Risks of Digital Identity in Education and Research Wallets

Amineh Akhavan saraf, Leibniz Supercomputing Centre – Munich

GN5-2 WP5 Trust and Identity – Wallets Team

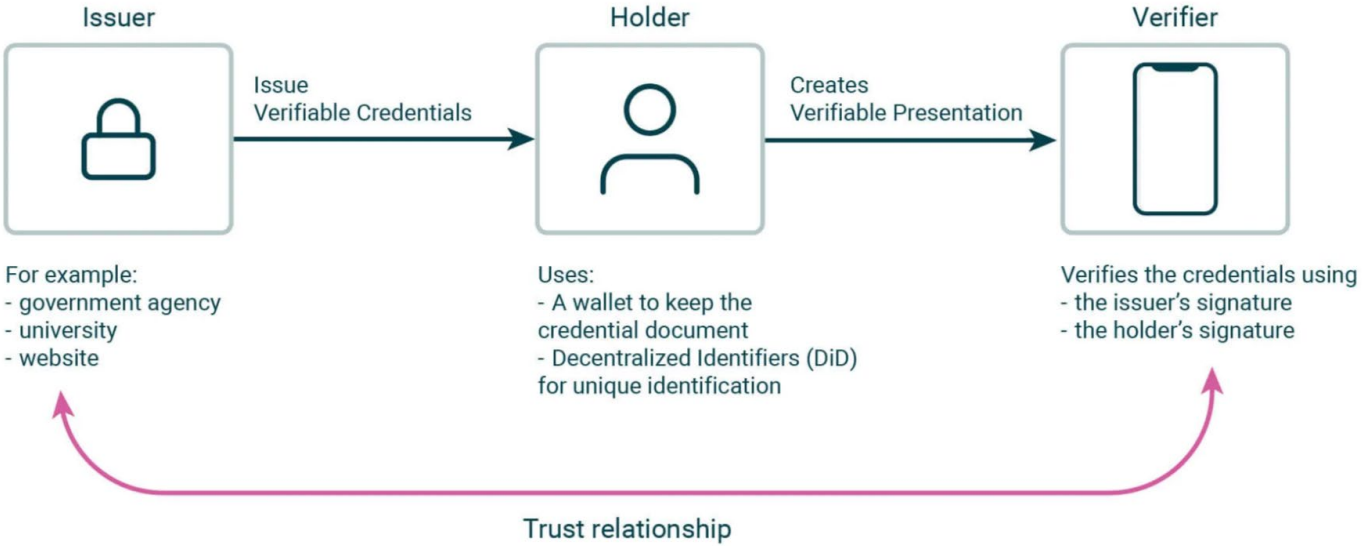
TNC25: Brighton, UK
10 June 2025

Agenda

- Introduction
- Risk Management
- Financial Risks
- Legal Risks
- Strategic Risks
- Security Risks
- Risks Assessment
- Conclusion

Introduction

A Digital identity in wallet enables you to **securely** prove and manage who you are in the digital world, in a way that is trusted, verifiable, **user-controlled**, and **interoperable** across services. Unlike traditional systems where your data lives with the identity provider, **wallet-based identity lives with you**.



Introduction

Wallet: A digital identity wallet is a **secure, encrypted database** that collects and holds keys, identifiers, and verifiable credentials (VCs). The wallet is also a digital address book, **collecting and maintaining** owner‘s relationships.

- VCs in research and education sector:
  - Academic/Research identity in the VC list
  - Diplomas and Degrees
  - Certificates
  - Transcripts
  - Digital Badges
  - Letters of Recommendation

Risk Management

Risk management is the process of **identifying**, **assessing** and controlling financial, legal, strategic and security risks to an organization's capital and earnings. [IBM]

Main Categories:

- Financial
- Legal
- Strategic
- Security

Financial Risks

Big Tech Companies (GAFAM)

- Google
- Apple
- Facebook(Meta)
- Amazon
- Microsoft

Competing Technology

- Ledger Technologies
  - Blockchain based
  - DAG based
- Non-Ledger Model

Environmental Cost / Cost

- Running and maintaining cost of Server vs Blockchain
- Electricity consumption

Financial Risks

Funding: A particular scarcity risk, due to lack of funding

- Supporting from government or institutes for research and development of DI is needed
- Only users benefit from it, not issuers
- Business-Plan definition is still in progress. Not only for R&E sector, but also being explored within the context of EUDI large-scale pilots.

GEANT is experienced in Fed- ID and need more funding to extend supporting wallet related activities

Marketing

- Lack of delivering attractive and user friendly services
- Highlighting practical user and stakeholders benefits of identity workflows

Legal Risks

Governmental Laws

- Some governmental policies impose to take a special orientation in technologies or protocols.
- Not enough maturity in existing legislations. Changes in governmental rules are not futuristic enough.
- The progress of codifying related rules is very slower than coming new technologies.
- eIDAS
  - eID in education sector is not the same as eID in eIDAS
  - Education sector is beyond Europe
- Overcoming national borders might impose barriers.

Rules in the Case of Misusing

- Unclear rules, undefined responsibility

Legal Risks

International Compatibility (ex. GDPR)

- Some countries have legal commitments, while others have none or follow different regulations, leading to incompatibility
- Different use of existing rules
- Local legislations (also sector or domain legislations) affects international behaviors. Local rules are various and people bring these to the international ecosystem and cause problems.

User Responsibility (consent)

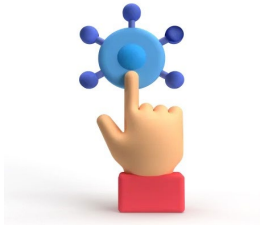
- Users will need to be mindful of what data they share and with whom.

Strategic Risks

Dependency→ whenever the system has a dependency on something or someone else.

1. **Paper credential**: in many cases just traditional paper credential flows are accepted or a digital one have to be confirmed by paper credential.
2. **Impact of EUDI:** limited coverage of EUDI leads to parallel ecosystem
3. **Non-scalable and change-resistant architecture**
4. **GAFAM Connected Services**

Strategic Risks



Usability → risk of developing systems that do not achieve users "needs and expectations“

1. **User-friendliness:** process, same terms
2. **Inclusion Challenges (Exclusion Impact)**
3. **Support mechanisms:** face-to-face, video or telephony
4. **Fragmented design solutions (Silos)**: Inefficient or disjointed user experiences across different platforms or services
5. **GAFAM**
    - GAFAM Services: easy of use leads to user spoiling
    - GAFAM shape user expectations

Strategic Risks - Usability

6. **Complexity vs. Control:** Balancing technical complexity with intuitive user control and overall ease of use.

Identity management involves trust, authentication, privacy, personal information, and security, with complex edge cases and technical standards.

Trust is built through understanding. If a system is too complex, it becomes difficult for users to use and accept it.

- Complexity for users
- Complexity for other parties

Strategic Risks

Interoperability (Standards and Protocols)

1. **Lack of standards and protocols**
2. **Influence of external standards and architectures**
3. **Incompatibility with legacy systems:** Interoperability with existing systems and standards, both within the research and education sector and with external stakeholders, is crucial. It brings also technical complexity
4. **Agreement delays:** Reaching consensus across many parties with different needs can be time-consuming. e.g.
    a. The Digital ID and Authentication Council of Canada (DIACC): 4-6 years
    b. The process of creating a framework for agreement by Australian government: 2015-2021
5. **EU standardization process** e.g. ELM v3, ARF
6. **National ID governance and EUDIW:** e.g. Unclear Cross boarding DI mapping in eIDAS 2

Strategic Risks

Acceptance → any risk regarding to acceptance from users and stakeholders

1. **Resistance to Change:** Resistance to change among stakeholders in the research and education sector and users.

2. **Social trends (Culture)**

Intermediaries → Intermediaries in digital ecosystem trying to keep their influence

1. Identity validation company with various rules. They are still needed despite the wallet ecosystem is promised.
2. Paper intermediaries
3. Wallet creators: GAFAM and BCs…

Strategic Risks

Integration (technical aspects)

1. Technical and Policy Shortcomings: Missing libraries, interfaces, tools
2. Failure to extend identity services without gap: other market solutions succeed to fill the gap

Ontopiness → The old solution remained and new solutions extend the existing one and do not replace. It mean new stuffs are all on the top.

Security Risks

Protecting Data → challenges in implementing various level of s

1. Security of devices
   a. Physical vulnerabilities: Device lost/defection (not availability of device or no battery)/ stolen
   b. Lack of Device Security

2. Security of Wallets: A Wallet (one App or Web page) with lots of functionalities and different sectors may face up with increasing Vulnerabilities

3. Security of Services (ex. Healthcare system): It means security dependency to
   a. Service/Issuer security
   b. Relying parties/Verifier
   c. Intermediaries

Security Risks

Losing Data and Recovery Mechanism→ lack of support mechanism by security issues

- Not enough recovery solution
- No insurance
- Revoking process

Dark Net → security economic: there is a business to generate fake IDs or misuse of real IDs, which could be used for money laundering or any other illegal activities

- Fake ID
- Misusing of VC

EUDI wallet legislation like ARF, Implementing Acts, eIDAS 2.0 defines requirements to address security vulnerabilities. However, the supporting standards, technologies (both hardware and software), and protocols are not yet mature enough for full implementation.

Risks Assessment

Probability of occurrence

- Once in 10 years
- Once in 5 years
- Once in 2 years
- Once in 1 years
- Many times in a year

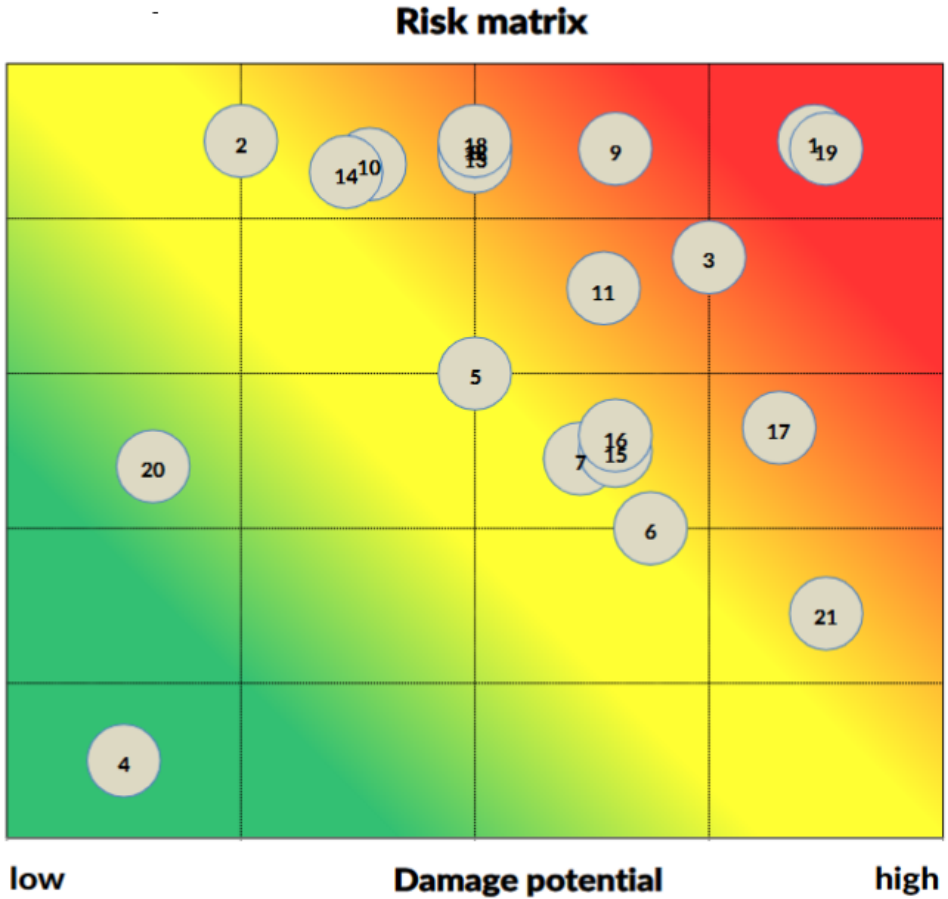
Potential damage

- Low
- Medium
- High
- Very High

Results from assessment in GN5-1

Potential damage / Occurrence Probability	Low	Medium	High	Very High
many times in a year	• Competing technology • Exposure to Governance Rules and standards	• Misusing of DID • Dependency • **Usability** • **Acceptance** • Protecting data	• User Responsibility	• GAFAM • Losing data
once in 1 years		• Funding	• Marketing • Intermediaries	
once in 2 years	• Dark Net		• Governments Rules • International Compatibility (ex. GDPR) • Interoperability (Standards and Protocols) • Integration	• *ontopiness*
once in 5 years				• Trust Infrastructure
once in 10 years	• Environmental cost			

Conclusion



Risk #	Red = Top risks 2024
19	Security Loss of Data
1	Fin GAFAM
9	Legal User responsibility
3	Fin Marketing
8	Legal DI misuse
11	Strategy Intermediaries
18	Security Protecting data
17	Strategy Ontopiness
10	Strategy Dependency
13	Strategy Usability
14	Strategy Acceptance
5	Fin Funding
16	Strategy Integration
15	Strategy Interoperability
12	Strategy Exposure
2	Fin Technology
6	Legal Governments
7	Legal Compatibility
21	Security Trust Infrastructure
20	Security Darknet
4	Fin Environmental Cost

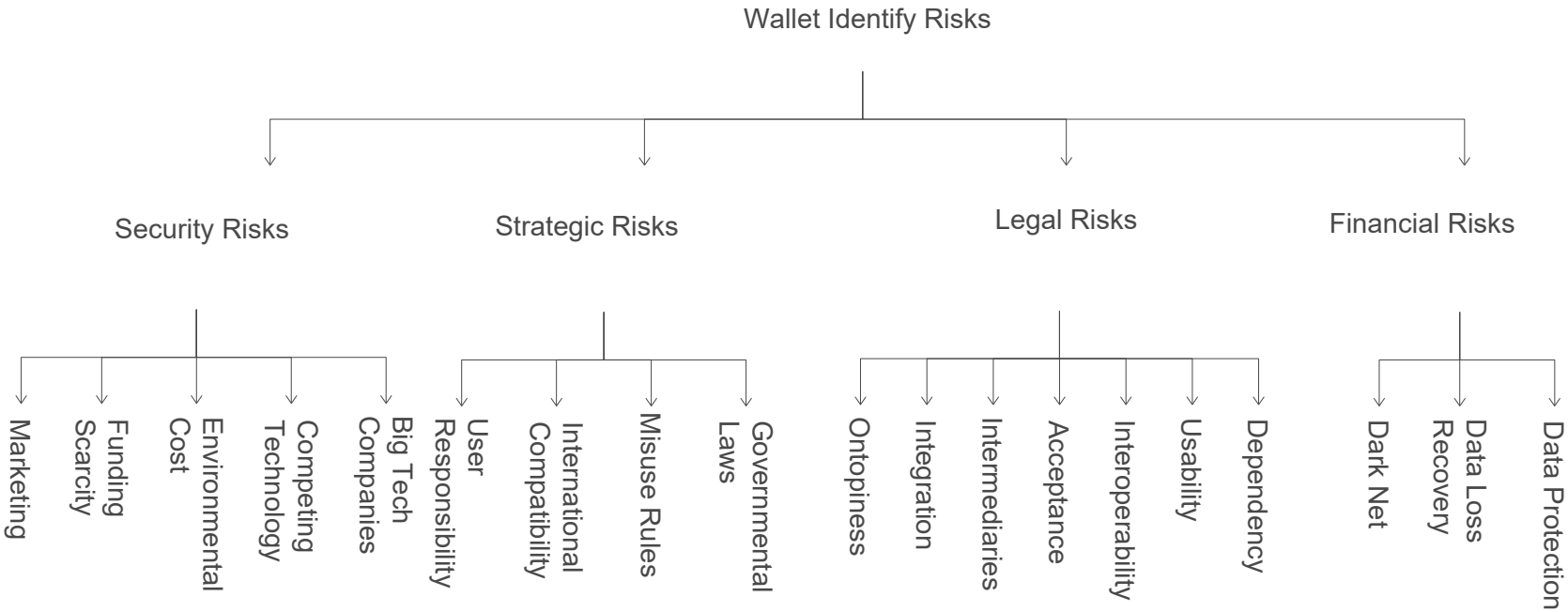
Start planning now for changes in Digital Identity

Join GEANT Wallet Community:

More Info on Wallet Wiki:

GEANT 5-2 WP5 T6 - Wallets Team

Risk Assessment Tree



Thank You

GEANT 5-2 WP5 T6 - Wallets Team

www.geant.org

Co-funded by
the European Union

References

- IDEA: Distributed Digital Identity and Decentralized Identifier
- Wallet: Windley, Phillip J.. Learning Digital Identity: Design, Deploy, and Manage Identity Architectures (p. 510). O'Reilly Media. Kindle Edition.
- What is Risk Management? | IBM
- How to control your biggest risks in digital identity — Public Digital

The main goal is to empower identity owners with more control over their digital identities, enhancing privacy, security, and interoperability.