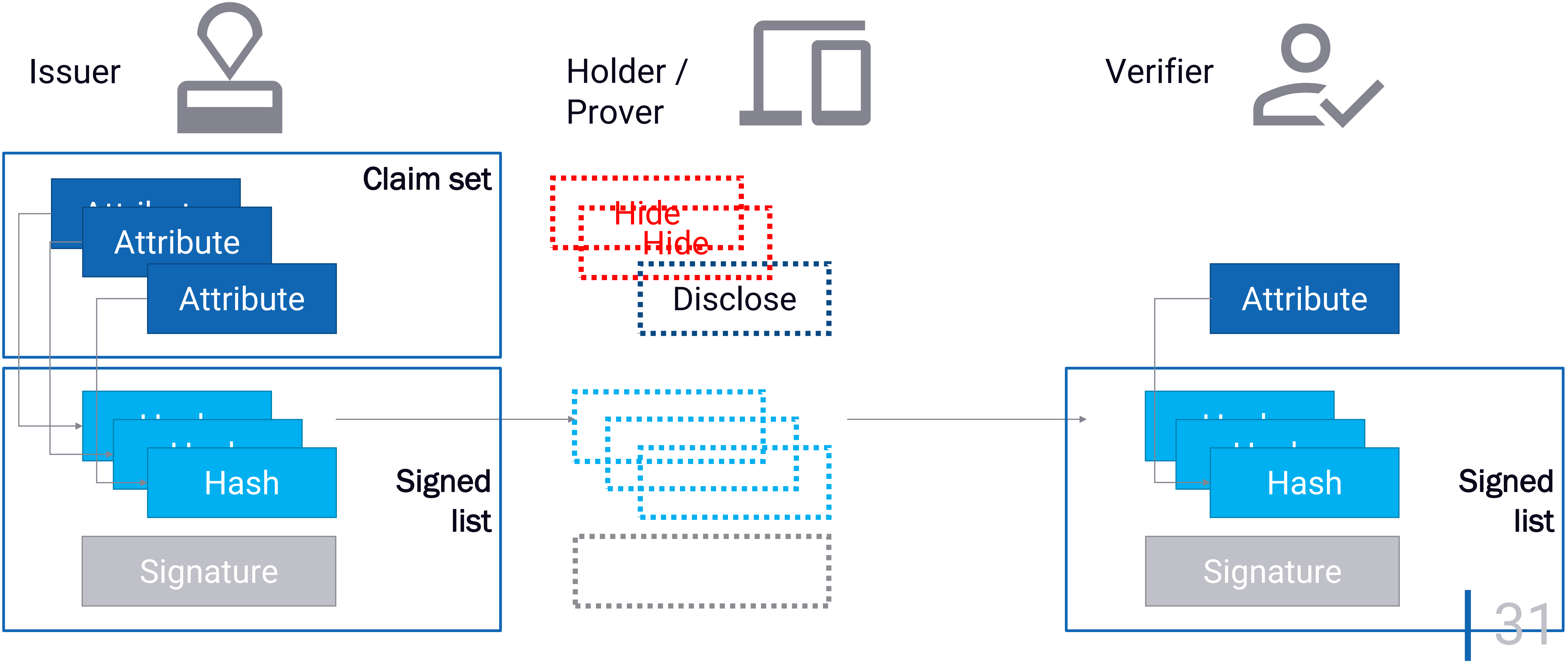
Predicate? age ≥ 18 ?

“The ability of a holder to make fine-grained decisions about what information to share.” [VC]

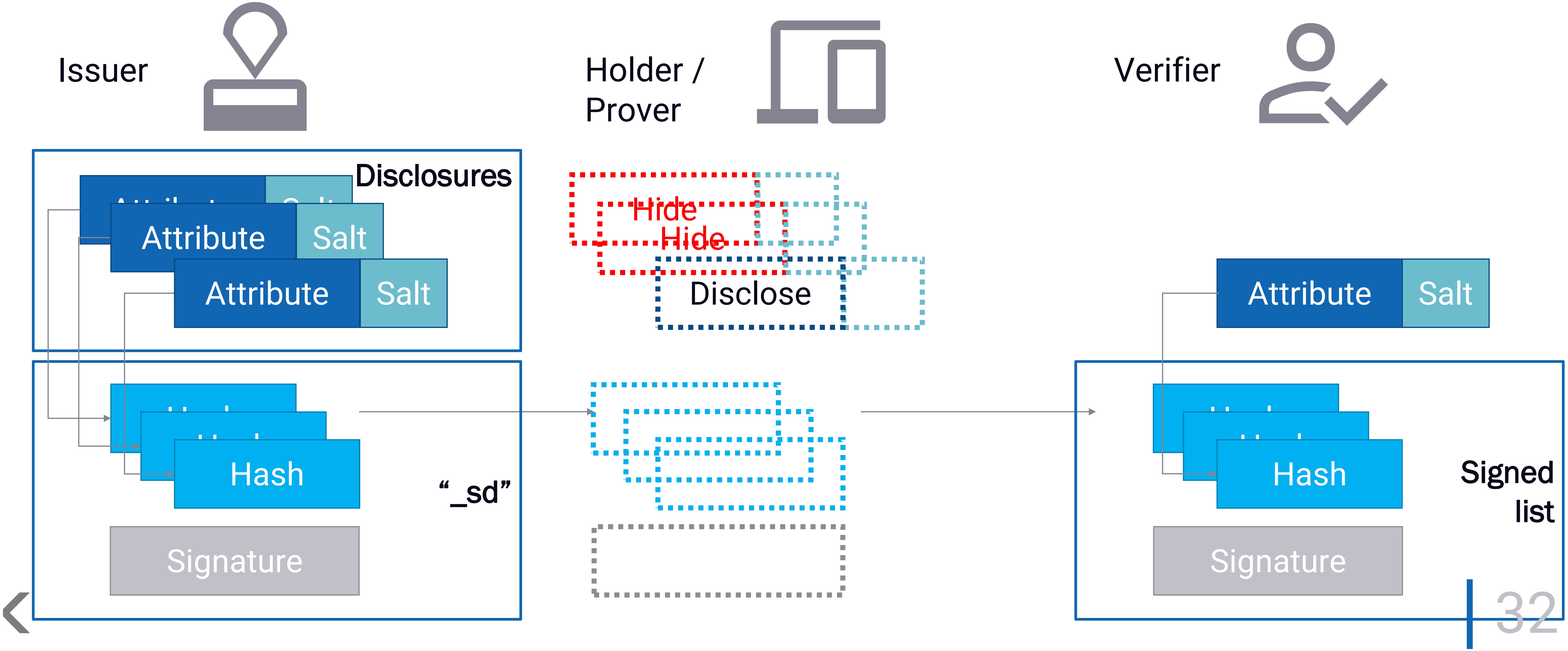
Selective disclosure
Verification (technical challenge)



Selective disclosure
Hash list



Selective disclosure
Salted hash list



Selective disclosure
Example SD-JWT - Issued

Attribute

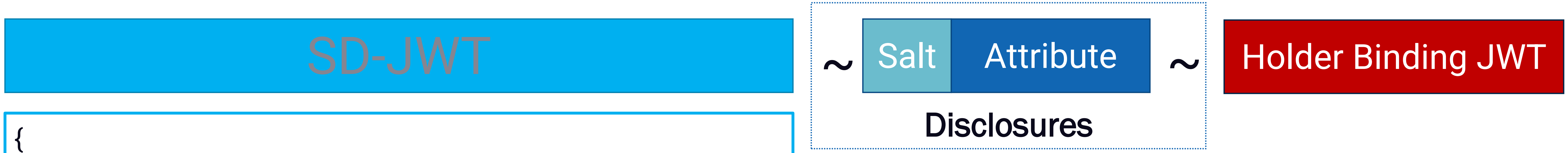
```
{
  "sub": "john_doe_42",
  "given_name": "John",
  "family_name": "Doe",
  "email": "johndoe@example.com",
  "phone_number": "+1-202-555-0101",
  "address": {
    "street_address": "123 Main St",
    "locality": "Anytown",
    "region": "Anystate",
    "country": "US"
  },
  "birthdate": "1940-01-01"
}
```

```
{
  "_sd": [
    "5nXy0Z3QiEba1V1lJzeKhAOGQXFlKLIWCLlhf_O-cmo",
    "9gZhHAhV7LZnOFZq_q7Fh8rzdqrrNM-hRWsVOlW3nuw",
    "S-JPBSkvqliFv1__thuXt3IzX5B_ZXm4W2qs4BoNFrA",
    "bviw7pWAkbzI078ZNVa_eMZvk0tdPa5w2o9R3Zycjo4",
    "o-LBCDrFF6tC9ew1vAlUmw6Y30CHZF5jOUFhpx5mogI",
    "pzkHIM9sv7oZH6YKDsRqNgFGLpEKIj3c5G6UKaTsAjQ",
    "rnAzCT6DTy4TsX9QCDv2wwAE4Ze20uRigtVNQkA52X0"
  ],
  "iss": "https://example.com/issuer",
  "iat": 1516239022,
  "exp": 1735689661,
  "_sd_alg": "sha-256",
  "cnf": {
    "jwk": {
      "kty": "EC",
      "crv": "P-256",
      "x": "TCAER19Zvu3OHF4j4W4vfSVoHIP1ILilDls7vCeGemc",
      "y": "ZxjiWWbZMQGHVWKVQ4hbSIirsVfuecCE6t4jT9F2HZQ"
}}}
```

Hash

Prover key

Selective disclosure
Example SD-JWT - Presented



```
{
 "_sd": [
  "5nXy0Z3QiEba1V1lJzeKhAOGQXFlKLIWCLlhf_O-cmo",
  "9gZhHAhV7LZnOFZq_q7Fh8rzdqrrNM-hRWsVOlW3nuw",
  "S-JPBSkvqliFv1__thuXt3IzX5B_ZXm4W2qs4BoNFrA",
  "bviw7pWAkbzI078ZNVa_eMZvk0tdPa5w2o9R3Zycjo4",
  "o-LBCDrFF6tC9ew1vAlUmw6Y30CHZF5jOUFhpx5mogI",
  "pzkHIM9sv7oZH6YKDsRqNgFGLpEKIj3c5G6UKaTsAjQ",
  "rnAzCT6DTy4TsX9QCDv2wwAE4Ze20uRigtVNQkA52X0"
 ],
 "iss": "https://example.com/issuer",
 "iat": 1516239022,
 "exp": 1735689661,
 "_sd_alg": "sha-256",
 "cnf": {
  "jwk": {
   "kty": "EC",
   "crv": "P-256",
   "x": "TCAER19Zvu3OHF4j4W4vfSVoHIP1ILilDls7vCeGemc",
   "y": "ZxjiWWbZMQGHVWKVQ4hbSIirsVfuecCE6t4jT9F2HZQ"
}}}
```

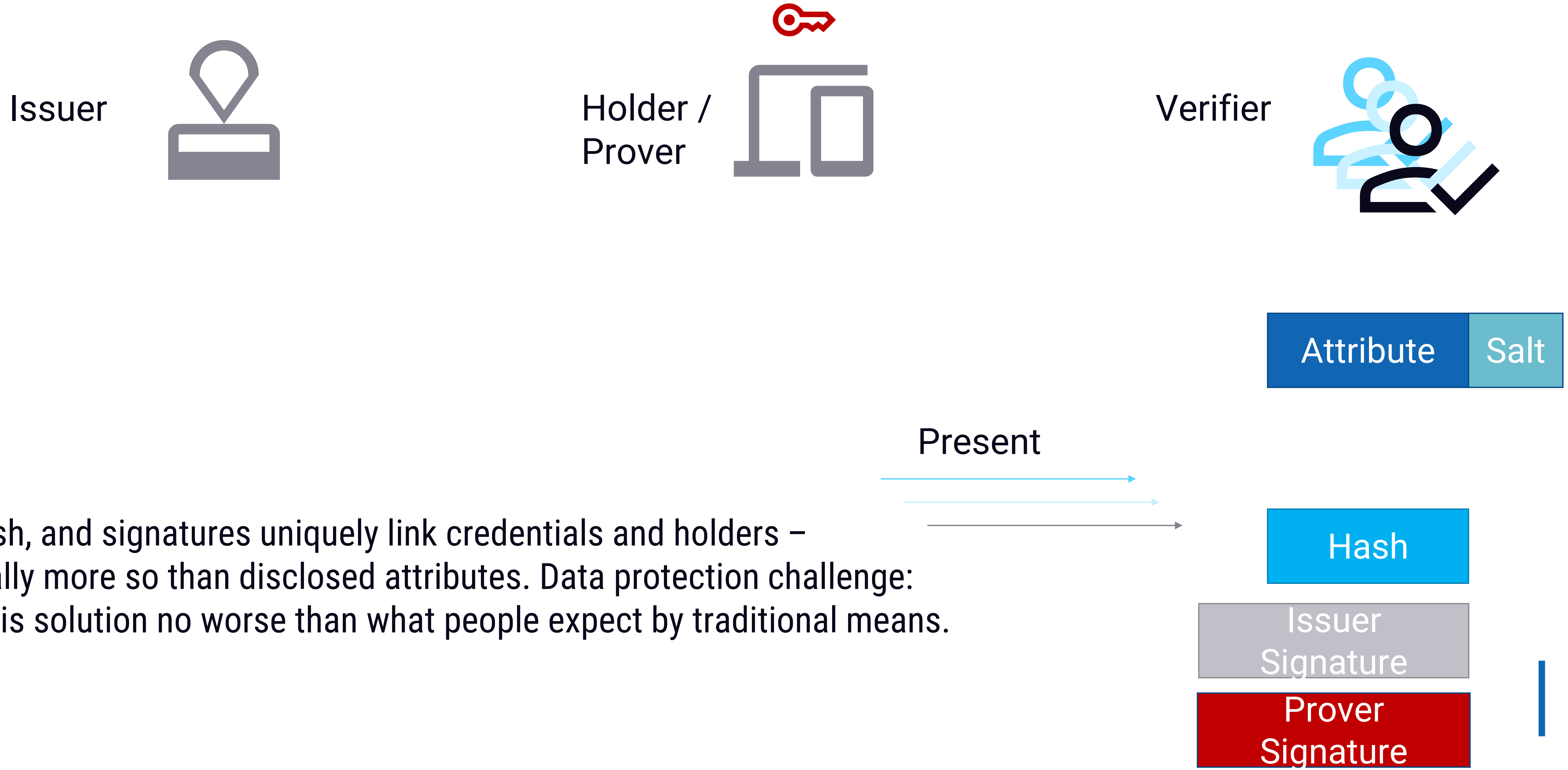
```
["rSLuznhiLPBDRZE1CZ88KQ", "sub", "john_doe_42"]
```

```
["Na3VoFFnVw28jOArk7INVg", "address",
{"street_address": "123 Main St", "locality":
"Anytown", "region": "Anystate", "country": "US"}]
```

```
{
 "alg": "ES256"
}{
 "nonce": "XZOUco1u_gEPknxS78sWWg",
 "aud": "https://example.com/verifier",
 "iat": 1677838084
}.
```

Prover Signature

Multiple presentation
Correlation (“linkability”)



Issuer

Holder / Prover

Verifier

Attribute | Salt

Present

Hash

Issuer Signature

Prover Signature

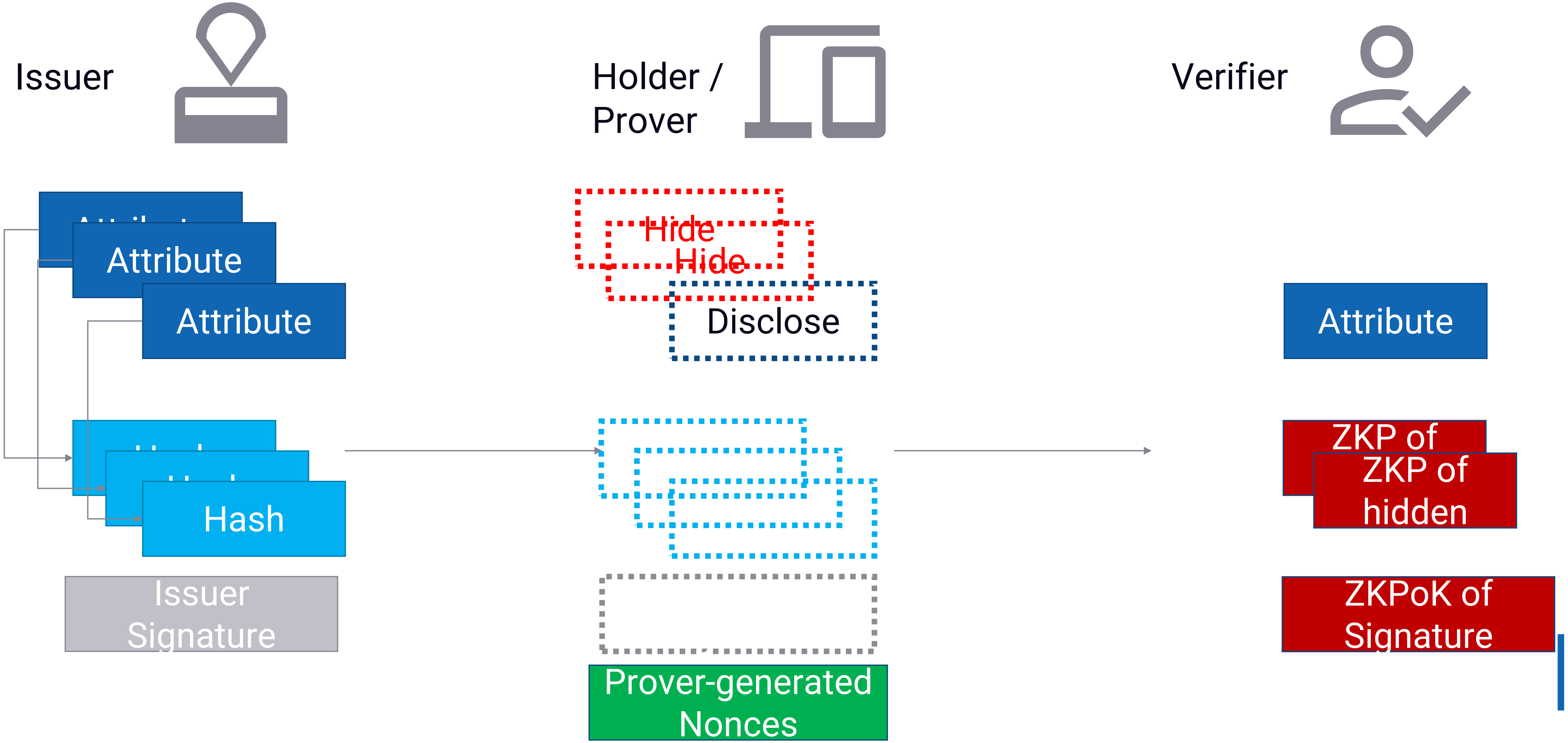
Salt, hash, and signatures uniquely link credentials and holders – potentially more so than disclosed attributes. Data protection challenge: make this solution no worse than what people expect by traditional means.

Linkability
Solutions

- In EUDI ARF: **hashed values + batch issuance**

- **Selective disclosure signatures**: signatures schemes that natively support selective disclosure of VC claims by using **non-interactive zero knowledge proofs NIZKP** (e.g., CL, BBS, BBS+, and PS signatures).
  - the prover generates a proof π and the verifier checks that π is valid without requiring additional interactions between prover and verifier.

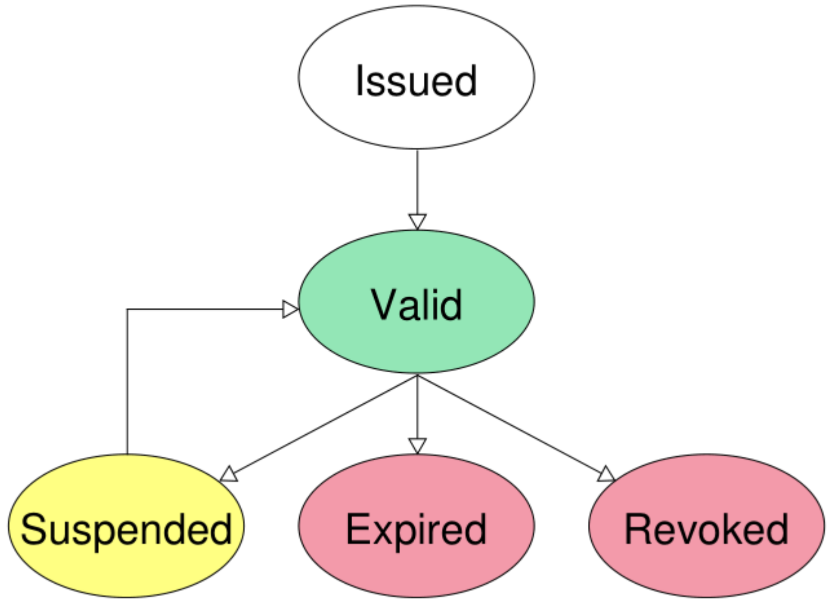
Zero knowledge proofs
Selective disclosure signatures



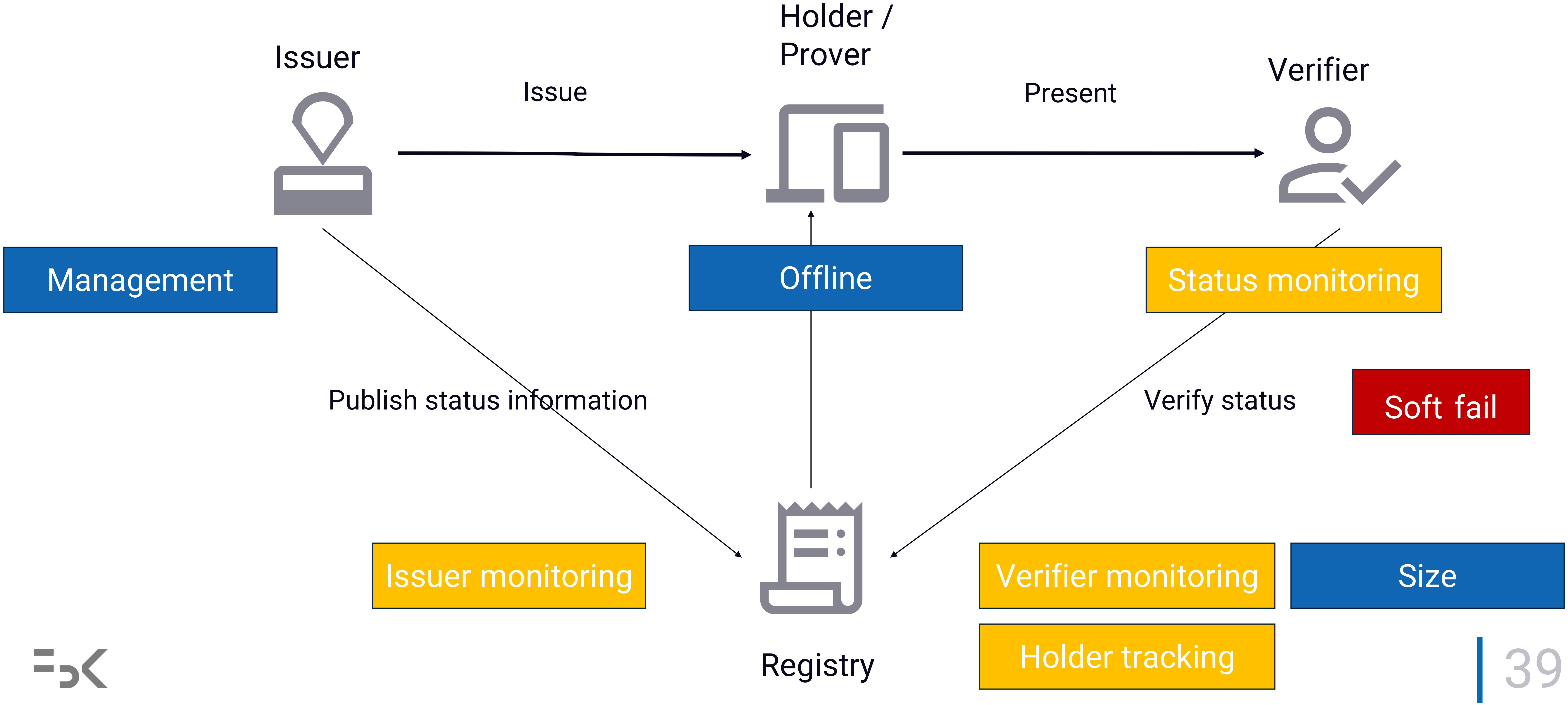
Credential status mechanisms
Revocation

- Managing the lifecycle of long-lived Credential, and in particular its status (e.g., valid or revoked)

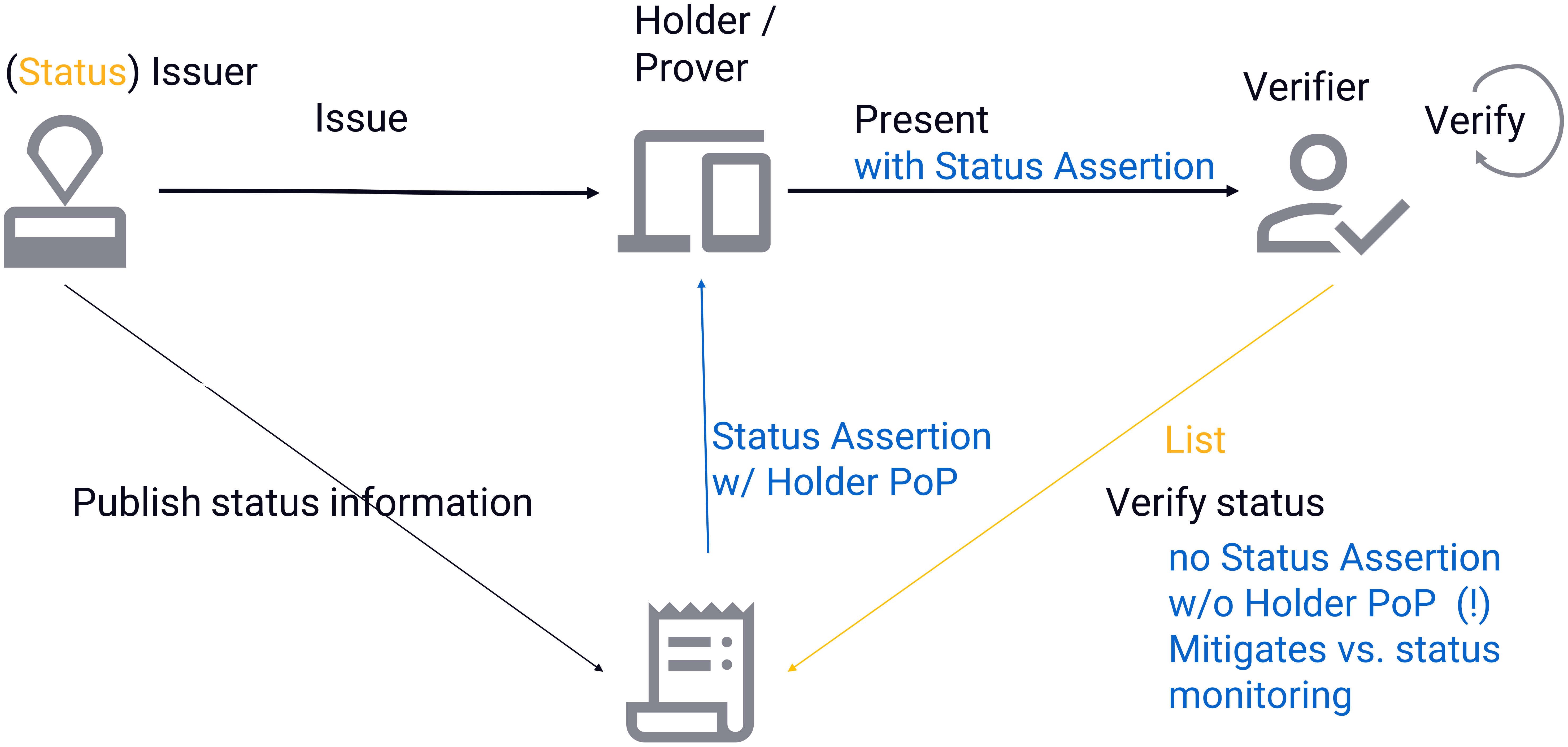
- Different status mechanisms from the literature, grouped by type:
  - **List-based**, e.g., Certificate Revocation Lists (CRL), Token Status List
  - **Assertion-based**, e.g., OCSP with Stapling, OAuth status Assertions (SA)
  - **Hybrid**, e.g., Cryptographic Accumulators (ACC), Dynamic Status List (DSL)



Credential status mechanisms
Security and Trust and Practicality



Credential status mechanisms
Status List vs. Status Assertion



(Status) Issuer

Issue

Holder / Prover

Present
with Status Assertion

Verifier

Verify

Publish status information

Status Assertion
w/ Holder PoP

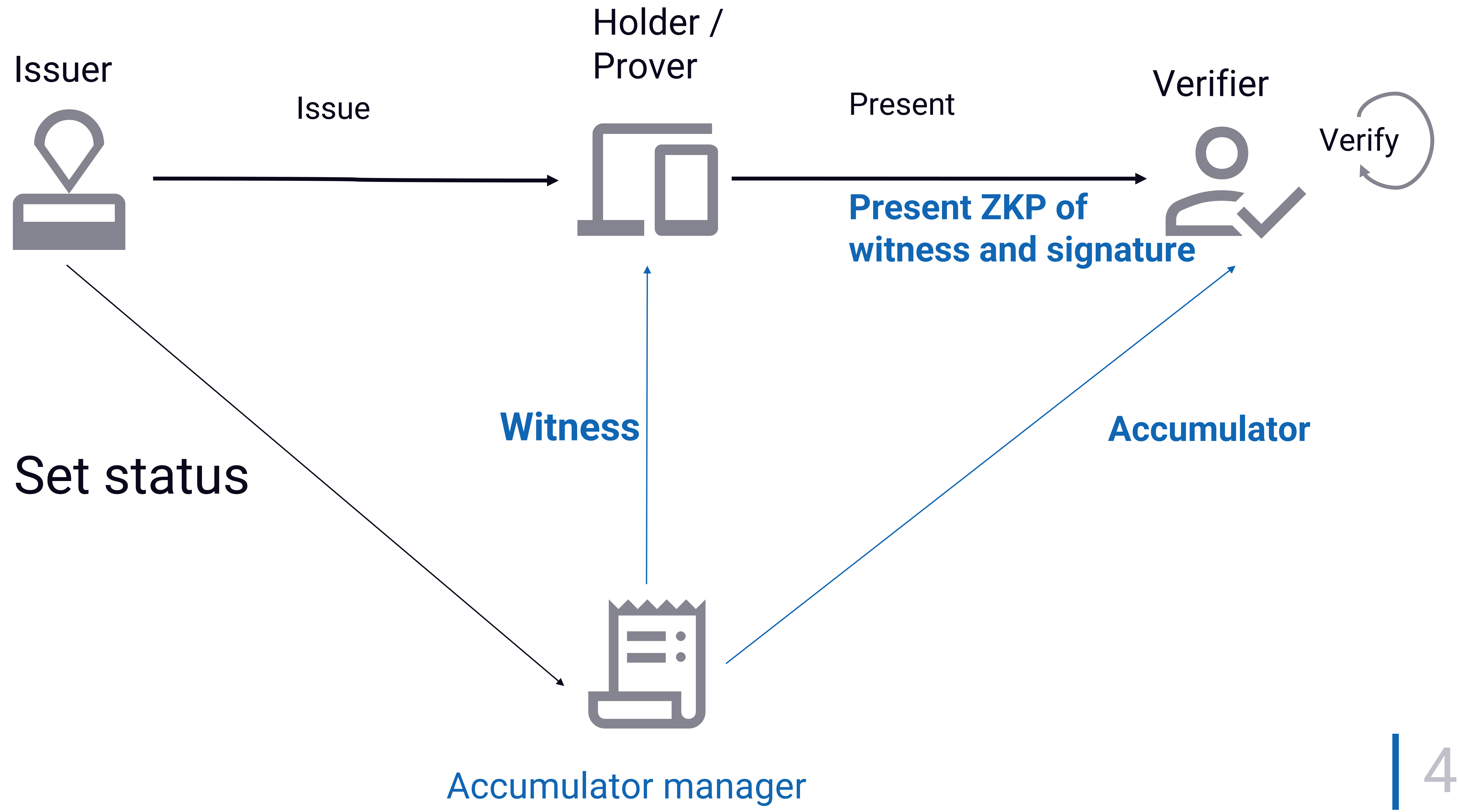
List

Verify status

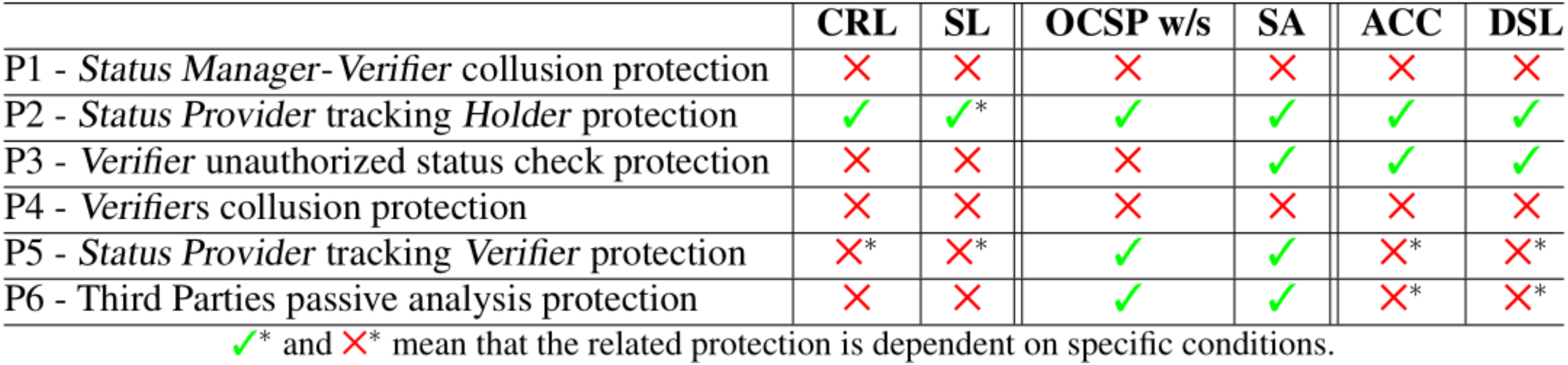
no Status Assertion
w/o Holder PoP (!)
Mitigates vs. status monitoring

Status Provider / Issuer – Status Responder

Credential status mechanisms
Hybrid: Accumulators



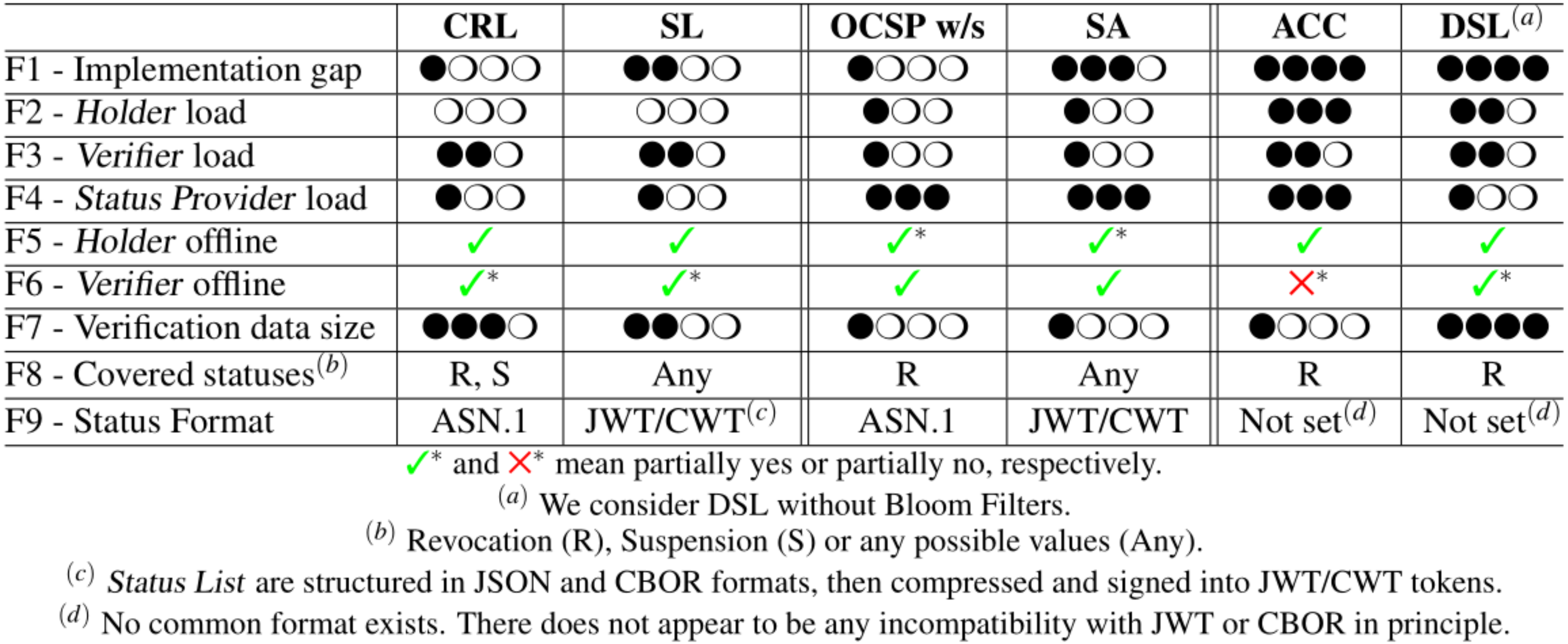
Credential status mechanisms
Privacy Comparison



	List-based		Assertion-based		Hybrid	
	CRL	**SL**	**OCSP w/s**	**SA**	**ACC**	**DSL**
P1 - *Status Manager-Verifier* collusion protection	✗	✗	✗	✗	✗	✗
P2 - *Status Provider* tracking *Holder* protection	✓	✓*	✓	✓	✓	✓
P3 - *Verifier* unauthorized status check protection	✗	✗	✗	✓	✓	✓
P4 - *Verifiers* collusion protection	✗	✗	✗	✗	✗	✗
P5 - *Status Provider* tracking *Verifier* protection	✗*	✗*	✓	✓	✗*	✗*
P6 - Third Parties passive analysis protection	✗	✗	✓	✓	✗*	✗*

✓* and ✗* mean that the related protection is dependent on specific conditions.

Credential status mechanisms
Features Comparison



	List-based		Assertion-based		Hybrid	
	CRL	**SL**	**OCSP w/s**	**SA**	**ACC**	**DSL**[a]
F1 - Implementation gap	●○○○	●●○○	●○○○	●●●○	●●●●	●●●●
F2 - *Holder* load	○○○	○○○	●○○	●○○	●●●	●●○
F3 - *Verifier* load	●●○	●●○	●○○	●○○	●●○	●●○
F4 - *Status Provider* load	●○○	●○○	●●●	●●●	●●●	●○○
F5 - *Holder* offline	✓	✓	✓*	✓*	✓	✓
F6 - *Verifier* offline	✓*	✓*	✓	✓	✗*	✓*
F7 - Verification data size	●●●○	●●○○	●○○○	●○○○	●○○○	●●●●
F8 - Covered statuses[b]	R, S	Any	R	Any	R	R
F9 - Status Format	ASN.1	JWT/CWT[c]	ASN.1	JWT/CWT	Not set[d]	Not set[d]

✓* and ✗* mean partially yes or partially no, respectively.

[a] We consider DSL without Bloom Filters.

[b] Revocation (R), Suspension (S) or any possible values (Any).

[c] *Status List* are structured in JSON and CBOR formats, then compressed and signed into JWT/CWT tokens.

[d] No common format exists. There does not appear to be any incompatibility with JWT or CBOR in principle.

Digital identity wallet

Outline

EU
European Digital Identity Wallet
Obtain and present your documents
Enter

EUDI Wallet Overview

Evolution of the eIDAS ecosystem and our research activities

Trust Framework

Overview

Selective Disclosure and Revocation Mechanisms

Overview and comparison of different approaches

Secure elements

Overview and comparison

Threat Model and Risk Analysis for the Wallet Ecosystem

Discussion on overall security and privacy aspects of digital identity wallets

Digital identity wallet
Outline

EU
European Digital Identity Wallet
Obtain and present your documents
Enter

EUDI Wallet Overview
Evolution of the eIDAS ecosystem and our research activities

Trust Framework
Overview

Selective Disclosure and Revocation Mechanisms
Overview and comparison of different approaches

Secure elements
Overview and comparison

Threat Model and Risk Analysis for the Wallet Ecosystem
Discussion on overall security and privacy aspects of digital identity wallets

Secure storage

- Users utilize credentials to authenticate themselves both **online** and **offline** across the EU, meeting different eIDAS levels of assurance (**LoAs**) for various **use cases**, e.g. governmental services, mobile driving licenses.

- The EUDI Architecture and Reference Framework (EUDI-ARF), formulated by the eIDAS Expert Group, outlines technical standards and best practice guidelines for creating interoperable EUDI Wallet implementations
- **Component: Wallet Secure Cryptographic Device (WSCD)**

Secure storage

Hardware-based implementations of the EUDI Wallet Secure Cryptographic Device

- EUDI-ARF proposes:

Local

- integrated within the User's device.

Local External

- External hw components interacting with User's device

Remote

- situated remotely, separate from the user's device

Secure storage

Italian Market Analysis

using data from: StatCounter GlobalStats, Canalys, and Kantar

Mobile OS	Mobile Vendor	Vendor Market Share in Italy	Secure Storage	eIDAS High Compliance (CC certified AVA_VAN.5)	eIDAS High Compliance Market Share
iOS 31.48 %	Apple	31.48%	Secure Enclave	×	-
Android 59.02 % & Samsung 0.38 %	Samsung	29.19%	StrongBox S3K250AF eSE and Knox Vault	✓	~ 9.05%
			TEE	×	-
	Xiaomi	14.25%	TEE	×	-
	Huawei	5.03%	Huawei iTrustee v3.0 on Kirin 980	×	-
	Oppo	5.34%	Trustonic TEE Kinibi	×	-
	Realme, Motorola, OnePlus & LG	5.59% ≈ (2.06 +1.87 + 0.89+ 0.77)	TEE	×	-
Android 8.4% & Others 0.4 %	Other or Unknown	9.12 % ≈ (3.21 + 5.91)	Strongbox Titan M2 eSE (in Pixel phones)	✓	~ 1.45%
			TEE	×	-

Local

- integrated within the User's device.

Secure storage

Italian Market Analysis

using data from: StatCounter GlobalStats, Canalys, and Kantar

Mobile OS	Mobile Vendor	Vendor Market Share in Italy	Secure Storage	eIDAS High Compliance (CC certified AVA_VAN.5)	eIDAS High Compliance Market Share
iOS 31.48 %	Apple	31.48%	Secure Enclave	×	-
Android 59.02 % & Samsung 0.38 %	Samsung	29.19%	StrongBox S3K250AF eSE and Knox Vault	✓	~ 9.05%
			TEE	×	-
				×	-
			v3.0 on Kirin 980	×	-
	Oppo	5.34%	Trustonic TEE Kinibi	×	-
	Realme, Motorola, OnePlus & LG	5.59% ≈ (2.06 +1.87 + 0.89+ 0.77)	TEE	×	-
Android 8.4% & Others 0.4 %	Other or Unknown	9.12 % ≈ (3.21 + 5.91)	Strongbox Titan M2 eSE (in Pixel phones)	✓	~ 1.45%
			TEE	×	-

~10.5% (= 9.05% + 1.45%)

of mobile devices currently come equipped with an eIDAS-High-compliant secure storage technology

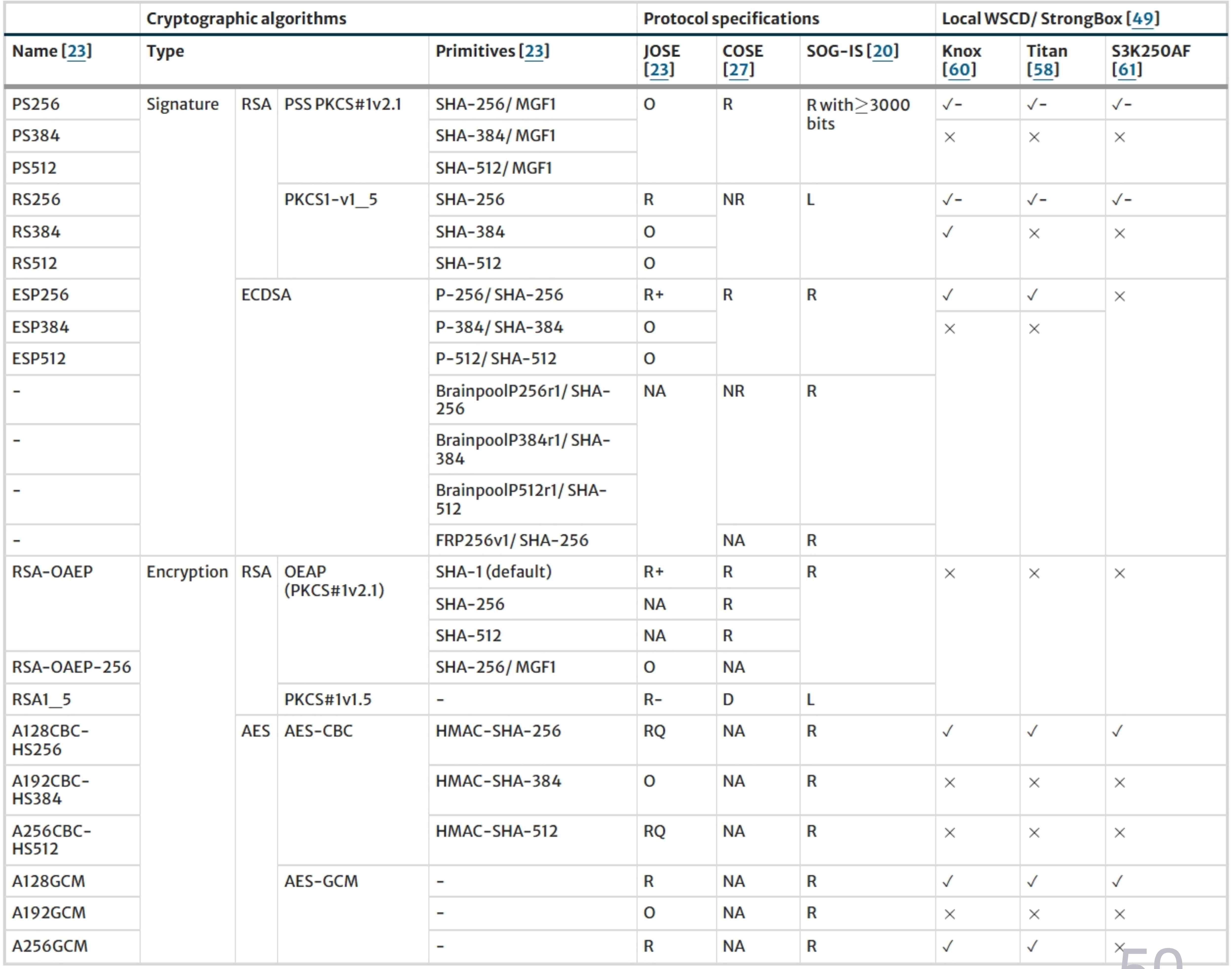
Local

- integrated within the User's device.

Secure Storage

Supported Cryptography

Not every CC-certified eIDAS-High WSCD (Android StrongBox) supports the full EUDI Wallet cryptographic suite—algorithm support is constrained by each device’s secure-element capabilities.



	Cryptographic algorithms				Protocol specifications			Local WSCD/ StrongBox [49]		
Name [23]	Type			Primitives [23]	JOSE [23]	COSE [27]	SOG-IS [20]	Knox [60]	Titan [58]	S3K250AF [61]
PS256	Signature	RSA	PSS PKCS#1v2.1	SHA-256/ MGF1	O	R	R with≥3000 bits	✓-	✓-	✓-
PS384				SHA-384/ MGF1				×	×	×
PS512				SHA-512/ MGF1						
RS256			PKCS1-v1_5	SHA-256	R	NR	L	✓-	✓-	✓-
RS384				SHA-384	O			✓	×	×
RS512				SHA-512	O					
ESP256		ECDSA		P-256/ SHA-256	R+	R	R	✓	✓	×
ESP384				P-384/ SHA-384	O			×	×	
ESP512				P-512/ SHA-512	O					
-				BrainpoolP256r1/ SHA-256	NA	NR	R			
-				BrainpoolP384r1/ SHA-384						
-				BrainpoolP512r1/ SHA-512						
-				FRP256v1/ SHA-256		NA	R			
RSA-OAEP	Encryption	RSA	OAEP (PKCS#1v2.1)	SHA-1 (default)	R+	R	R	×	×	×
				SHA-256	NA	R				
				SHA-512	NA	R				
RSA-OAEP-256				SHA-256/ MGF1	O	NA				
RSA1_5			PKCS#1v1.5	-	R-	D	L			
A128CBC-HS256		AES	AES-CBC	HMAC-SHA-256	RQ	NA	R	✓	✓	✓
A192CBC-HS384				HMAC-SHA-384	O	NA	R	×	×	×
A256CBC-HS512				HMAC-SHA-512	RQ	NA	R	×	×	×
A128GCM			AES-GCM	-	R	NA	R	✓	✓	✓
A192GCM				-	O	NA	R	×	×	×
A256GCM				-	R	NA	R	✓	✓	×

R(+/-), recommended (strongly/less); *NR*, not recommended; *O*, optional; *RQ*, required; *L*, legacy; *D*, deprecated; *NA*, not available; ✓, supported; ✓-, supported only with 2048 bits; ×, not supported

Secure storage

Local external: Smart cards, FIDO Tokens

Smart cards qualify as a solution when they are CC certified to meet AVA_VAN.5 requirements.

- Italian CIE 3.0:
  - widespread adaption, but currently is read-only, making the chip's data immutable and rendering the card unsuitable for such integration.
- FIDO (Fast Identity Online) tokens:
  - password replacement with stronger biometric and cryptographic authentication methods.
  - under evaluation to obtain FIDO LoA 3+ certification, ensuring compliance with the eIDAS High LoA

Local External

- External hw components interacting with User's device

Secure storage

Remote: Hardware Security Module (HSM)

- HSMs qualify as a solution when they are CC certified to meet AVA_VAN.5 requirements.
- Offline Support: Since remote HSMs inherently support online use, offering offline availability can be challenging.

Remote

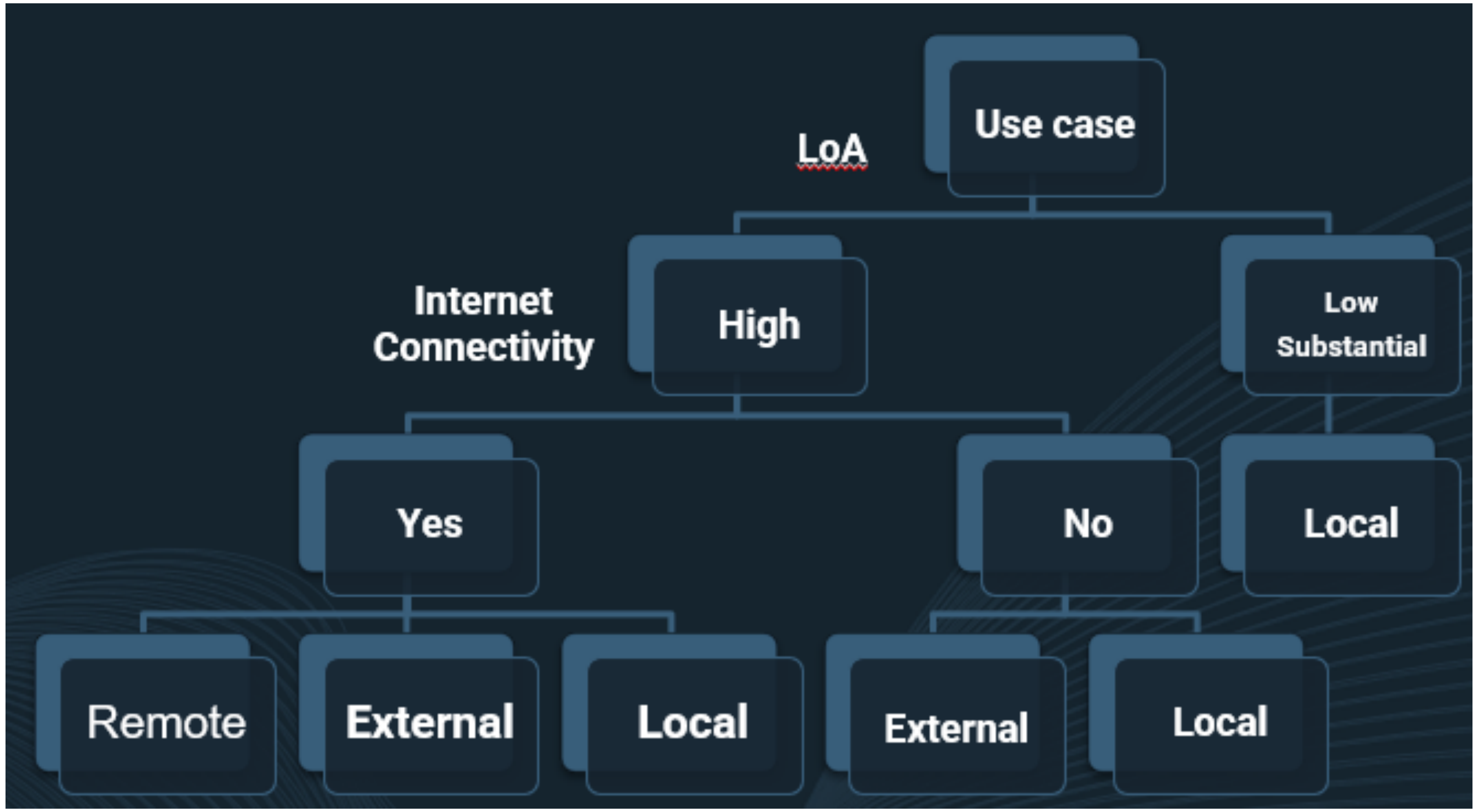
- situated remotely, separate from the user's device

Secure storage

Hybrid architecture

Integrating:

- **mobile secure storage** for use cases requiring **offline** access with **less stringent security** demands,
- **external HSMs** for **online** scenarios that necessitate **higher security**.



Balanced combination of **security** and **availability**, crucial for maintaining operational consistency and user assurance even in the face of connectivity constraints.

Digital identity wallet
Outline

EU
European Digital Identity Wallet
Obtain and present your documents
Enter

EUDI Wallet Overview

Evolution of the eIDAS ecosystem and our research activities

Trust Framework

Overview

Selective Disclosure and Revocation Mechanisms

Overview and comparison of different approaches

Secure elements

Overview and comparison

Threat Model and Risk Analysis for the Wallet Ecosystem

Discussion on overall security and privacy aspects of digital identity wallets

Digital identity wallet
Outline

EU
European Digital Identity Wallet
Obtain and present your documents
Enter

EUDI Wallet Overview

Evolution of the eIDAS ecosystem and our research activities

Trust Framework

Overview

Selective Disclosure and Revocation Mechanisms

Overview and comparison of different approaches

Secure elements

Overview and comparison

Threat Model and Risk Analysis for the Wallet Ecosystem

Discussion on overall security and privacy aspects of digital identity wallets

Conclusions

Research Challenges of the Digital Identity Wallet

EU
European Digital Identity Wallet
Obtain and share your documents
Enter

Trust Framework

Secure elements

Selective Disclosure and Revocation Mechanisms

Threat Model and Risk Analysis for the Wallet Ecosystem

...and many others..

- Research Opportunities (!)
  - Need of Crypto solutions and design of usable and secure protocols for digital wallet

Digital Identity Wallet
Our academic contributions

1. R. Germenia, S. Manfredi, G. Sciarretta, M. Scuro, A. Tomasi. **Comparison of Credential Status Mechanisms for the Digital Wallet Ecosystem**. In *Proceedings of the 39th Annual IFIP WG 11.3 Conference on Data and Applications Security and Privacy (DBSec 2025).*

2. Z. Ebadi Ansaroudi, G. Sciarretta, A. De Maria, S. Ranise. **Navigating Secure Storage Requirements for EUDI Wallets**. EURASIP Journal on Information Security, 2025.

3. A. Sharif, Z. Ebadi Ansaroudi, G. Sciarretta, D. Pöhn, M. Mollaeefar, W. Hommel, S. Ranise. **Protecting Digital Identity Wallet: A Threat Model in the Age of eIDAS 2.0**. In: 19th International Conference on Risks and Security of Internet and Systems (CRiSIS 2024).

4. A. Flamini, G. Sciarretta, M. Scuro, A. Sharif, A. Tomasi, S. Ranise. **On Cryptographic Mechanisms for the Selective Disclosure of Verifiable Credentials**. In: *Journal of Information Security and Applications (JISA)*, 2024.

5. A. Flamini, S. Ranise, G. Sciarretta, M. Scuro, A. Sharif, A. Tomasi. **A First Appraisal of Cryptographic Mechanisms for the Selective Disclosure of Verifiable Credentials**. In: *20th International Conference on Security and Cryptography (SECRYPT 2023).*

6. Z. E. Ansaroudi, R. Carbone, G. Sciarretta, and S. Ranise. **Control is Nothing Without Trust: A First Look into Digital Identity Wallet Trends**. In: *Proceedings of the 37th Annual IFIP WG 11.3 Conference on Data and Applications Security and Privacy (DBSec 2023).*

7. A. Sharif, M. Ranzi, R. Carbone, G. Sciarretta, S. Ranise. **SoK: A Survey on Technological Trends for (pre)Notified eIDAS Electronic Identity Schemes.** In: *17th International Workshop on Frontiers in Availability, Reliability and Security (FARES2022).*

8. A. Sharif, M. Ranzi, R. Carbone, G. Sciarretta, F. A. Marino, S. Ranise. **The eIDAS Regulation: A Survey of Technological Trends for European Electronic Identity Schemes.** In: *MDPI Journal of Applied Science (APPLSCI)*, 2022.

Roberto Carbone

carbone@fbk.eu

FONDAZIONE
BRUNO KESSLER

CENTER FOR
CYBERSECURITY

STRIDE – Secure and TRaceable Identities in Distributed Environments.

SERICS

SECURITY AND RIGHTS IN THE CYBERSPACE

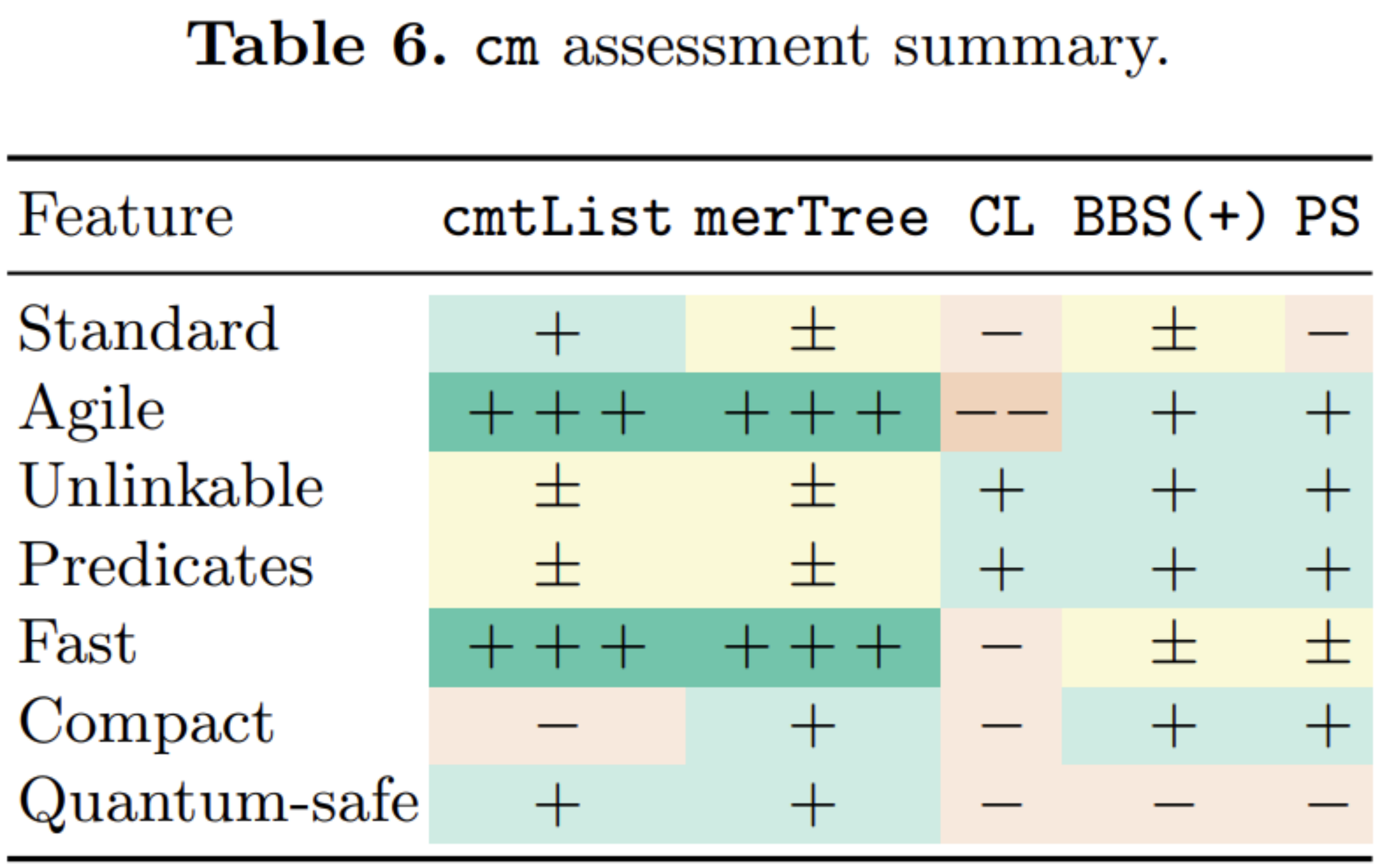


Table 6. `cm` assessment summary.

Feature	`cmtList`	`merTree`	`CL`	`BBS(+)`	`PS`
Standard	+	±	−	±	−
Agile	+ + +	+ + +	− −	+	+
Unlinkable	±	±	+	+	+
Predicates	±	±	+	+	+
Fast	+ + +	+ + +	−	±	±
Compact	−	+	−	+	+
Quantum-safe	+	+	−	−	−

Digital Id wallet: Trust and Functionalities

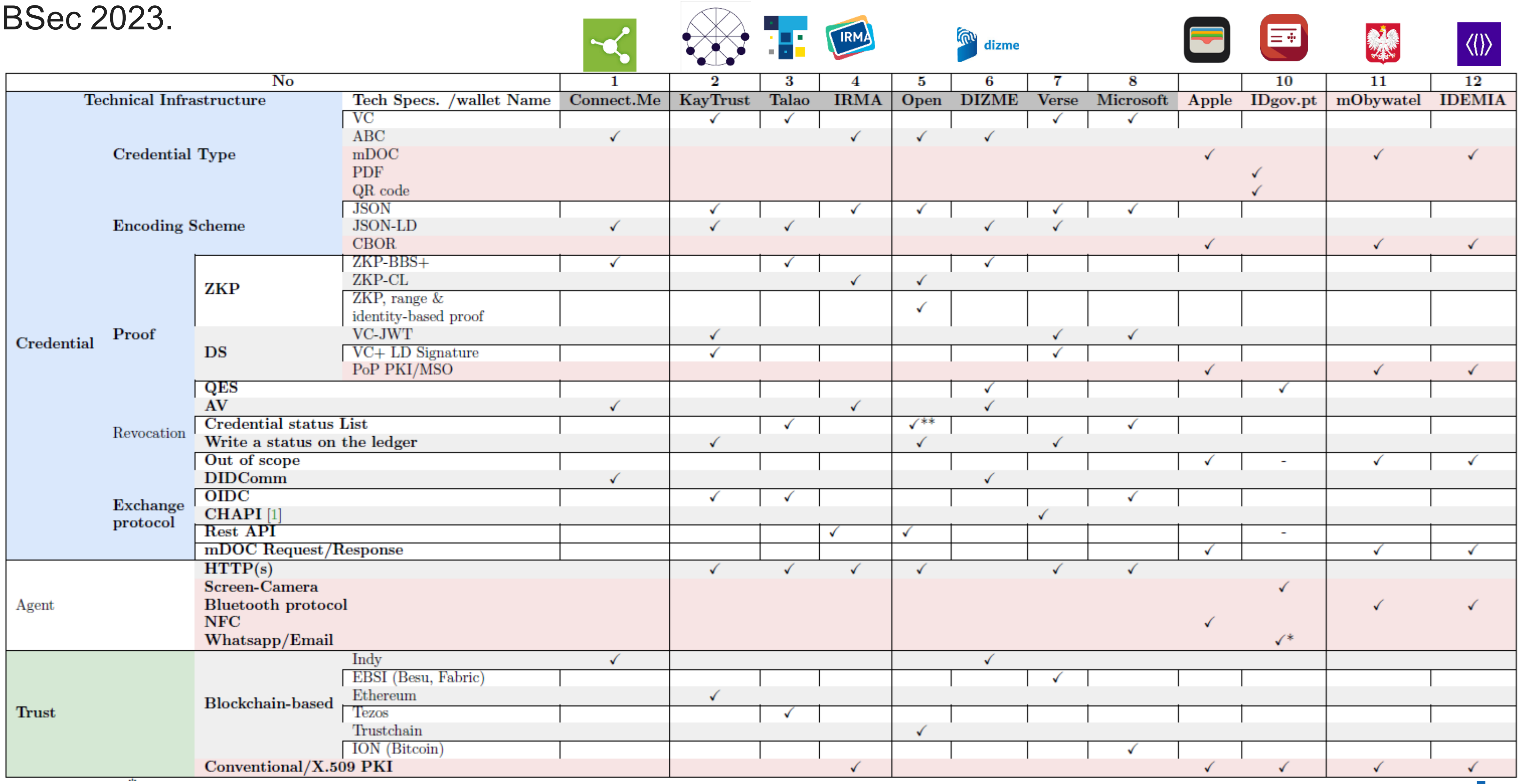
Amir Sharif, Roberto Carbone, Giada Sciarretta, Francesco Antonio Marino, Silvio Ranise. *PID Issuance for the eIDAS 2.0 Wallets: Do not throw the Baby with the Bathwater*. ITASEC, 2023.

Zahra Ebadi Ansaroudi, Roberto Carbone, Giada Sciarretta, and Silvio Ranise. *Control is Nothing Without Trust: A First Look into Digital Identity Wallet Trends*. DBSec 2023.

ITASEC 2023

RQ1: How is the trust established?

RQ2: How are credentials managed?



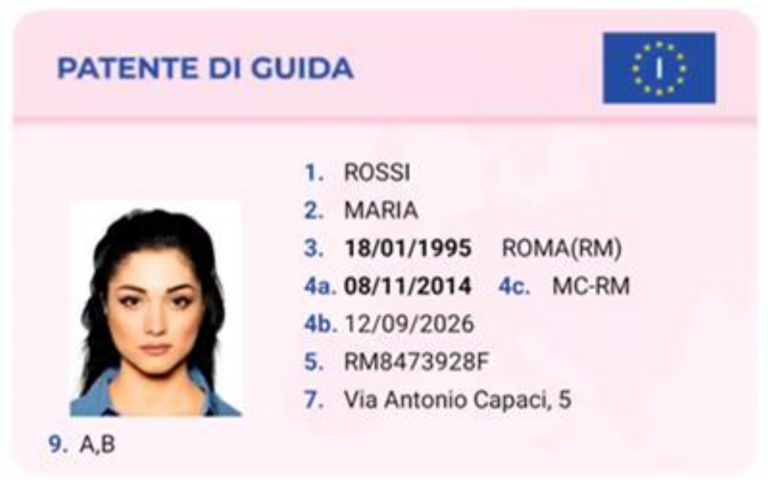
No				1	2	3	4	5	6	7	8		10	11	12
Technical Infrastructure			Tech Specs. /wallet Name	Connect.Me	KayTrust	Talao	IRMA	Open	DIZME	Verse	Microsoft	Apple	IDgov.pt	mObywatel	IDEMIA
Credential	Credential Type		VC		✓	✓				✓	✓				
			ABC	✓			✓	✓	✓						
			mDOC									✓		✓	✓
			PDF										✓		
			QR code										✓		
	Encoding Scheme		JSON		✓		✓	✓		✓	✓				
			JSON-LD	✓	✓	✓			✓	✓					
			CBOR									✓		✓	✓
	Proof	ZKP	ZKP-BBS+	✓		✓			✓						
			ZKP-CL				✓	✓							
			ZKP, range & identity-based proof					✓							
		DS	VC-JWT		✓					✓	✓				
			VC+ LD Signature		✓					✓					
			PoP PKI/MSO									✓		✓	✓
		QES							✓				✓		
		AV		✓			✓		✓						
	Revocation	Credential status List				✓		✓**			✓				
		Write a status on the ledger			✓			✓		✓					
		Out of scope										✓	-	✓	✓
	Exchange protocol	DIDComm		✓					✓						
		OIDC			✓	✓					✓				
		CHAPI [1]								✓					
		Rest API					✓	✓					-		
		mDOC Request/Response										✓		✓	✓
Agent		HTTP(s)			✓	✓	✓	✓		✓	✓				
		Screen-Camera											✓		
		Bluetooth protocol												✓	✓
		NFC										✓			
		Whatsapp/Email											✓*		
Trust		Blockchain-based	Indy	✓					✓						
			EBSI (Besu, Fabric)							✓					
			Ethereum		✓										
			Tezos			✓									
			Trustchain					✓							
			ION (Bitcoin)								✓				
		Conventional/X.509 PKI					✓					✓	✓	✓	✓

Digital Id wallet: Selective disclosure mechanisms

“The ability of a holder to make fine-grained decisions about what information to share.”

A. Flamini, G. Sciarretta, M. Scuro, A. Sharif, A. Tomasi, S. Ranise. *On Cryptographic Mechanisms for the Selective Disclosure of Verifiable Credentials*. Elsevier Journal of Information Security and Applications (JISA) 2024.

Andrea Flamini, Giada Sciarretta, Amir Sharif, Alessandro Tomasi, Silvio Ranise. *A First Appraisal of Cryptographic Mechanisms for the Selective Disclosure of Verifiable Credentials*. SECRYPT 2023.



PATENTE DI GUIDA

1. ROSSI
2. MARIA
3. **18/01/1995** ROMA(RM)
4a. **08/11/2014** 4c. MC-RM
4b. 12/09/2026
5. RM8473928F
7. Via Antonio Capaci, 5
9. A,B

Selective disclosure signature mechanims
e.g. for proof of age

18/01/1995