
yivi
The Identity Wallet

Caesar Groep

Martijn Kamphuis

Wouter Ensink

Sara Vahdati Pour

Luc Spaas

Dibran Mulder

Sietse Ringers

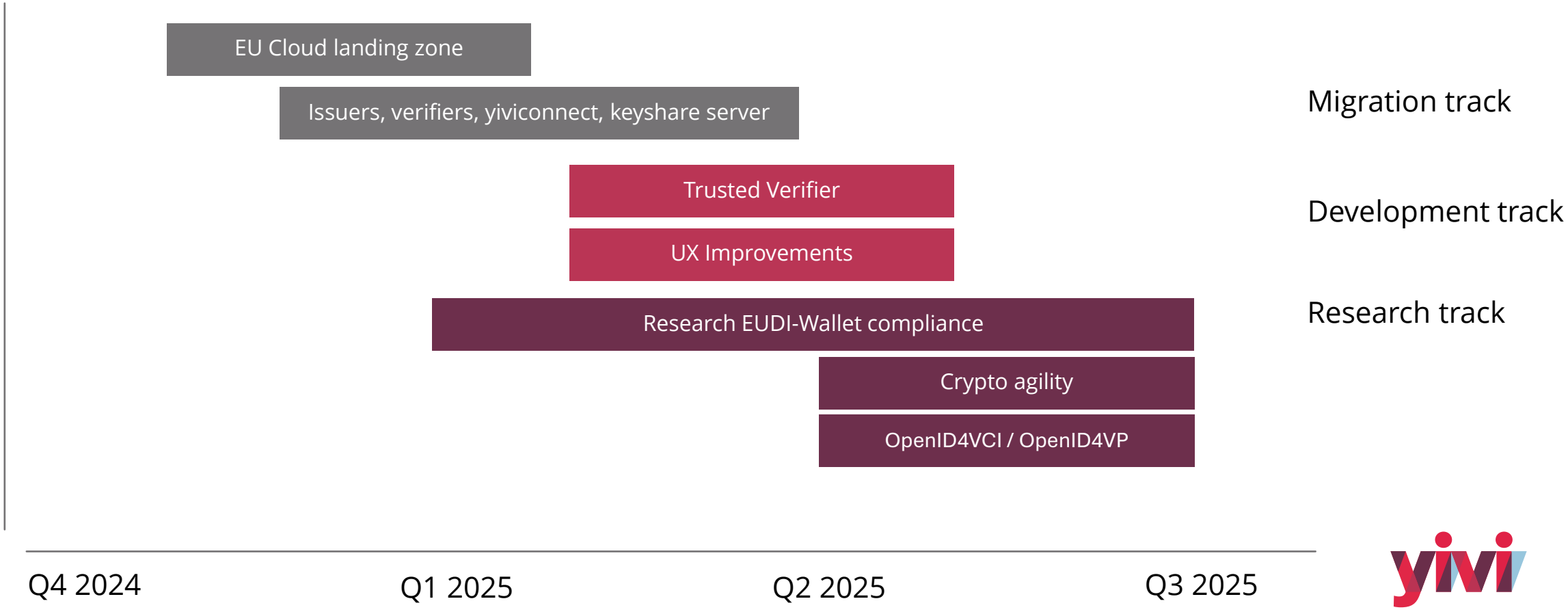
Quincy de Jong

Jasper van der Linden

Agenda

- Roadmap
- Cloud migration
- UX improvements
- EUDI compliance
- Trusted Verifiers
- Community

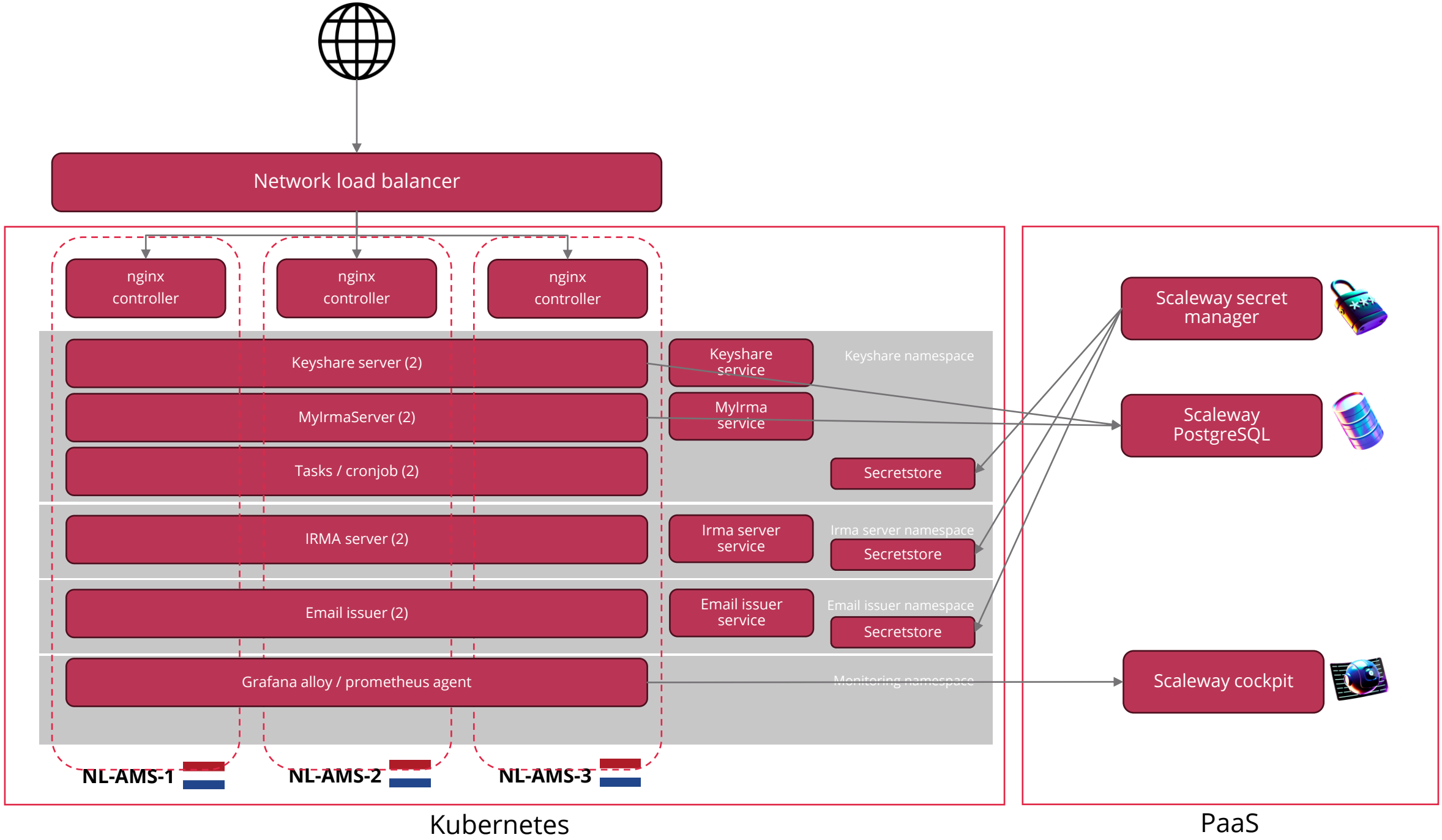
Yivi roadmap



Cloud migration

- Scaleway is a European sovereign cloud provider.
  - Offers public cloud like interfaces, such as Terraform providers.
  - Has multiple regions in Europe: Paris, Amsterdam and Warsaw.
  - Offers availability zones within a region. At least 3 physically separated data centers.
  - Offers startup program, reducing hosting costs.
  - Has many PaaS-services, such as:
    - Kubernetes
    - Secret manager
    - PostgreSQL
    - Grafana
    - Etc..

Scaleway yivi



Cloud migration

Resource	Old location	New location	Status
Mail	yivi@caesar.nl and noreply@sidn.nl	support@yivi.app and noreply@mail.yivi.app	🚀 Rolling out
SMS issuer	https://sidnsmsissuer.yiviconnect.nl/issuance/sms	https://sms-issuer.yivi.app	✅ Ready
Email issuer	https://sidnemailissuer.yiviconnect.nl/issuance/email	https://email-issuer.yivi.app	✅ Ready
iDIN issuer	https://privacybydesign.foundation/uitgifte/idin/	https://idin-issuer.yivi.app	✅ Ready
Attribute index	https://privacybydesign.foundation/attribute-index/en/	https://attribute-index.yivi.app	✅ Ready
Atumd	https://irma.sidn.nl/atumd/	https://atumd.yivi.app	🚀 Rolling out
Scheme	https://privacybydesign.foundation/schememanager/pbdf/	https://scheme.yivi.app/pbdf/	🚀 Rolling out
Docs	https://irma.app/docs	https://docs.yivi.app	✅ Ready
Demo's	https://privacybydesign.foundation/demo/	https://demos.yivi.app	🚀 Rolling out
Yivi Connect	URL remains unchanged	URL remains unchanged	🚀 Rolling out
Keyshare server	https://irma.sidn.nl/tomcat/irma_keyshare_server	https://keyshare.yivi.app	March 2025
MyIrma	URL remains unchanged	URL remains unchanged	March 2025
Open	URL remains unchanged	URL remains unchanged	February 2025

UX

Understandable

Reading level checks
Reduce number of steps for important actions
Styling consistency

Accessible

Comply with WCAG 2 (later more)
Test with target audience

Trustworthy

Transparent data sharing
Imagery and styling of trusted parties
Be clear about who, how and why

Beautiful

Clear, helpful images
Fluid, helpful animations
Balanced, responsive layout

UX - WCAG 2 Compliance

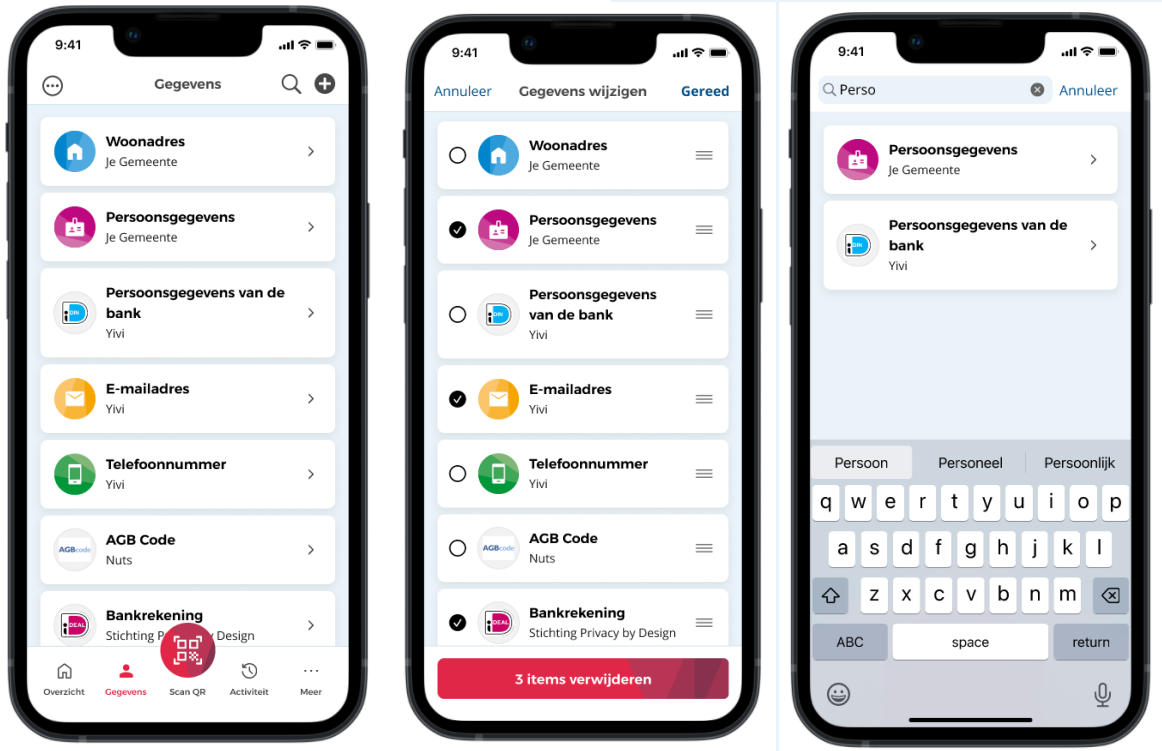
- European Accessibility Act (EAA)
- Web Content Accessibility Guideline
- AA required for governments
- Aiming for AAA
- Touch targets
- Contrast ratios
- Screen readers
- Portrait + landscape
- Multiple input mechanisms
- And more

UX - QR-code button on login page

- Quick access to QR scanner.
- Familiar UX with banking apps, most of them already have it.

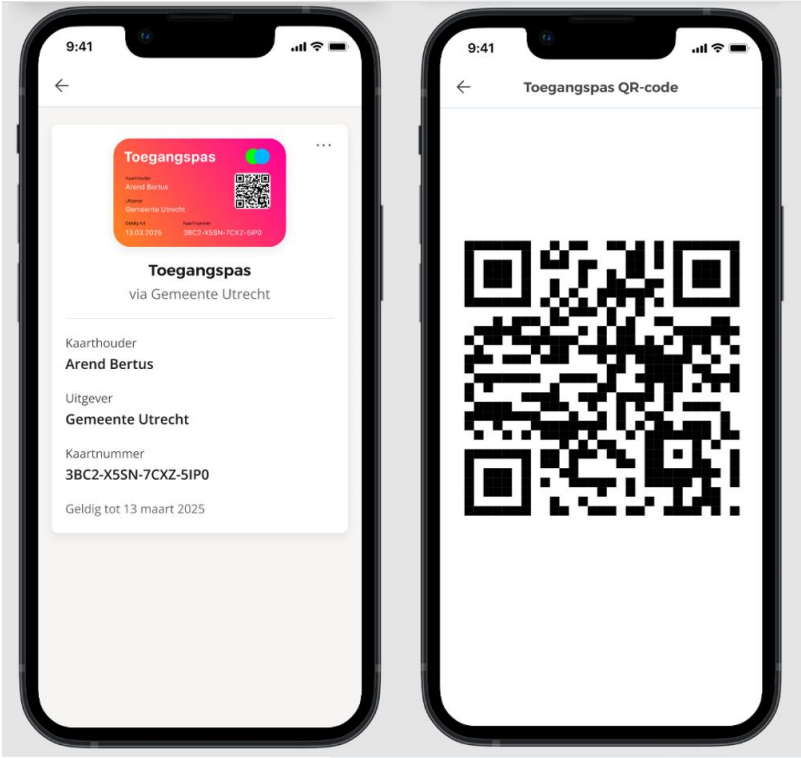
UX - Improved card organization & navigation

- Show where cards go with animation
  - Makes more sense when only 1 page
- Allow users to sort, reorganize & categorize
- Add search option
- (move + button to app bar to make room?)



UX - Brand extensions

- Issuers should be able to customize cards
  Requires scheme extension
- Assess implications for accessibility and selective disclosure.
- Inspiration: SVG templates in SD-JWT VC



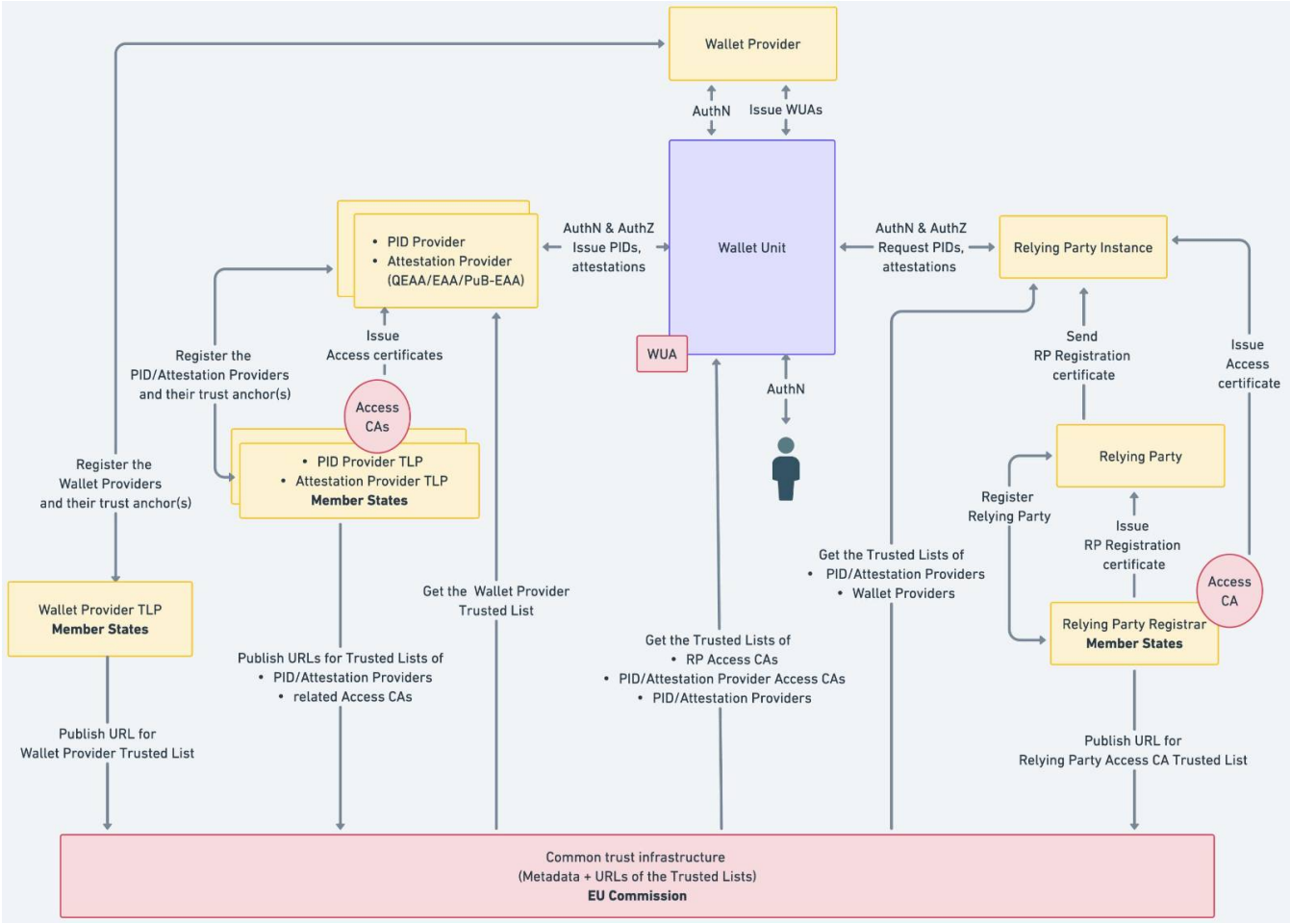
EUDI-wallet compliance

- We want to **align with EUDI standards** so that Yivi takes part in the EUDI-wallet ecosystem, we want to achieve that by becoming **crypto agile**.
- Fundamental research ahead:
  - What are the implications of **crypto agility**, in the sense that Yivi can support multiple trust frameworks, protocols and cryptographic implementations.
  - The ARF is standardizing on OpenID4VCI and OpenID4VP protocols, for respectively issuance and disclosure.
    - Can we embed Idemix credentials in it, there is support for AnonCreds which is kind of familiar to Idemix.
    - What features of the IRMA protocol do we lose when we adopt OpenID4VCI and OpenID4VP, such as ChainedSessions, Randomblind issuance
    - Other wallets claim to be ARF compliant but are often only using OpenID4VCI and OpenID4VP.
  - How can we leverage work done by the NL Wallet?
    - The NL Wallet is mostly written in Rust, how can we adopt it in the Yivi App and IRMA Server

ARF 1.5

- First review of ARF 1.5 published 3 days ago.
- Member state scope expanded
  - Relying party registrar
  - Wallet Provider Trusted List Provider

- Relying party registrar
  - New protection for over authentication
- Access Certificate Authorities
  - New role which allows for re-use of existing infrastructure.



ARF 1.5

- A new risk has been identified on privacy concerns which Yivi takes care of:
  - Relying party linkability (Multi show unlinkability)
  - Attestation provider linkability (Issuer unlinkability)
- This topic will be explored in context of ARF 2.0.
- European Commision Tender for ZKP-based age verification.

Development, Consultancy and Support for an Age Verification Solution
EC-CNECT/2024/OP/0073

7.4.3.5 RISKS AND MITIGATION MEASURES RELATED TO USER PRIVACY

User privacy is a key aspect in the design and implementation of the EUDI Wallet ecosystem. Attributes are presented as electronic attestations using formats based on salted and hashed attributed. These attestations contain unique, fixed elements such as hash values, public keys, and signatures. Malicious Relying Parties could exploit these values to track Users by storing and comparing them across multiple transactions, identifying recurring patterns. This privacy threat, known as **Relying Party linkability**, can occur within a single Relying Party or among colluding entities.

A similar privacy threat arises when colluding Relying Parties share unique values with a malicious Attestation Provider, allowing it to track User activity across multiple services. In this case, it's called **Attestation Provider linkability**.

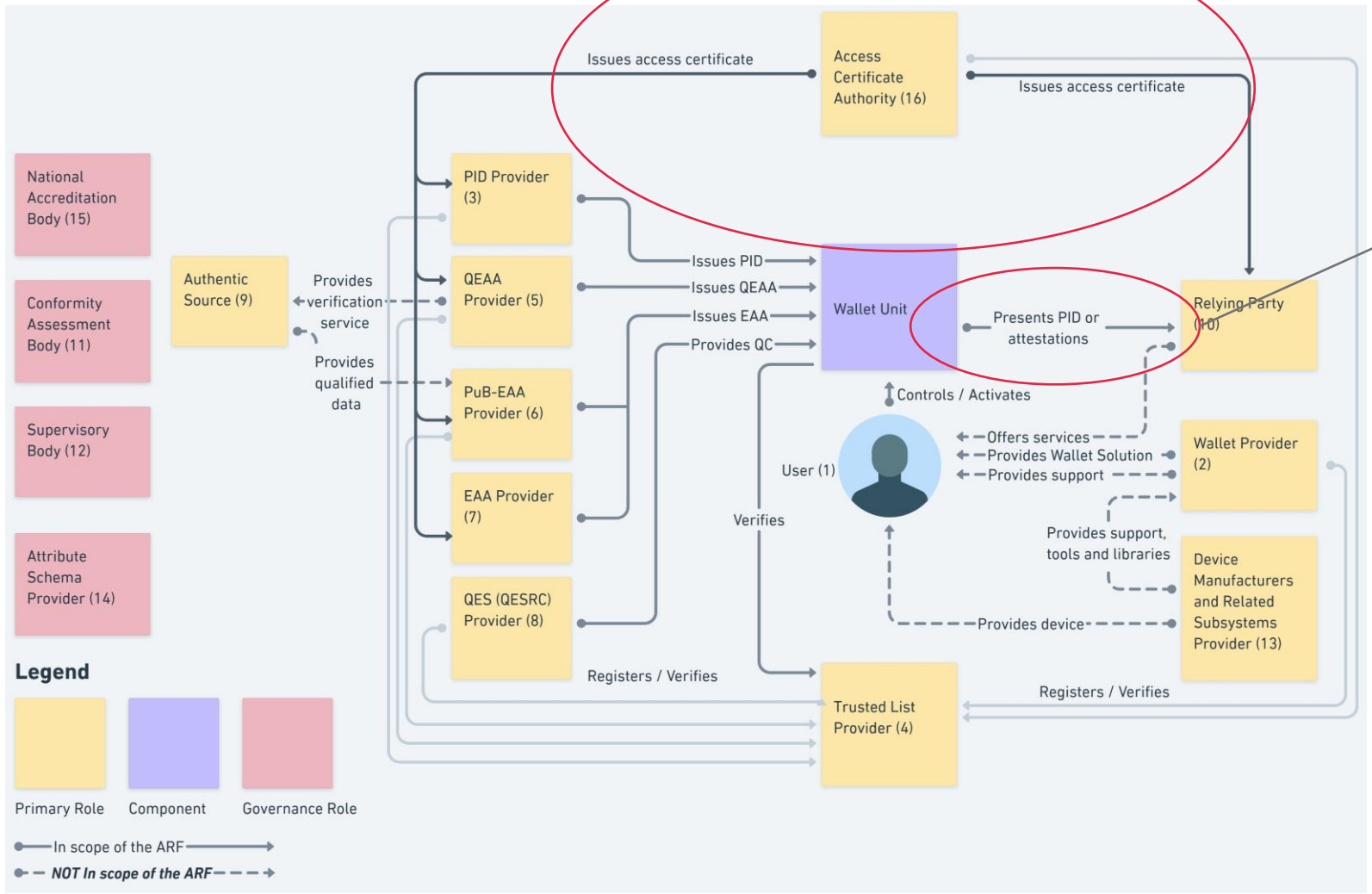
Regarding the mitigation of these risks:

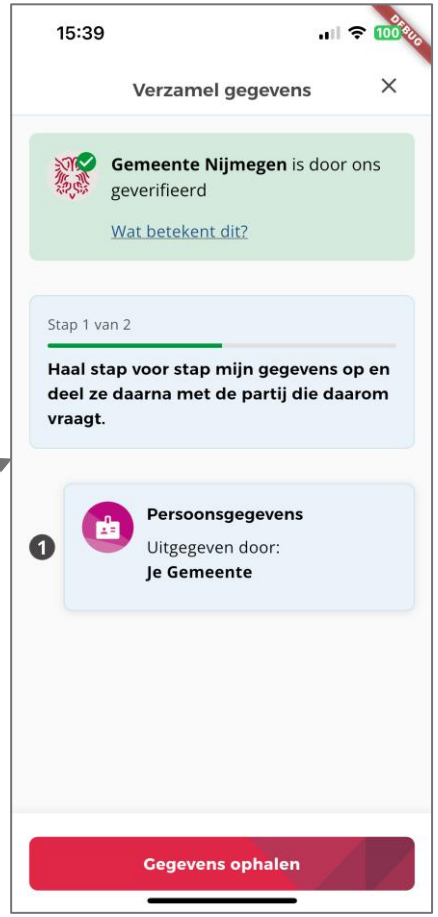
- A trustworthy PID Provider or Attestation Provider can mitigate Relying Party linkability, either partially or fully, by issuing multiple PIDs or attestations to the same User. Wallet Units can use these attestations as disposable (single-use) or Relying Party-specific, ensuring that different Relying Parties receive distinct attestations that cannot be linked. However, this approach increases issuance complexity and management overhead. This topic will be further explored in the context of the next major release of ARF. Additionally, organizational and enforcement measures can help deter Relying Parties from colluding and tracking Users. In particular, Relying Parties found in violation will have their access certificates revoked, preventing them from further interactions with Wallet Units.
- Attestation Provider linkability cannot be fully eliminated when using attestation formats based on salted hashes. The only viable mitigation is to adopt Zero-Knowledge Proofs (ZKPs) as a verification mechanism instead of relying on salted-attribute hashes. However, the integration of ZKPs in the EUDI Wallet ecosystem is still under discussion and development due to the complexity of implementing ZKP solutions in secure hardware and the lack of support in currently available secure hardware (WSCDs). This topic will be further explored in the context of of the next major release od the ARF. As with Relying Party linkability, organizational and enforcement measures can help deter Attestation Providers from colluding and tracking Users. Additionally, many Attestation Providers are subject to regular audits, making it easier to detect collusion and tracking compared to Relying Parties.

Zero-Knowledge Proof (ZKP) mechanisms for verifying personal information are highly promising and essential for ensuring privacy in various use-case scenarios. They enable Users to prove statements such as "I am over 18" without disclosing any personal data, offering a robust solution for privacy-preserving authentication and verification.

One key area of development is age verification, where the European Commission is actively exploring and testing ZKP-based solutions. The outcomes of this initiative could pave the way for the adoption of ZKPs within the EUDI Wallet ecosystem, further strengthening privacy protections in future implementations.

Trusted Verifiers





Trusted Verifiers - Yivi Portal

- Register organizations, both **verifiers** and **issuers**.
  - Without explicit usage of KVK credentials.
  - Name, logo, domain, slug, etc.
  - Yivi users should be able to become maintainers of an organization.
  - DNS check for organization ownership.
  - Signing our terms and conditions. In the future maybe billing.
  - Request for sponsorship.
- Trust framework management
  - Idemix public keys
  - Certificate management
  - Over-authentication protection, disclosure permissions.

Yivi Community

- We have talked to ~50 organizations mainly in the Insurance, Energy, Governmental and Health sector.

- Proof of Concept with Post Quantum Yivi
  - Research Intern @ Max Planck Institute for Security and Privacy (MPI-SP)
  - Builds upon research of Bas Westerbaan (prev. Radboud, now Cloudflare)
  - zkDilithium implementation.
  - Key challenge is performance 1000 generation/100ms verification on a MacBook

Questions

 d.mulder@caesar.nl

 yivi.app / caesar.nl

 Dibran Mulder

 DibranMulder