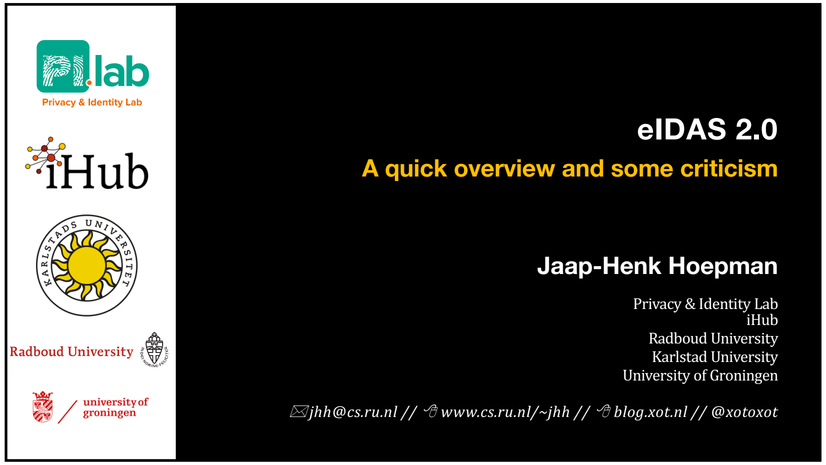

Privacy & Identity Lab
iHub
Radboud University
university of groningen

eIDAS 2.0

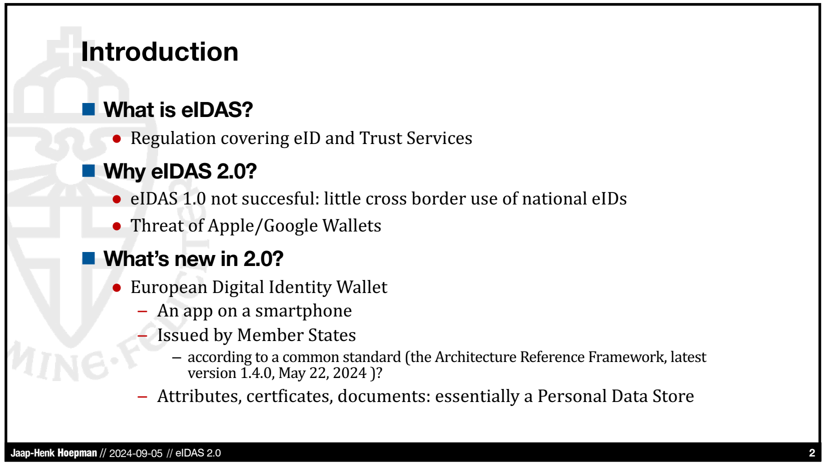
A quick overview and some criticism

Jaap-Henk Hoepman

Privacy & Identity Lab
iHub
Radboud University
Karlstad University
University of Groningen

✉jhh@cs.ru.nl // www.cs.ru.nl/~jhh // blog.xot.nl // @xotoxot

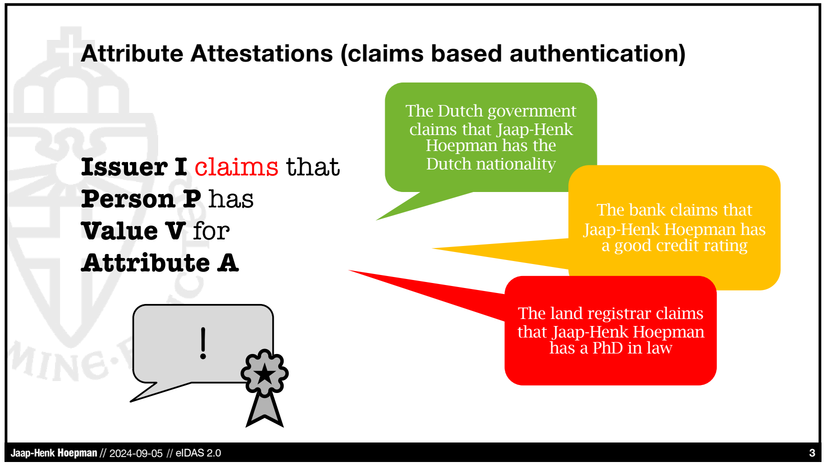
1



Introduction

- **What is eIDAS?**
  - Regulation covering eID and Trust Services
- **Why eIDAS 2.0?**
  - eIDAS 1.0 not succesful: little cross border use of national eIDs
  - Threat of Apple/Google Wallets
- **What's new in 2.0?**
  - European Digital Identity Wallet
    - An app on a smartphone
    - Issued by Member States
      - according to a common standard (the Architecture Reference Framework, latest version 1.4.0, May 22, 2024)?
    - Attributes, certficates, documents: essentially a Personal Data Store

2

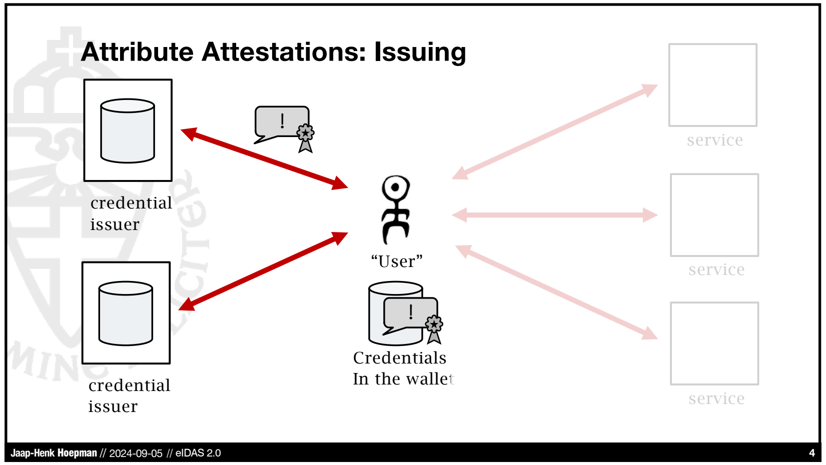


Attribute Attestations (claims based authentication)

Issuer I claims that
Person P has
Value V for
Attribute A

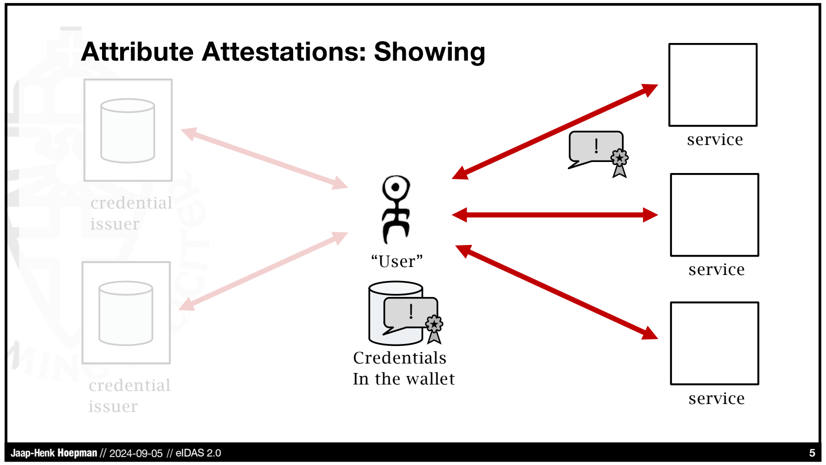
The Dutch government claims that Jaap-Henk Hoepman has the Dutch nationality
The bank claims that Jaap-Henk Hoepman has a good credit rating
The land registrar claims that Jaap-Henk Hoepman has a PhD in law
!

3



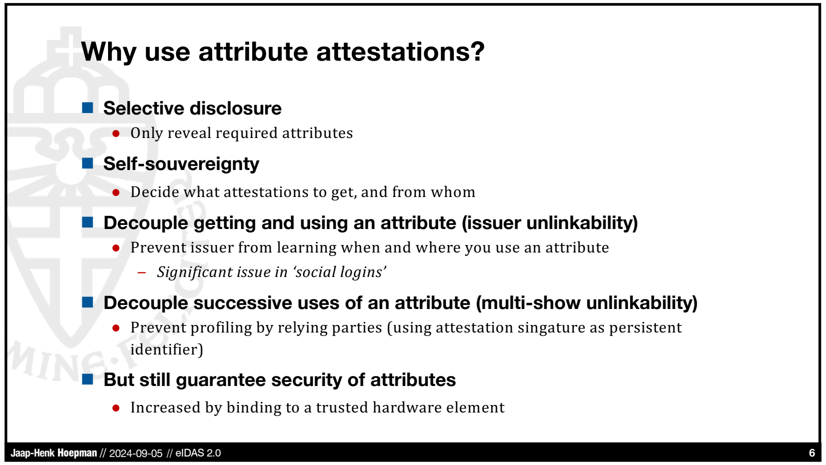
Attribute Attestations: Issuing

4



Attribute Attestations: Showing

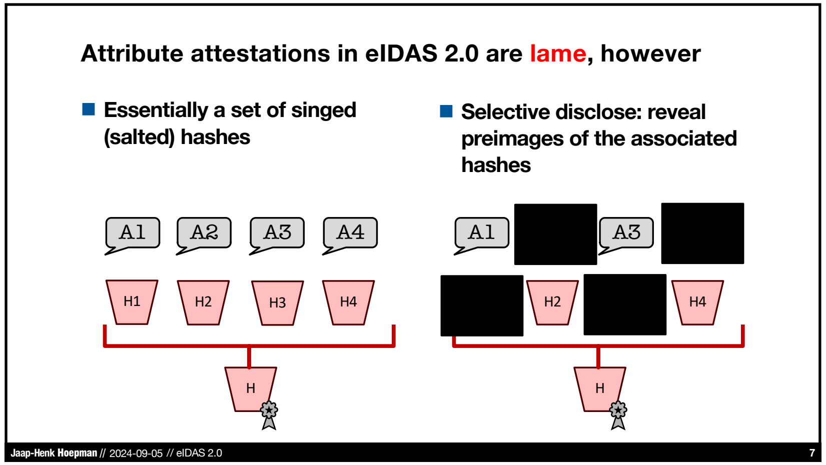
5



Why use attribute attestations?

- **Selective disclosure**
  - Only reveal required attributes
- **Self-souvereignty**
  - Decide what attestations to get, and from whom
- **Decouple getting and using an attribute (issuer unlinkability)**
  - Prevent issuer from learning when and where you use an attribute
    - *Significant issue in 'social logins'*
- **Decouple successive uses of an attribute (multi-show unlinkability)**
  - Prevent profiling by relying parties (using attestation singature as persistent identifier)
- **But still guarantee security of attributes**
  - Increased by binding to a trusted hardware element

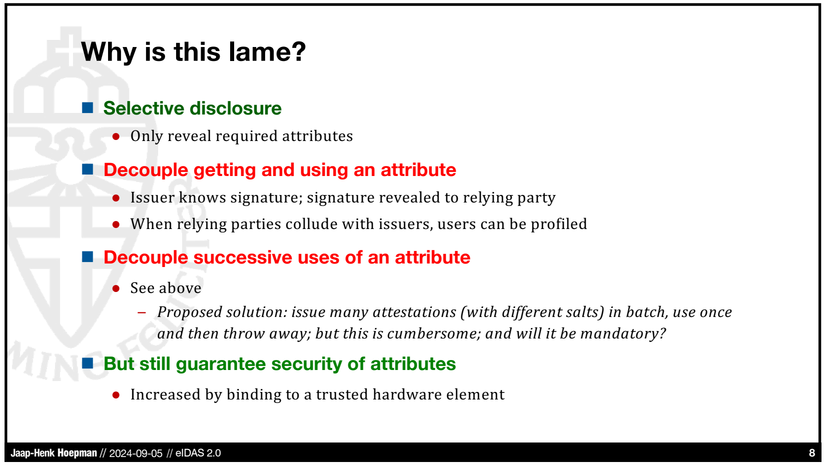
6



Attribute attestations in eIDAS 2.0 are lame, however

- **Essentially a set of singed (salted) hashes**
- **Selective disclose: reveal preimages of the associated hashes**

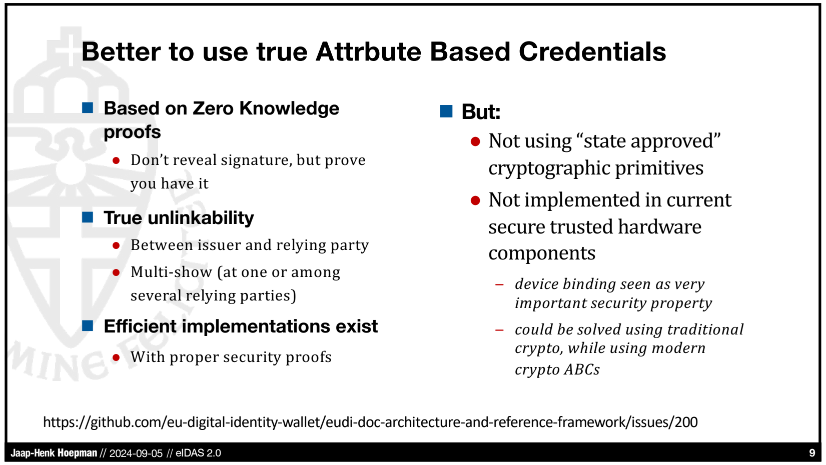
7



Why is this lame?

- **Selective disclosure**
  - Only reveal required attributes
- **Decouple getting and using an attribute**
  - Issuer knows signature; signature revealed to relying party
  - When relying parties collude with issuers, users can be profiled
- **Decouple successive uses of an attribute**
  - See above
    - *Proposed solution: issue many attestations (with different salts) in batch, use once and then throw away; but this is cumbersome; and will it be mandatory?*
- **But still guarantee security of attributes**
  - Increased by binding to a trusted hardware element

8

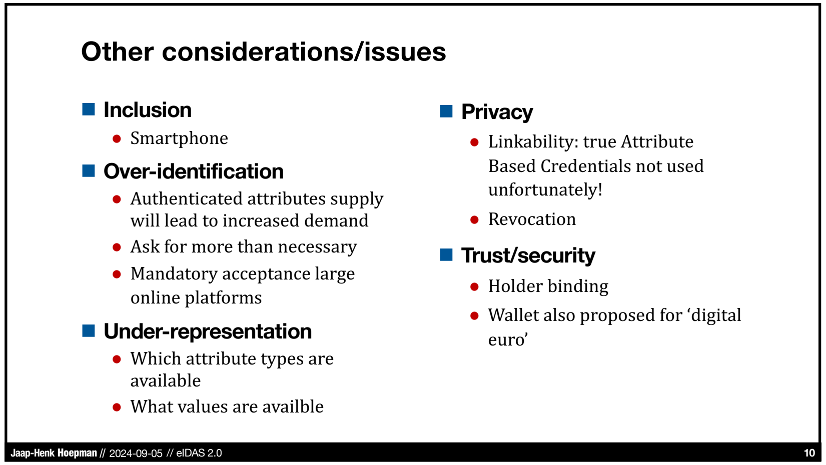


Better to use true Attrbute Based Credentials

- **Based on Zero Knowledge proofs**
  - Don't reveal signature, but prove you have it
- **True unlinkability**
  - Between issuer and relying party
  - Multi-show (at one or among several relying parties)
- **Efficient implementations exist**
  - With proper security proofs
- **But:**
  - Not using "state approved" cryptographic primitives
  - Not implemented in current secure trusted hardware components
    - *device binding seen as very important security property*
    - *could be solved using traditional crypto, while using modern crypto ABCs*

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

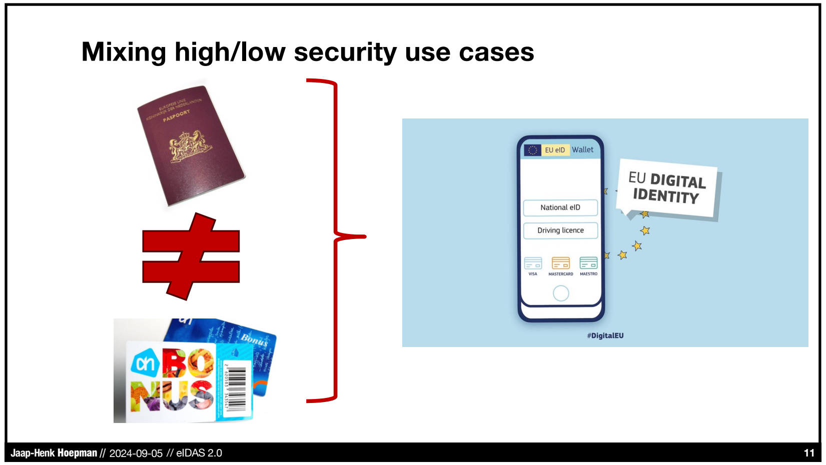
9



Other considerations/issues

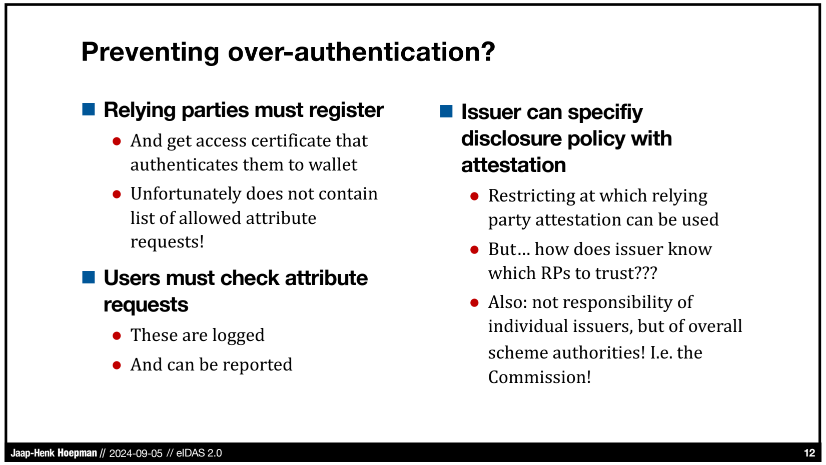
- **Inclusion**
  - Smartphone
- **Over-identification**
  - Authenticated attributes supply will lead to increased demand
  - Ask for more than necessary
  - Mandatory acceptance large online platforms
- **Under-representation**
  - Which attribute types are available
  - What values are availble
- **Privacy**
  - Linkability: true Attribute Based Credentials not used unfortunately!
  - Revocation
- **Trust/security**
  - Holder binding
  - Wallet also proposed for 'digital euro'

10



Mixing high/low security use cases

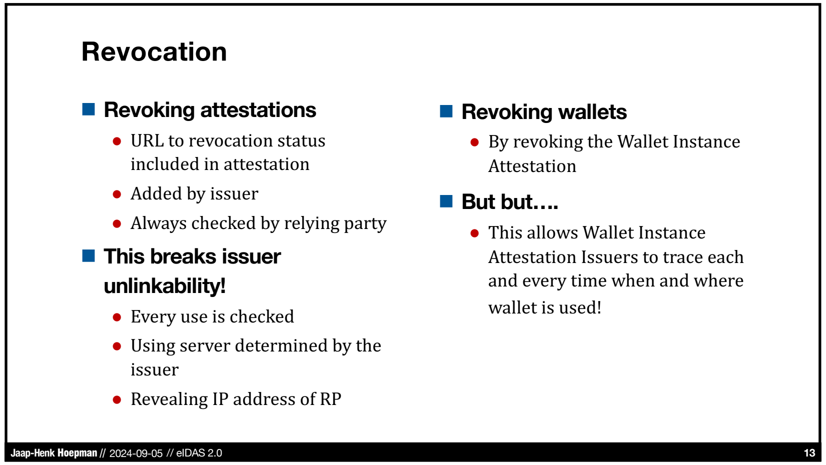
11



Preventing over-authentication?

- **Relying parties must register**
  - And get access certificate that authenticates them to wallet
  - Unfortunately does not contain list of allowed attribute requests!
- **Users must check attribute requests**
  - These are logged
  - And can be reported
- **Issuer can specifiy disclosure policy with attestation**
  - Restricting at which relying party attestation can be used
  - But… how does issuer know which RPs to trust???
  - Also: not responsibility of individual issuers, but of overall scheme authorities! I.e. the Commission!

12

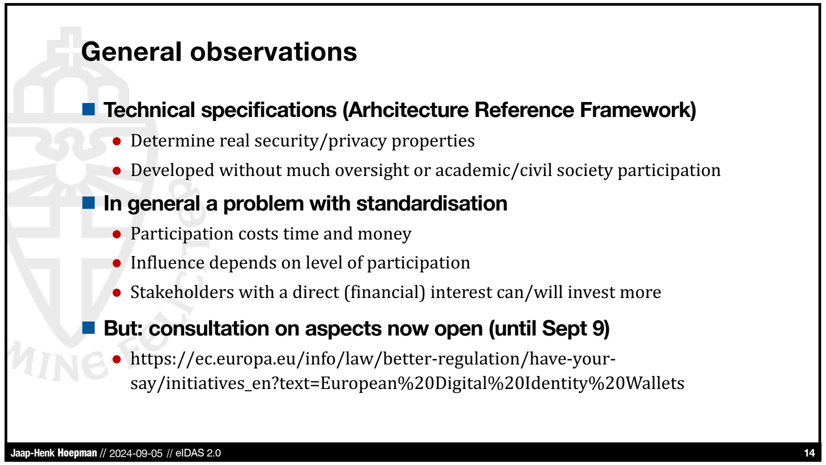


Revocation

- **Revoking attestations**
  - URL to revocation status included in attestation
  - Added by issuer
  - Always checked by relying party
- **This breaks issuer unlinkability!**
  - Every use is checked
  - Using server determined by the issuer
  - Revealing IP address of RP
- **Revoking wallets**
  - By revoking the Wallet Instance Attestation
- **But but….**
  - This allows Wallet Instance Attestation Issuers to trace each and every time when and where wallet is used!

Jaap-Henk Hoepman // 2024-09-05 // eIDAS 2.0 13

13

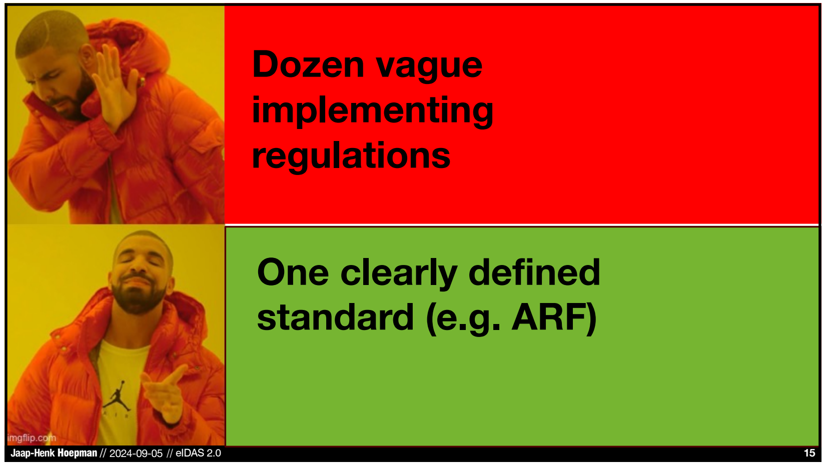


General observations

- **Technical specifications (Arhcitecture Reference Framework)**
  - Determine real security/privacy properties
  - Developed without much oversight or academic/civil society participation
- **In general a problem with standardisation**
  - Participation costs time and money
  - Influence depends on level of participation
  - Stakeholders with a direct (financial) interest can/will invest more
- **But: consultation on aspects now open (until Sept 9)**
  - https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives_en?text=European%20Digital%20Identity%20Wallets

Jaap-Henk Hoepman // 2024-09-05 // eIDAS 2.0 14

14



Dozen vague implementing regulations

One clearly defined standard (e.g. ARF)

Jaap-Henk Hoepman // 2024-09-05 // eIDAS 2.0 15

15

Questions?

[Monty Python's Argument Clinic sketch]

Jaap-Henk Hoepman // 2024-09-05 // eIDAS 2.0 16

16