Perspectief op cryptografie voor wallets

Subtitle

Jaap-Henk Hoepman

iHub / Radboud University
Karlstad University

✉ jhh@cs.ru.nl // www.cs.ru.nl/~jhh // @xotoxot.bsky.social
// @xot@someone.elses.computer/

1

Context: eIDAS 2.0, identity wallets

- **Wat is eIDAS?**
  - Verordening aangaande eID en Trust Services
- **Waarom een versie 2.0?**
  - eIDAS 1.0 niet succesvol: weinig transnational gebruik
  - Dreiging van Apple/Google Wallets
- **Wat is er nieuw in 2.0?**
  - European Digital Identity Wallet
    - App op a smartphone
    - Uitgegeven door lidstaten
      - Gezamelijke standaard (de Architecture Reference Framework / ARF)
    - Attributes, certficates, documents: zeg maar een Personal Data Store

EUROPEAN COMMISSION

Brussels, 3.6.2021
COM(2021) 281 final

2021/0136 (COD)

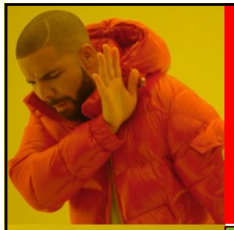
Proposal for a

REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL

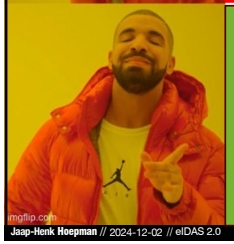
amending Regulation (EU) No 910/2014 as regards establishing a framework for a European Digital Identity

{SEC(2021) 228 final} - {SWD(2021) 124 final} - {SWD(2021) 125 final}

2



Allemaal vage “implementing acts”

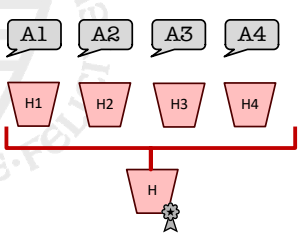


Één duidelijke standaard, opgesteld met *alle* betrokkenen

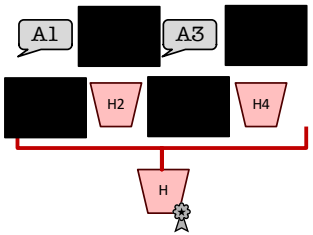
3

Attribute attestations in eIDAS 2.0 zijn lame

- **Eigenlijk een verzameling signed (salted) hashes**



- **Selective disclosure: maak preimages van de hashes openbaar**



4

Waarom is dit lame?

- **Selective disclosure**
- **Issuer unlinkability**
- **Multi show unlinkability**
  - Voorgestelde “oplossing”: geef meerdere attestaties tegelijk uit die ieder één keer gebruikt worden.
- **Betrouwbaarheid van de attributen**

5

Oplossing

- **EUID wallets zouden echte Anonymous / Attribute Based Credentials moeten gebruiken**
  - BBS+ / CL (Idemix/Yivi)
  - Issuer unlinkability
  - Multi-show unlinkabilityx

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 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 realised 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 credential mechanism fall short of the privacy requirements that were explicitly defined after extensive 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 do not see a way to fix the proposed solution to meet all the privacy features as required by the regulation; we believe that a larger redesign is in order.

In this document, we propose to use a different cryptographic mechanism instead; namely, *anonymous credentials*. Anonymous credentials were designed specifically to achieve authentication and identification that are both secure and privacy-preserving. As a result, they fully meet the requirements put forth in the eIDAS 2.0 regulation. Moreover, they are by now a mature technology. This technology was developed more than twenty years ago, and extensive efforts have been expended to analyze, improve, implement, standardize, test, and deploy it. Anonymous credentials are well understood by the scientific community.

Our specific recommendation is to use the BBS family of anonymous credentials. For BBS, thanks to prior work by the W3C, the Decentralized Identity Foundation, IETF/IRTF, ISO, and other standardization

*Writing as an individual and speaking for himself.

1

6

Echter

- **ABCs gebruiken moderne cryptografie**
  - BBS+ of CL
  - Hebben security bewijzen
  - Maar (nog) niet gestandaardiseerd
  - En niet op de SOGIS lijst van goedgekeurde cryptografische algoritmen
- **(Daarom) geen trusted hardware support**
  - En dat maakt device binding lastig

7

Device binding ‘hack’

- **Gebruik een echt (BBS+ / CL) credential**
- **TE bevat standaard ECDSA private key k**
  - Elk credential bevat de bijbehorende public key K
  - Issuer controleert dit!
- **Showing protocol**
  - Normaal: ZK bewijs $\{\alpha_1, \dots, \alpha_h | C(\alpha_1, \dots, \alpha_h, a_1, \dots, a_r)\}$
  - ECDSA handtekening $\sigma = sign(k, c)$ over challenge c met private key k in TE:
  - Nu: ZK bewijs $\{\alpha_1, \dots, \alpha_h, \sigma | C(\alpha_1, \dots, \alpha_h, a_1, \dots, a_r) \wedge K = \alpha_i \wedge verify(K, \sigma, c)\}$
- **Vergelijkbaar met device binding in ARF**
  - Attestation bevat public key
  - Wallet Secure Cryptographic Device (WSCD; lokaal of remote SE) bevat de private key
  - Wallet moet challenge tekenen
- **Geen ZKP, dus wallet linkbaar via public key**

8

Onlinkbaarheid?

- **Binnen huidige ARF met mdoc / SD-JWT attrbute attestations**
  - Batch uitgifte van sinlge-use attestations
  - Is dat schaalbaar?
  - Nog steeds issuer linkability
- **Gebruik ZK bewijzen**
  - Kan ook over standaard signature schemes (zoals ECDSA)
- **Stap over op BBS+ / CL**
  - Versnel standaardisatie
  - Moedig TE implementaties aan
-

9

Revocation

- **Op basis van Wallet Unit Attestation**
  - Of <24 uur geldig
  - Of bevat revocation information
- **Revocation information**
  - Bepaald door issuer
  - URL naar lijst van revoked attestations
  - Index in deze lijst
- **Deze index maakt tracking van wallets mogelijk**
  - Door meerdere relying parties
  - Maar ook door issuer

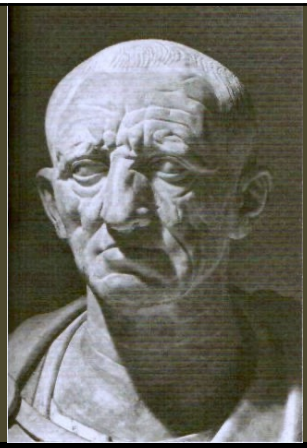
10

Discussie

[Monty Python's Argument Clinic sketch]

- **Migratiepad naar betere onlinkbaarheid?**
- **Holder binding?**

11



12