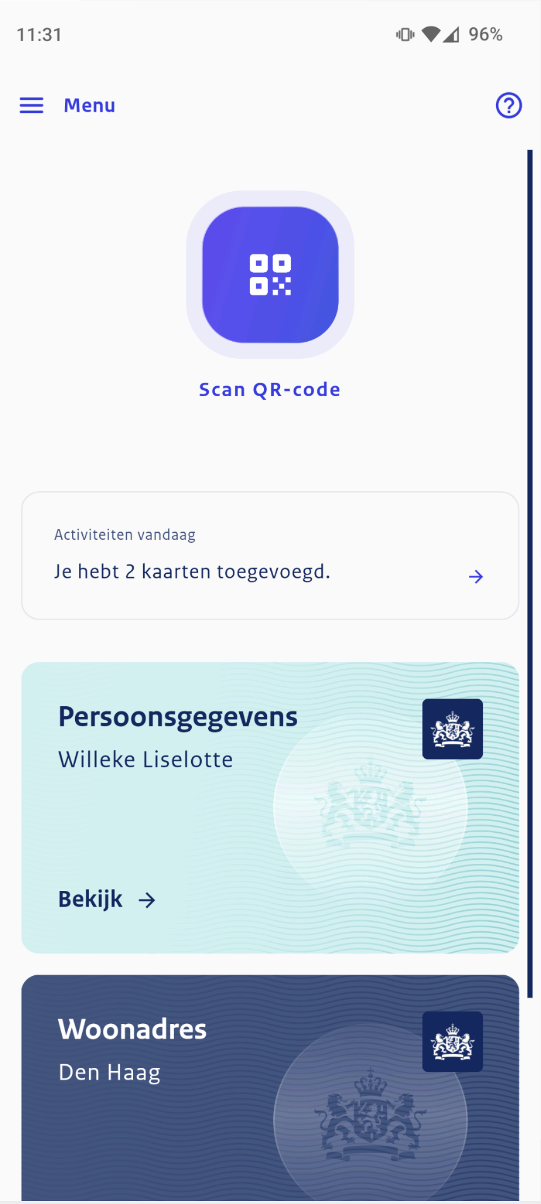
(Cryptografische) ontwikkelingen in EUDI wallets

Sietse Ringers

Yivi meeting
11 oktober 2024



11:31 96%

Activiteiten vandaag

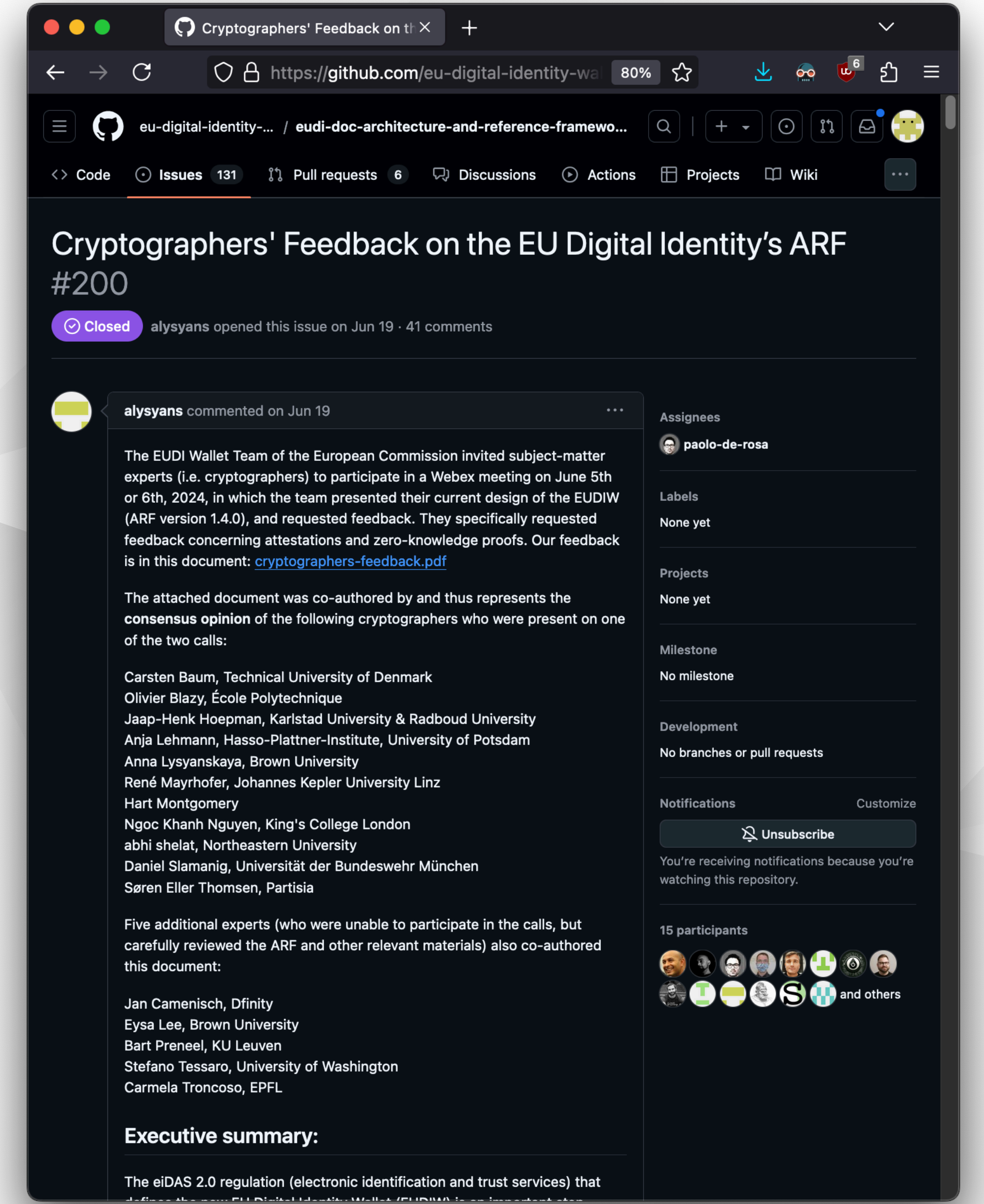
Je hebt 2 kaarten toegevoegd.

Persoonsgegevens

Willeke Liselotte

Woonadres

Den Haag


Cryptographers' Feedback on th
https://github.com/eu-digital-identity-wa
80%
eu-digital-identity-... / eudi-doc-architecture-and-reference-framewo...
Code
Issues 131
Pull requests 6
Discussions
Actions
Projects
Wiki

Cryptographers' Feedback on the EU Digital Identity's ARF #200

Closed alysyans opened this issue on Jun 19 · 41 comments

alysyans commented on Jun 19

The EUDI Wallet Team of the European Commission invited subject-matter experts (i.e. cryptographers) to participate in a Webex meeting on June 5th or 6th, 2024, in which the team presented their current design of the EUDIW (ARF version 1.4.0), and requested feedback. They specifically requested feedback concerning attestations and zero-knowledge proofs. Our feedback is in this document: cryptographers-feedback.pdf

The attached document was co-authored by and thus represents the **consensus opinion** of the following cryptographers who were present on one of the two calls:

Carsten Baum, Technical University of Denmark
Olivier Blazy, École Polytechnique
Jaap-Henk Hoepman, Karlstad University & Radboud 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
abhi shelat, Northeastern University
Daniel Slamanig, Universität der Bundeswehr München
Søren Eller Thomsen, Partisia

Five additional experts (who were unable to participate in the calls, but carefully reviewed the ARF and other relevant materials) also co-authored this document:

Jan Camenisch, Dfinity
Eysa Lee, Brown University
Bart Preneel, KU Leuven
Stefano Tessaro, University of Washington
Carmela Troncoso, EPFL

Executive summary:

The eiDAS 2.0 regulation (electronic identification and trust services) that

Assignees
paolo-de-rosa

Labels
None yet

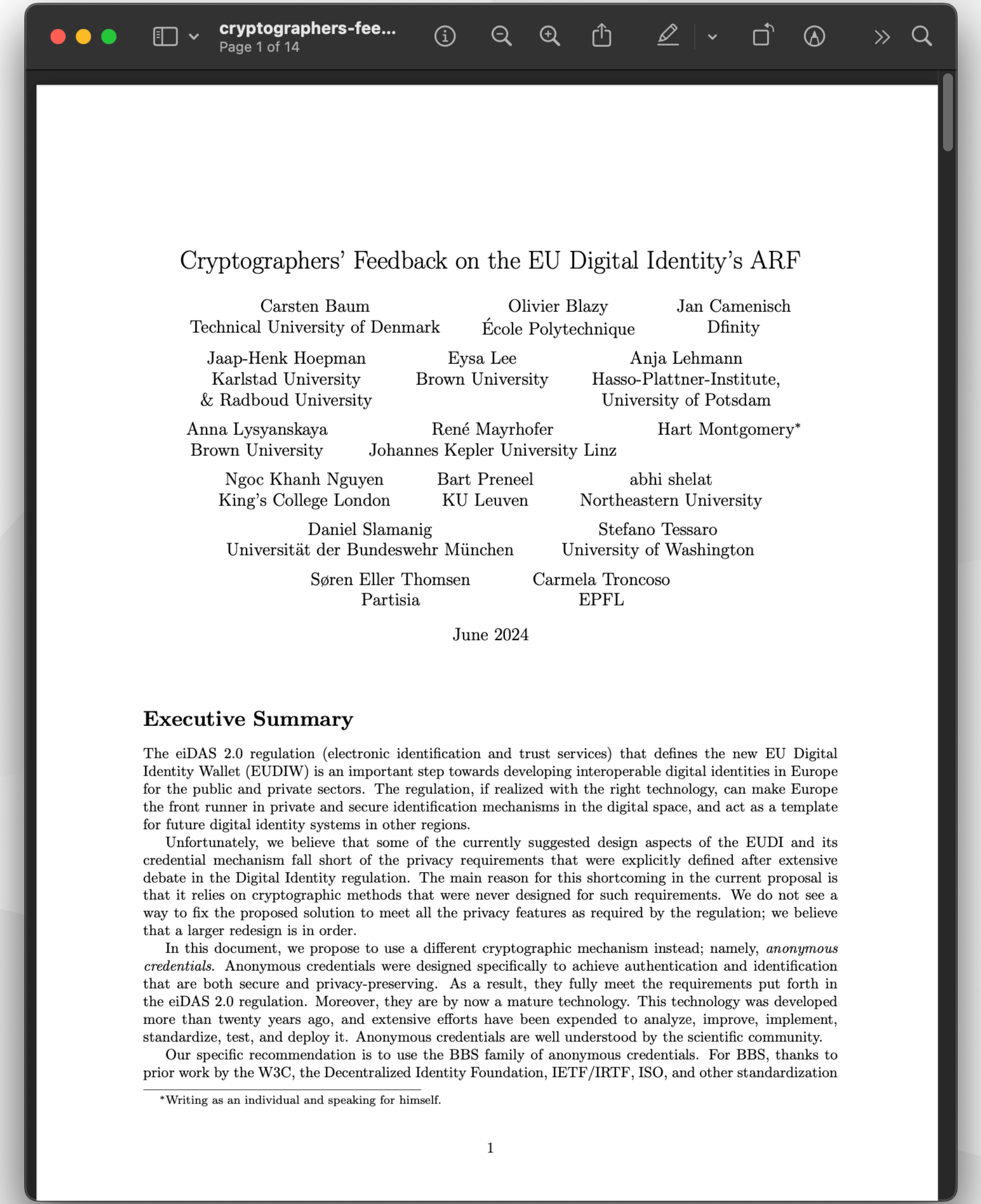
Projects
None yet

Milestone
No milestone

Development
No branches or pull requests

Notifications Customize
Unsubscribe
You're receiving notifications because you're watching this repository.

15 participants
and others



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 realized 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.

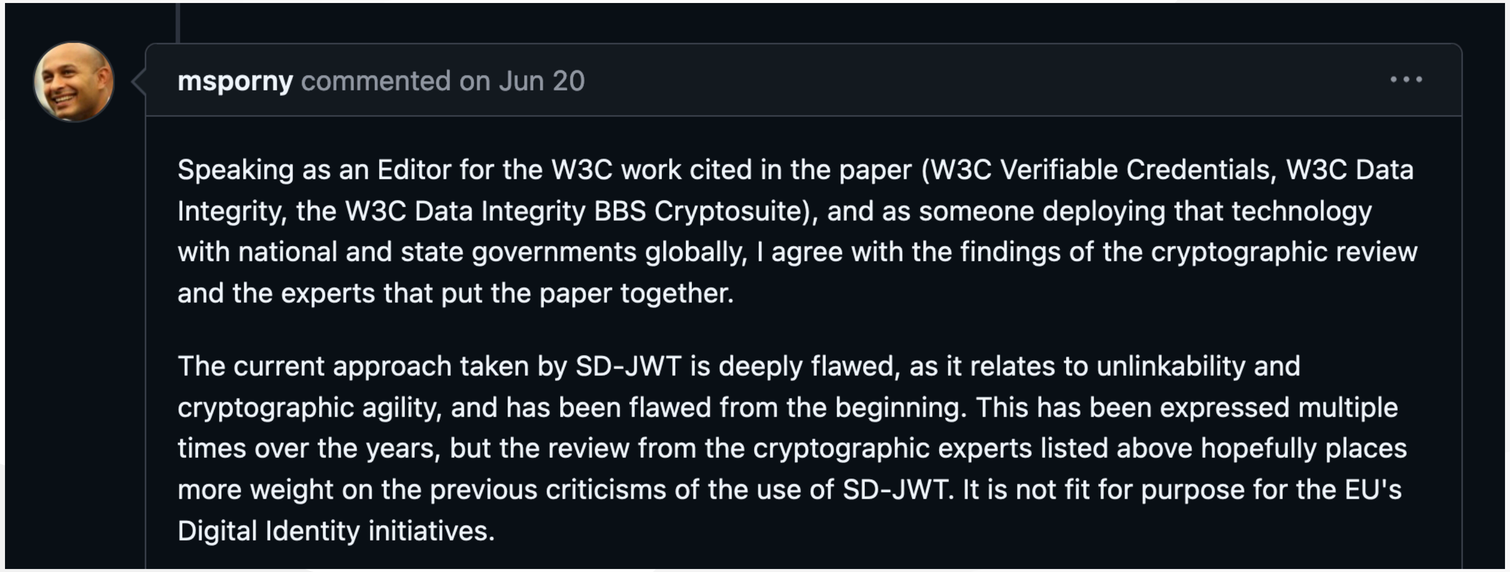
Unfortunately, we believe that some of the currently suggested design aspects of the EUDI and its credential mechanism fall short of the privacy requirements that were explicitly defined after extensive debate in the Digital Identity regulation. The main reason for this shortcoming in the current proposal 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.

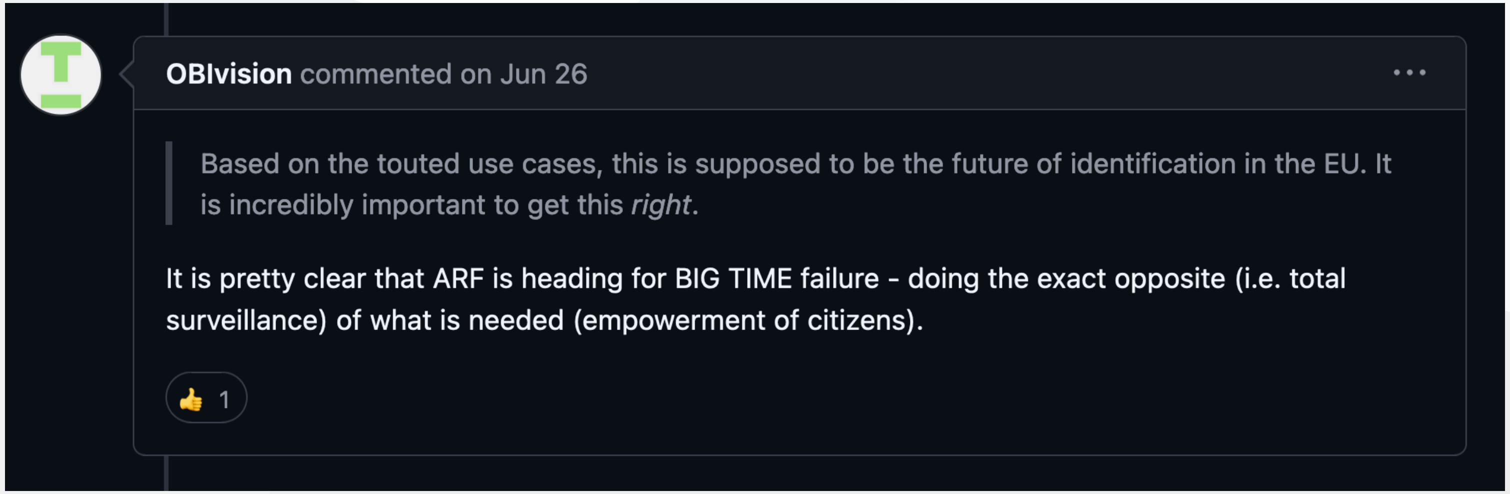
Github comments



msporny commented on Jun 20

Speaking as an Editor for the W3C work cited in the paper (W3C Verifiable Credentials, W3C Data Integrity, the W3C Data Integrity BBS Cryptosuite), and as someone deploying that technology with national and state governments globally, I agree with the findings of the cryptographic review and the experts that put the paper together.

The current approach taken by SD-JWT is deeply flawed, as it relates to unlinkability and cryptographic agility, and has been flawed from the beginning. This has been expressed multiple times over the years, but the review from the cryptographic experts listed above hopefully places more weight on the previous criticisms of the use of SD-JWT. It is not fit for purpose for the EU's Digital Identity initiatives.



OBIvision commented on Jun 26

> Based on the touted use cases, this is supposed to be the future of identification in the EU. It is incredibly important to get this *right*.

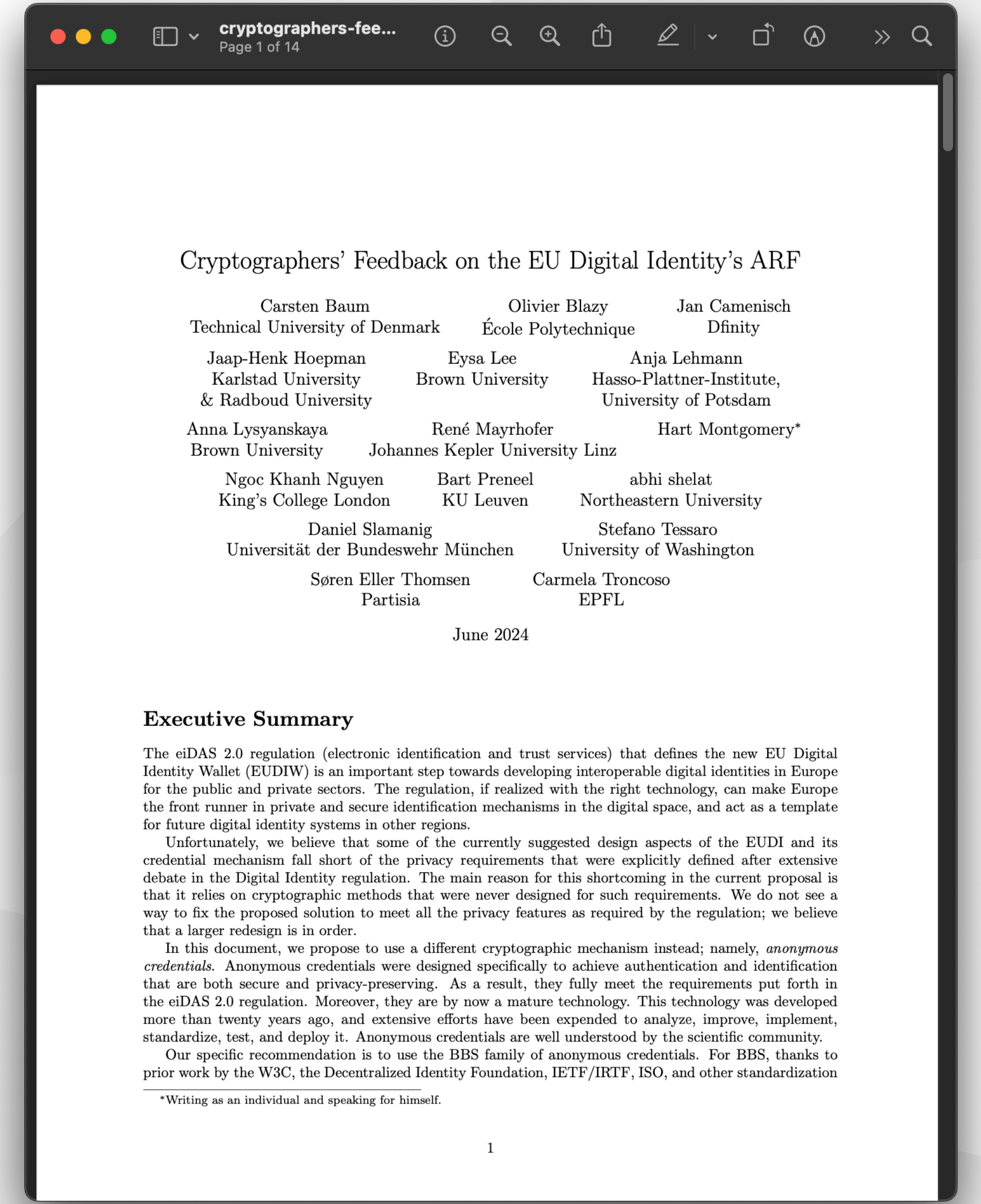
It is pretty clear that ARF is heading for BIG TIME failure - doing the exact opposite (i.e. total surveillance) of what is needed (empowerment of citizens).

👍 1

TL;DR

EUDI wallets en de ARF zouden *anonymous credentials* moeten gebruiken

- BBS+, Idemix (Yivi)
- Multishow unlinkability
- Issuer unlinkability



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

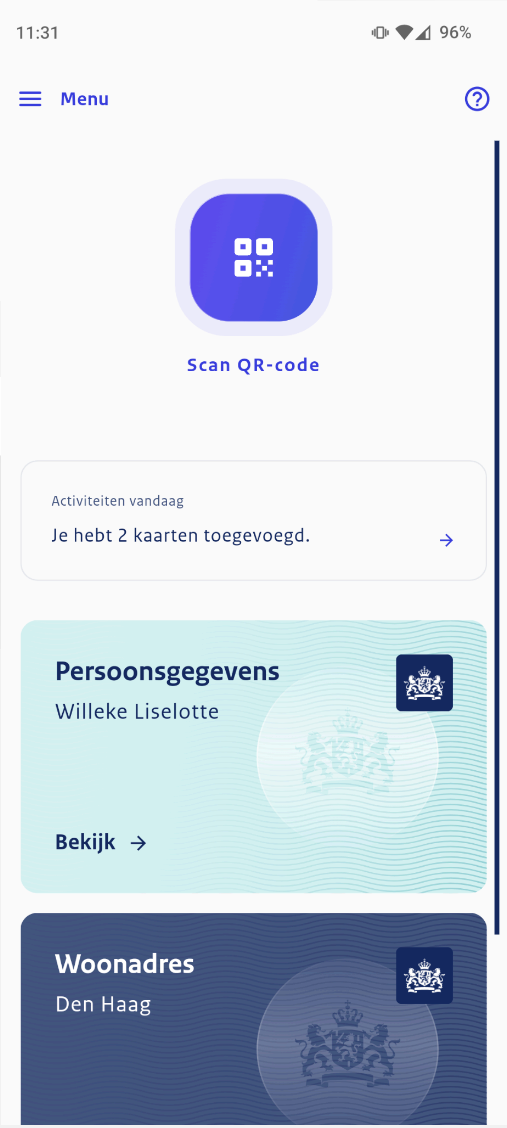
The eiDAS 2.0 regulation (electronic identification and trust services) that defines the new EU Digital Identity Wallet (EUDIW) is an important step towards developing interoperable digital identities in Europe for the public and private sectors. The regulation, if realized with the right technology, 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.



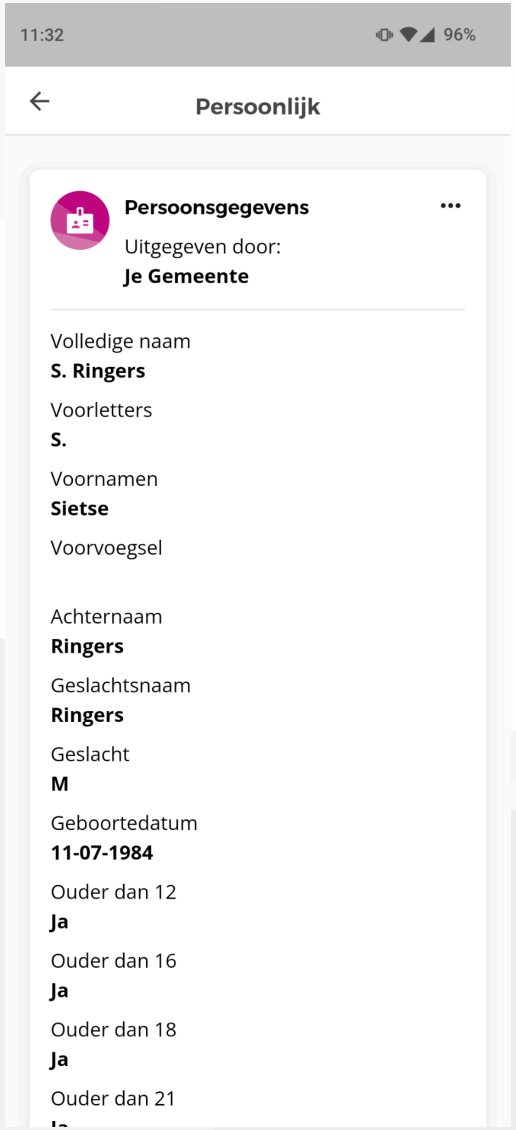
Activiteiten vandaag

Je hebt 2 kaarten toegevoegd.

Persoonsgegevens
Willeke Liselotte

Bekijk →

Woonadres
Den Haag



Persoonsgegevens
Uitgegeven door:
Je Gemeente

Volledige naam
S. Ringers

Voorletters
S.

Voornamen
Sietse

Voorvoegsel

Achternaam
Ringers

Geslachtsnaam
Ringers

Geslacht
M

Geboortedatum
11-07-1984

Ouder dan 12
Ja

Ouder dan 16
Ja

Ouder dan 18
Ja

Ouder dan 21

Waar gaat het over?

De privacy-eigenschappen van ID wallets:

- Attribuut-gebaseerde authenticatie
  - Selective disclosure
- Decentraal
  - Geen issuer involvement bij disclosure
- ARF: leidend document in EUDI wallet design

Credentials: cryptografie

Twee varianten:

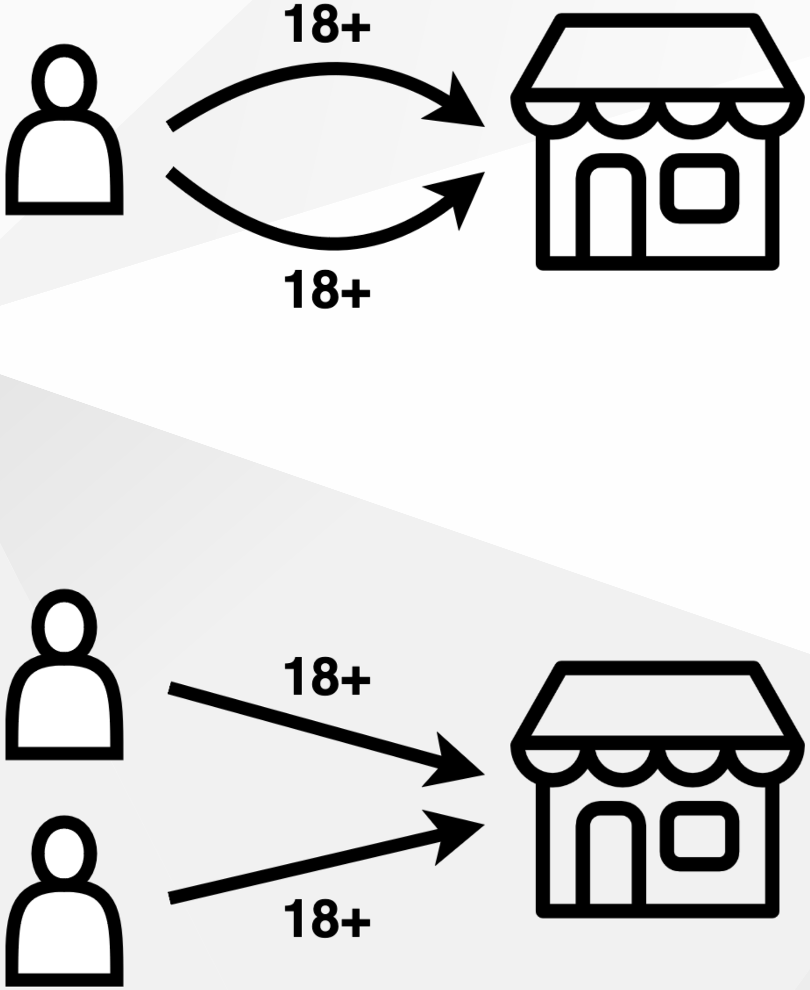
- **ARF:** issuer plaatst digitale handtekening (e.g. ECDSA) over attributen en user public key
- **BBS+/Idemix:** middels zero knowledge proof over attributen en issuer signature
    - **Idemix:** gebruikt door Yivi; RSA-gebaseerd ($n = pq$)
    - **BBS+:** dezelfde features; efficiënter; EC-gebaseerd; HSM friendly

Versimpeld ARF-style credential

```
{
  "payload": {
    "attributes": {
      "given_name": "John",
      "family_name": "Doe",
      "birthdate": "1980-01-01",
      "is_over_18": true
    },
    "user_public_key": "GZWVz_D4jXElRMG86xeTmsmErMiLrf8_05sQb4Qt-LbD8A[...]"
  },
  "issuer_signature": "gfOKR152uklVggQjVrkBFHAHPc-tF86xeTms1xtVdXqnGNm[...]"
}
```

Verder versimpeld ARF-credential

```
{
  "payload": {
    "attributes": {
      "is_over_18": true
    },
    "user_public_key": "GZWVz_D4jXElRMG86xeTmsmErMiLrf8_05sQb4Qt-LbD8A[...]"
  },
  "issuer_signature": "gfOKR152uklVggQjVrkBFHAHPc-tF86xeTms1xtVdXqnGNm[...]"
}
```



Privacy: multishow unlinkability

Als je twee keer hetzelfde niet-unieke attribuut aan de RP laat zien, kan hij je niet herkennen

- Oplosbaar met batch issuance van credentialkopieën
- Elke credentialkopie is single use

Privacy: issuer unlinkability

*Als je twee keer hetzelfde niet-unieke attribuut aan de RP laat zien, kan hij je niet herkennen, **zelfs als de issuer met hem meewerkt***

- Niet haalbaar in ARF-setup, alleen met BBS+/Idemix
- Alleen relevant wanneer geen van je attributen je identificeren
  - Kleine fractie van wallet usecases
  - Zwakke user binding

Hardware binding

> “ *Any type of digital credential, anonymous or not, can be copied from one device to another. [...] Mitigation strategies (outside the scope of this position paper) include storing the users’ keys in secure enclave* ”

- Niet uit de scope van de ARF en implementaties
- Oplosbaar met keyshare server
  - Geen support voor offline disclosures
- Gangbare mobiele secure hardware (SE/TEE) ondersteunt geen Idemix/BBS+ maar wel ECDSA

Revocatie

> *Revocation is a hard problem in practice. [...] [Short lived credentials] work for anonymous credentials as well*

- Short lived credentials zijn:
  - ofwel niet granulair genoeg
  - ofwel een grote belasting voor de issuer
- unlinkable revocatie met accumulatoren is lastig
  - kan zoals in Yivi, maar gebruikt RSA-achtige keys
  - technisch gecompliceerd in BBS+
- revocatie kan prima met https://www.w3.org/TR/vc-bitstring-status-list/
  - linkbaar: unieke identifier in elk credential

Post-quantum security

“ *The [ARF approach] is [not] post-quantum secure* ”

… maar is wel eenvoudig PQ-secure te maken

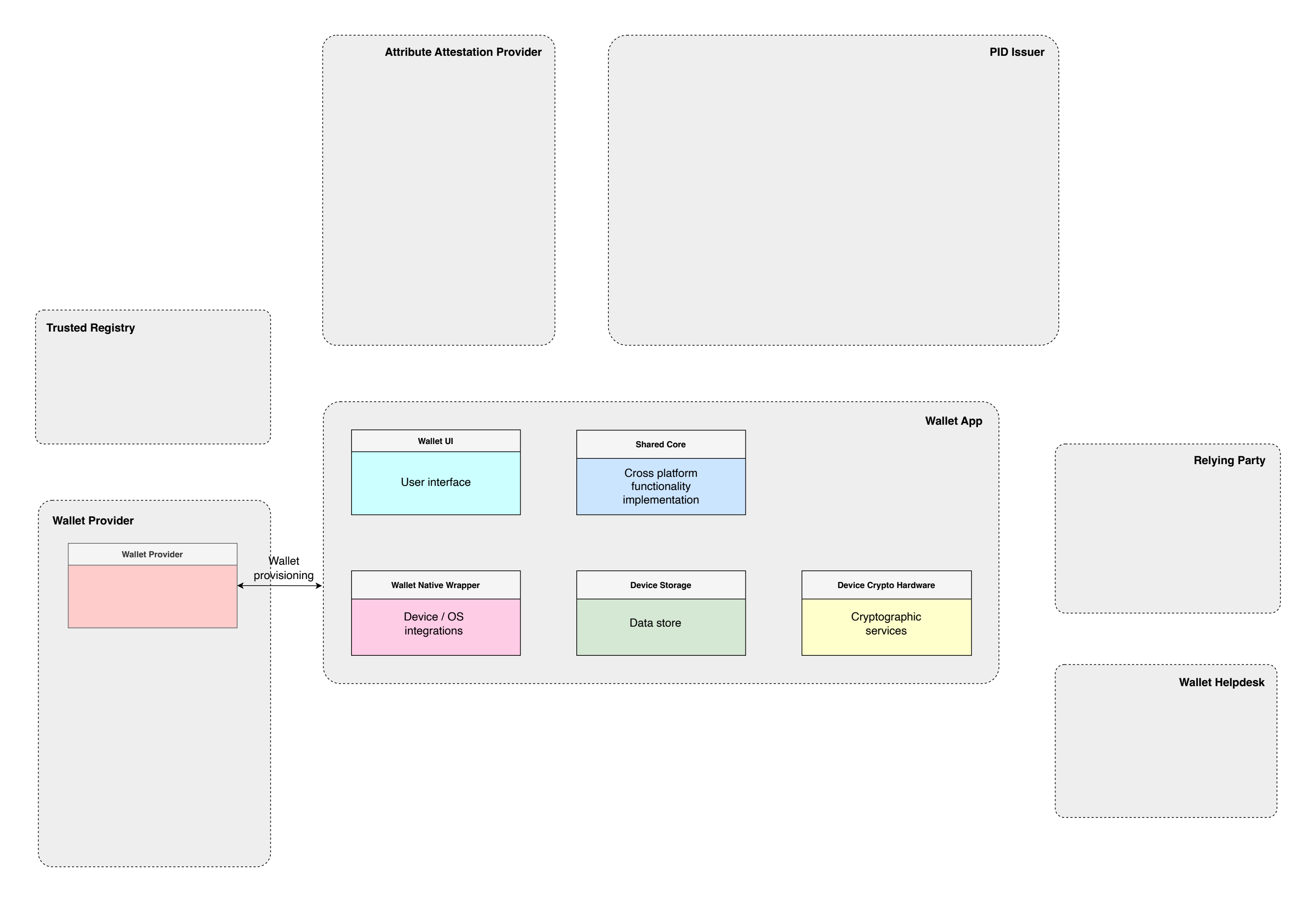
“ *Currently, there do not exist anonymous credential schemes that are plausibly post-quantum secure, scalable to the eIDAS setting and have high quality software implementations.* ”

Samengevat

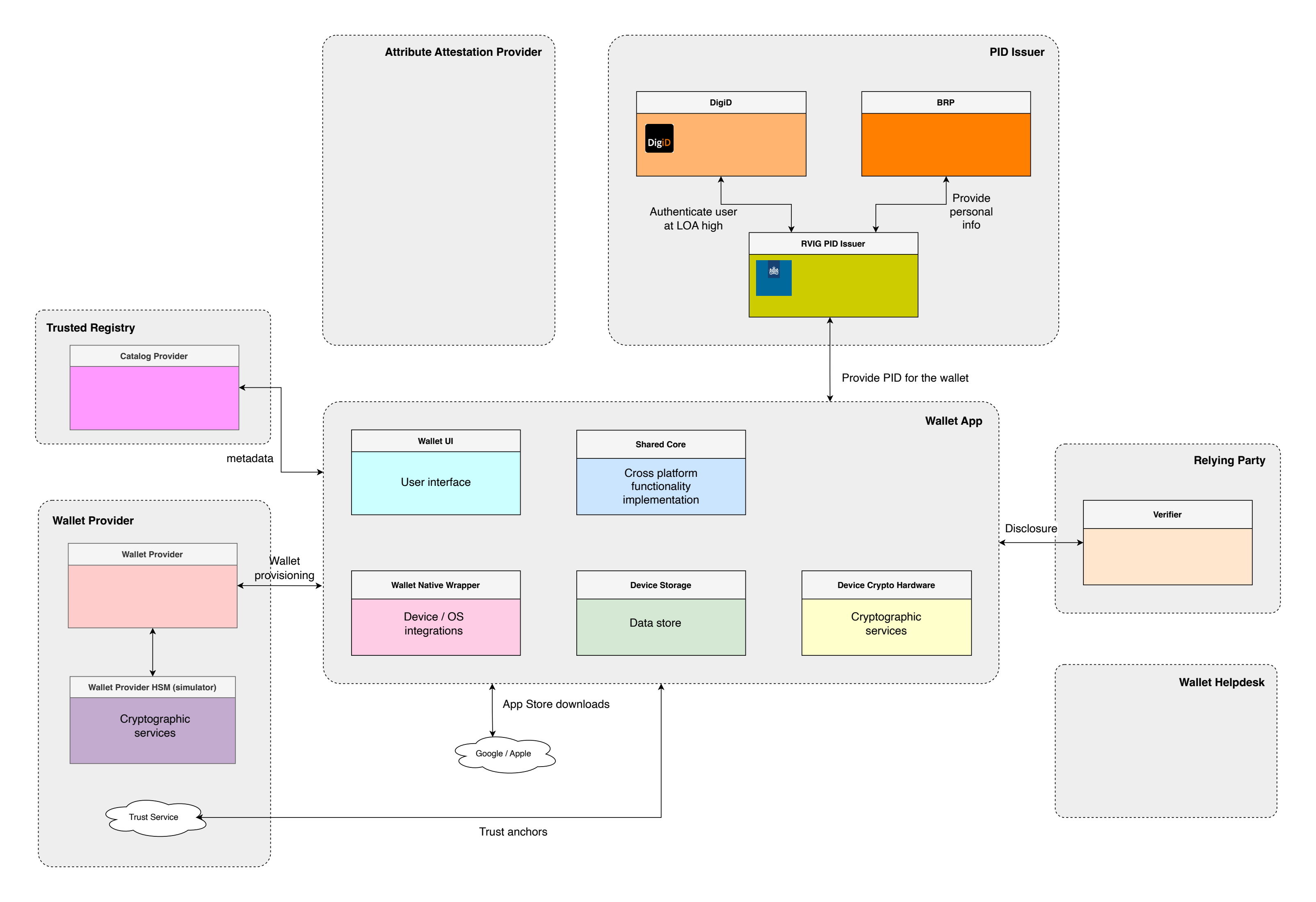
- Privacy & unlinkability: geldige kritiek maar beperkte impact
    - Single use credentials komen qua privacy een behoorlijk eind
- Weinig houvast op lastige issues waar een wallet implementatie wel iets mee moet
- Mogelijke way forward voor BBS+:
    - Alleen online
    - Offline: hybride oplossing met ARF-style credentials
    - Gebruik van linkable revocation

NL Wallet update & demo

NL wallet: mei 2023



NL wallet: nu


Attribute Attestation Provider
PID Issuer
DigiD
DigiD
BRP
Authenticate user at LOA high
Provide personal info
RVIG PID Issuer
Provide PID for the wallet
Trusted Registry
Catalog Provider
metadata
Wallet App
Wallet UI
User interface
Shared Core
Cross platform functionality implementation
Wallet Provider
Wallet Provider
Wallet provisioning
Wallet Native Wrapper
Device / OS integrations
Device Storage
Data store
Device Crypto Hardware
Cryptographic services
Relying Party
Verifier
Disclosure
Wallet Provider HSM (simulator)
Cryptographic services
App Store downloads
Google / Apple
Wallet Helpdesk
Trust Service
Trust anchors

Demo