Keep It Secret, Keep It Safe — ZK-Proofs in the EU Identity Wallet

Olivier Blazy — Ecole Polytechnique

Future Cryptography 2026 — Estonian Academy of Sciences

Blazy Olivier

Professor @ Ecole Polytechnique

Olivier.blazy@polytechnique.edu

- Lead of the French C2 Work group from 2020-2024
- Author of the **HQC** NIST Standard for PQ-encryption
- Creator of the French PoC for Online Age Verification
- Expert for the French Delegation of the EUDIW
- Scientific Director of the CIEDS
- Academic Research on Cryptography, privacy protection, …

<- Website

Email ->

Why this is our problem

450 million citizens, one wallet model, every relying party in Europe

Identity primitives suddenly have to scale: pseudonymity, unlinkability, revocation

Get this wrong and we lock bad cryptography in for a decade, and lose citizens trust

Estonia has been here before: your e-ID story is now everyone’s

eIDAS 2.0: the road to a wallet

2014

eIDAS 1.0: qualified signatures, no wallet

Jun 2021

COM proposal for a European Digital Identity

May 2024

Reg. (EU) 2024/1183 enters into force

Nov 2024

ARF v1.4: first concrete cryptographic targets

By end of 2026

Each Member State must offer at least one wallet

EU DI Wallet

Three actors, one credential

Issuer: government, bank, university — signs an attestation

Holder: the citizen, with the wallet on a phone

Verifier: a relying party: airline, hotel, online shop

Trust:

verifier trusts issuer's signature

holder trusts the wallet to hide what isn't asked

Two privacy questions, not one

Privacy vs. the verifier: what can the relying party reconstruct after I show my credential?

Privacy vs. the issuer: what can the issuer learn about where, when, and to whom I presented?

The two are **independent**: a scheme can give one and silently break the other

Issuer-privacy is the hard one: the issuer is the state, and it never goes away

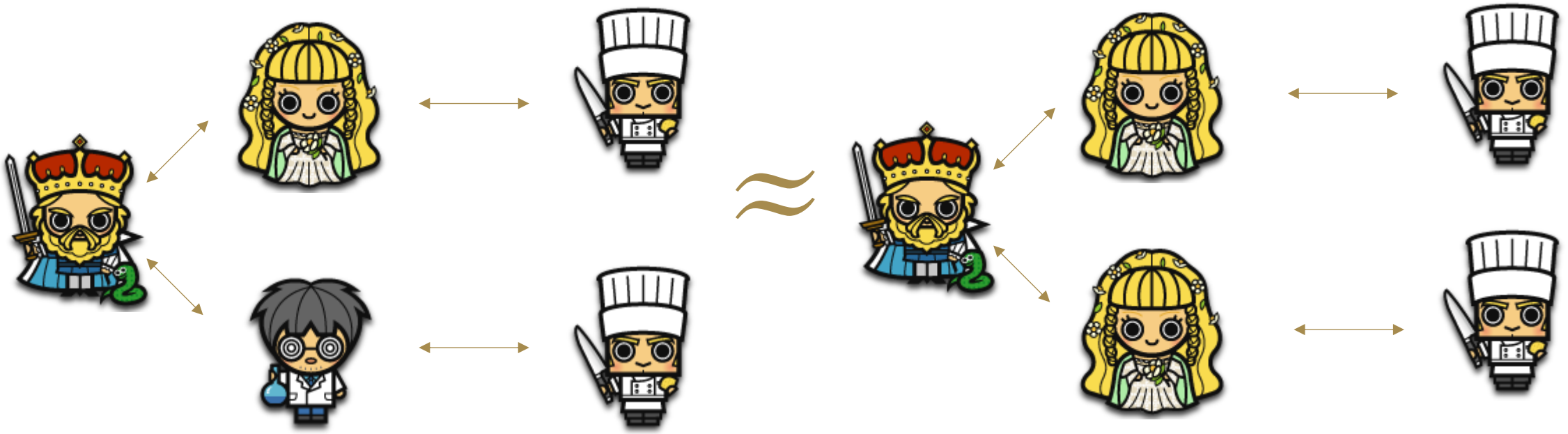
Every design choice in the wallet must be evaluated against both threat models

Privacy vs. the verifier

~~**Unlikeability**~~ **Unlinkability:** after seeing two credential presentations, no verifier should be able to infer whether they come from the same user

Privacy vs. the issuer

Unlinkability: after seeing two credentials it generated, the issuer should not be able to determine whether they come from the same user



Two credential formats, one wallet

SD-JWT VC

IETF draft, JSON-based

Salted-hash selective disclosure
Holder-binding via JWT key confirmation
Easiest path to web verifiers

mdoc / ISO 18013-5

Ratified ISO standard, CBOR-based

Mobile Security Object with hash digests
Optimised for proximity (Bluetooth / NFC)
Aligns with the mobile driving licence

The unlinkability problem

Two presentations of the same SD-JWT carry the same JWT signature

Two verifiers can **collude**: or one verifier across two visits
→ “Same wallet” is provable from the signature alone

mdoc has the same property: MSO is a stable, signed object
“Selective disclosure” ≠ “private”: this is where ZK enters

Why a stable issuer signature kills issuer-privacy

Two presentations of the same SD-JWT carry the same issuer signature σ

Scenario: Alice shows her credential at 09:14 at an airport, then at 14:02 at a pharmacy

If the issuer ever sees the presentations *through a revocation check, an audit log, or a court order* it sees the same σ both times

No collusion between verifiers required: the issuer alone correlates the two visits

The stable signature is an identifier across the issuer's view of the world too

This is what BBS **removes**: every presentation is a **fresh**, **re-randomised** σ' that even the signer cannot recognise

Batch issuance: the tempting shortcut

Idea: issue N one-shot credentials at once; the holder uses each only once

Easy to deploy: reuses existing SD-JWT / mdoc machinery, no new crypto primitives

Gives a wallet-level "**unlinkability**" at presentation time: each token looks fresh

Many real deployments are heading this way: it ships fast, it demos well

Worth taking seriously before we explain why it is a dead-end

Why batch issuance is a **bad** first solution

Issuer-privacy is GONE: the issuer can predict every future presentation

Tokens are not bound to a verifier: a relying party can reuse, pool, or trade them across users

Refill problem: when the holder runs out, they contact the issuer again (issuer learns presentation patterns)

Cryptographic **dead-end**: once shipped, migrating to BBS or anon-creds is politically very hard

Easy to deploy, easy to regret: exactly the lock-in we should avoid for 10+ years

Zero-knowledge proofs

Goal: convince a **verifier** that a statement is true (without revealing why)

Three properties: **completeness** (true statements convince), **soundness** (false ones don't), **zero-knowledge** (proof reveals nothing else)

Examples: "I know x such that H(x) = y", "I am over 18", "I hold a valid issuer signature"

Non-interactive via Fiat–Shamir: a single message replaces a multi-round protocol

Concrete schemes: Σ-protocols, Bulletproofs, Groth16, Plonk, Halo2, STARKs: different cost / setup trade-offs

How ZK fits the EU Identity Wallet

Anonymous credentials: prove “I hold a valid issuer signature” without revealing it: restores verifier- and issuer-**unlinkability**

Selective disclosure with **unlinkability**: everything hash-SD does, plus **no stable identifier**

Predicate proofs: “over 18”, “EU resident”, “earns under €X” without disclosure

Membership / revocation: prove “I am not on the revocation list”

Composability: chain proofs into complex policies without re-issuing

BBS signatures, briefly

Pairing-based signature on a list (m_1, …, m_n) of messages

Standardised by IRTF: “BBS over BLS12-381”
Verification: two pairings
Signing: one exponentiation per message

Killer feature: prover can derive a randomised proof-of-knowledge of σ
Selective disclosure becomes a **free** corollary

More flexibility is better for adoption

Locking into a single verification circuit narrows the set of supported use cases

ZK-proofs enable complex policies, e.g.:

lives in Paris surburbs AND (under 18 **OR** (between 16 and 25 **AND** Studying) **OR** (more than 62 **AND** Retired) **OR** civil servant **OR** social worker **OR** welfare recipient (**in** {RSA,ASS,CSS,AME, AAH,AEEH}) **OR** welfare card holder (**in** {CI, CMI}) **OR** Veteran **OR** Travel Pass holder (**in** {Imagine R, Améthyste, TST, Navigo Senior}) **OR** member of car-pooling service (**in** {Citiz, Clem', Communauto}))

(*simplified* Veligo (Parisian bike rental) reduction rules)

Policies should be expressive, and adaptable to any use case on the fly, without re-issuance or heavy recomputations.

Framing proofs around "positive" use cases (discounts, eligibility) also helps public acceptance.

Take-aways

01

SD ≠ private

Batch issuance ≠ private

02

BBS is the bet

03

Predicates are the next frontier

04

PQ is wide open

05

Revocation needs ZK too

06

Crypto won't fix law


Merci
ÉCOLE POLYTECHNIQUE
INSTITUT POLYTECHNIQUE DE PARIS