FONDAZIONE BRUNO KESSLER
CENTER FOR CYBERSECURITY

So many Anonymous Credentials, so little adoption: can we escape the Linkability Well in Identity Management?

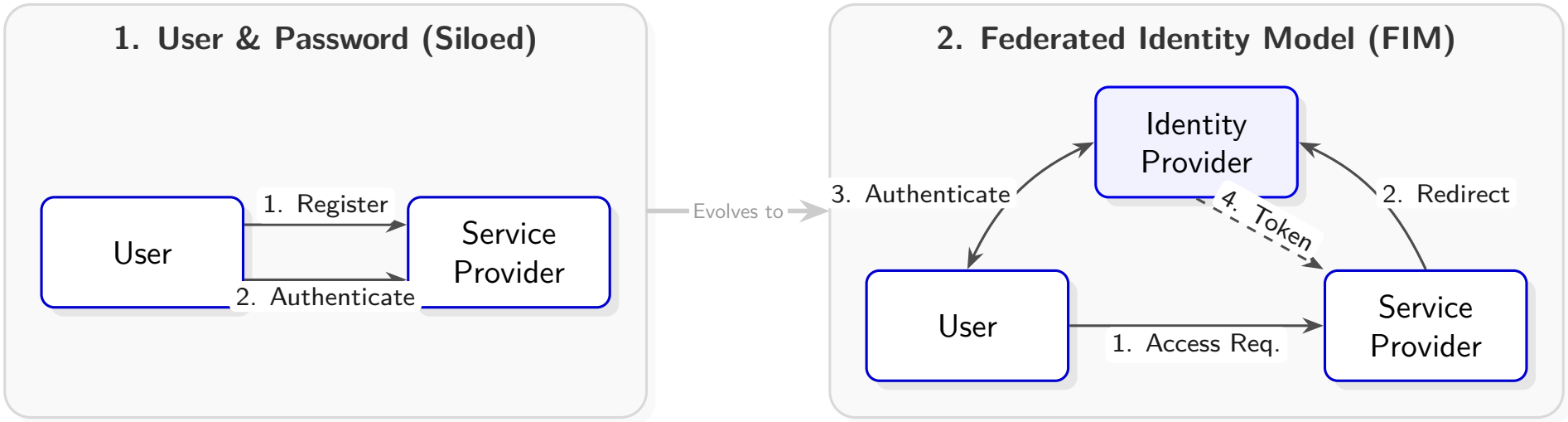
Andrea Moro

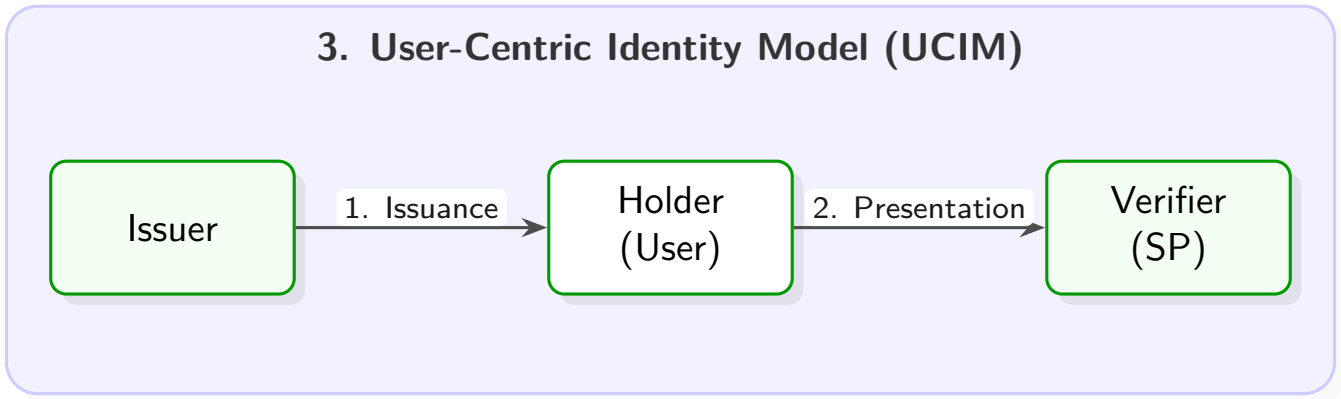
4th International Workshop on Trends in Digital Identity

April 21, 2026

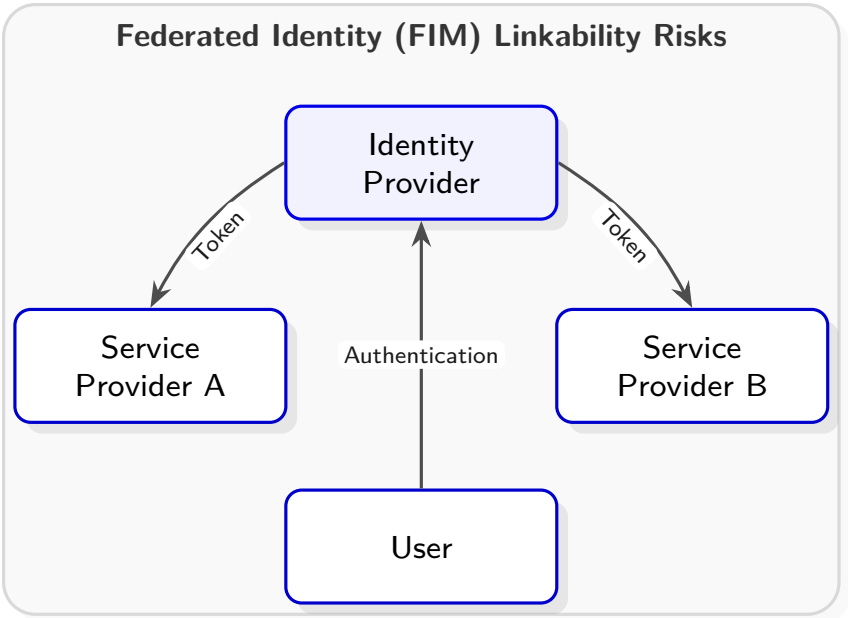
Summary

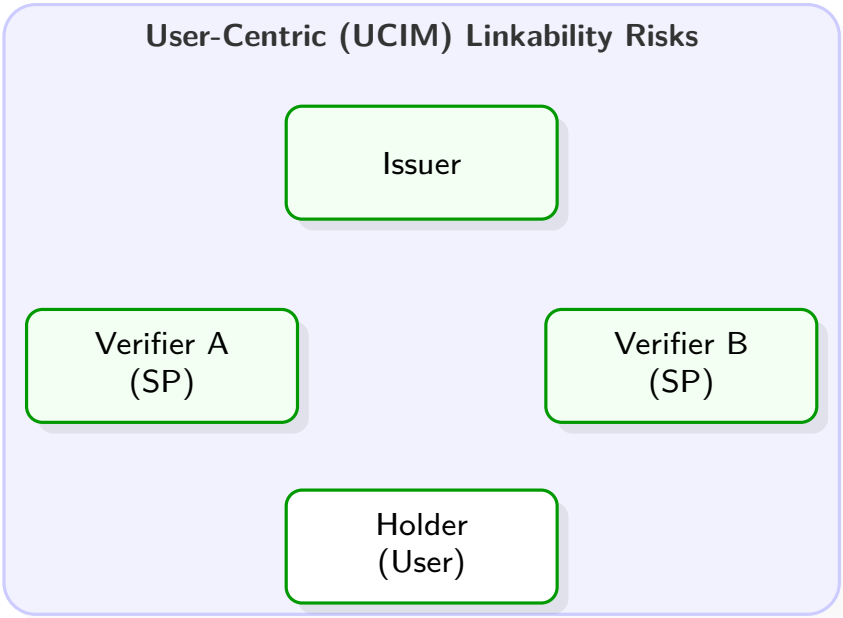
Madamin, dell'Identità Digitale il catalogo è questo





Privacy Risks

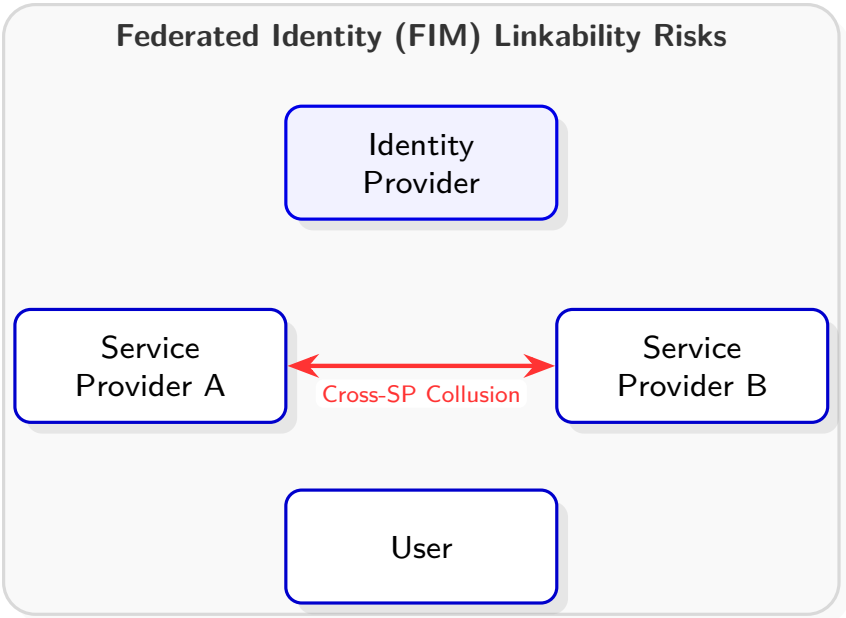


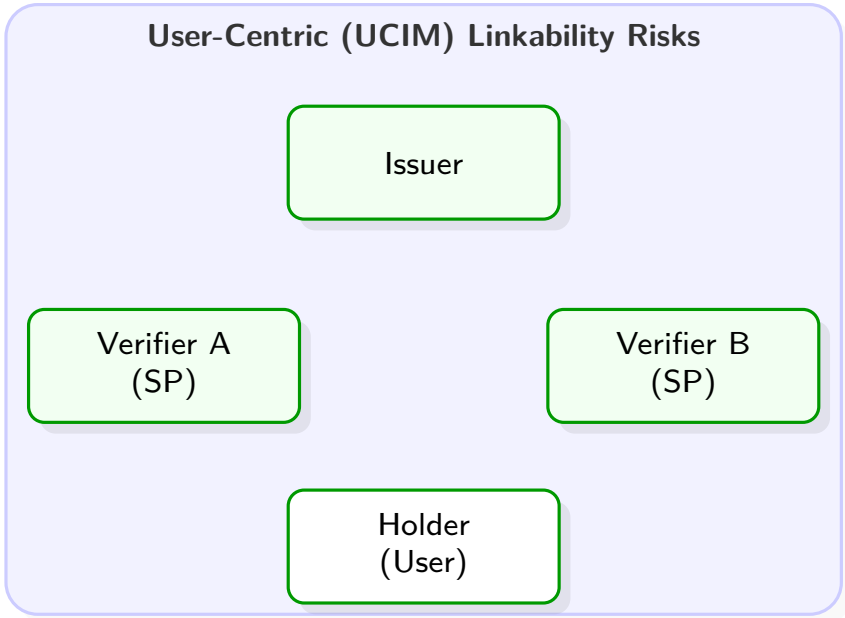


FIM Privacy Problems

UCIM Privacy Exploits

Privacy Risks



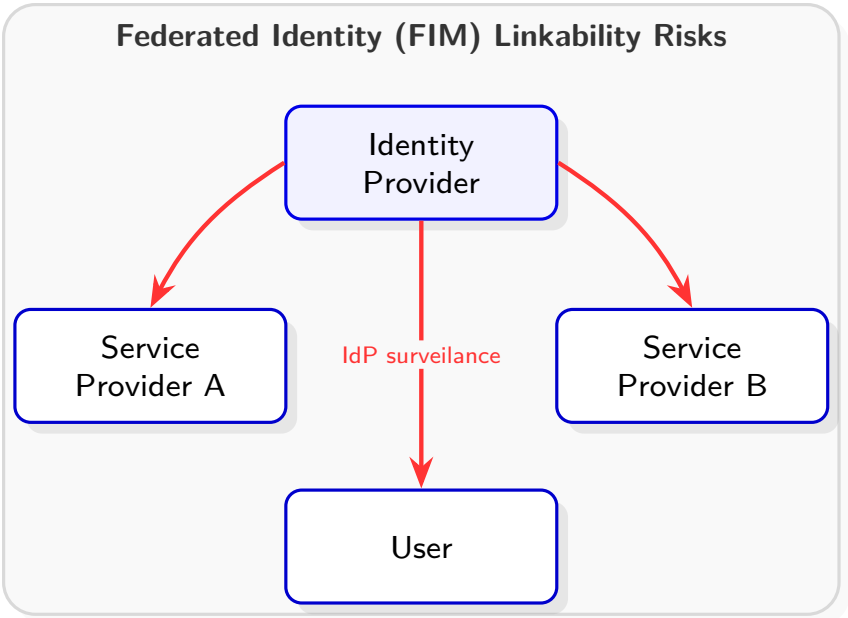


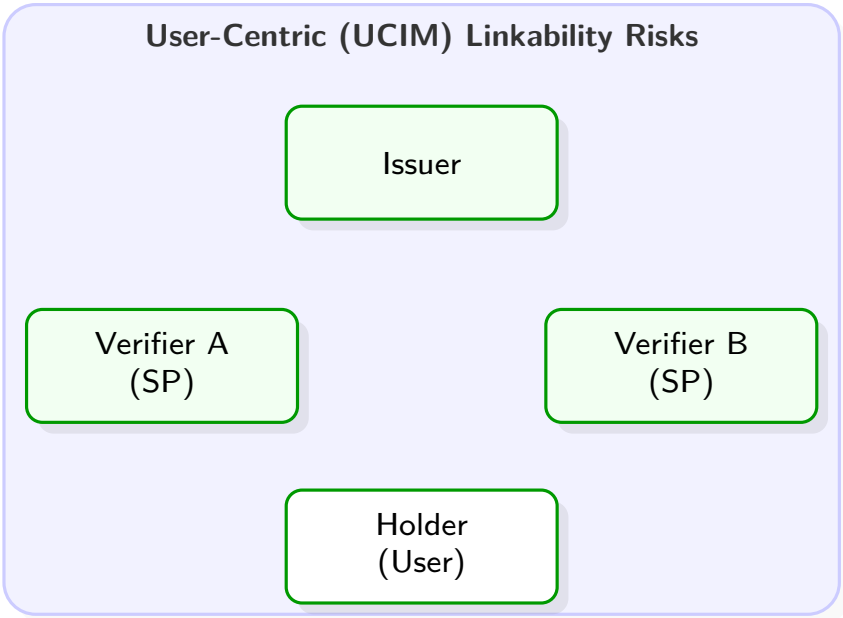
FIM Privacy Problems

- **Cross-SP Linkability**: Service Providers collude to track and profile the user.

UCIM Privacy Exploits

Privacy Risks



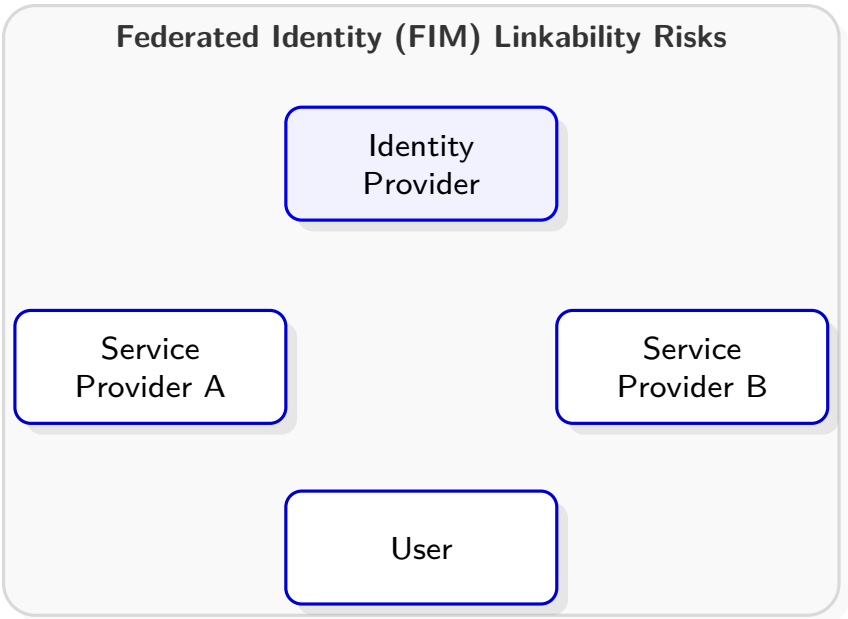


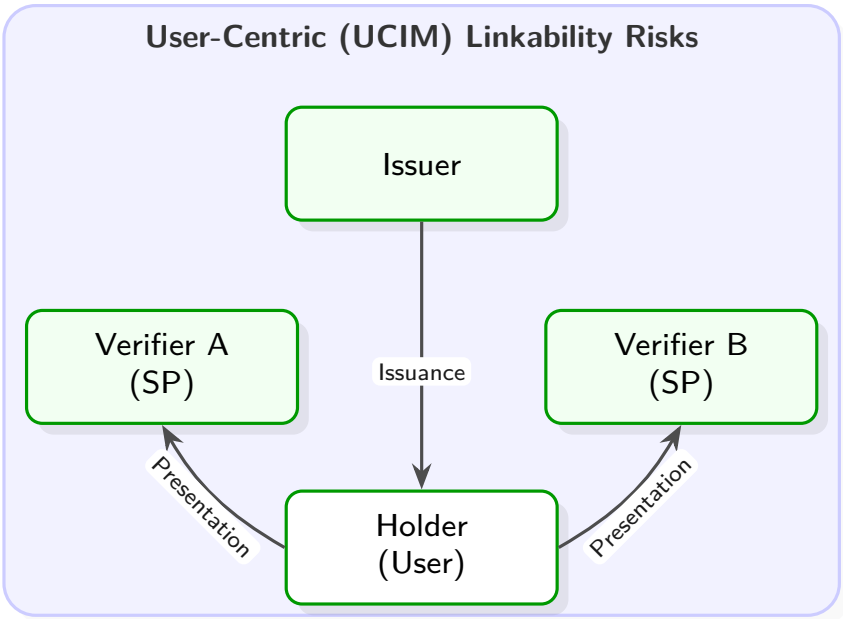
FIM Privacy Problems

- **Cross-SP Linkability**: Service Providers collude to track and profile the user.
- **IdP surveilance**: The IdP acts as a centralized point of surveillance.

UCIM Privacy Exploits

Privacy Risks



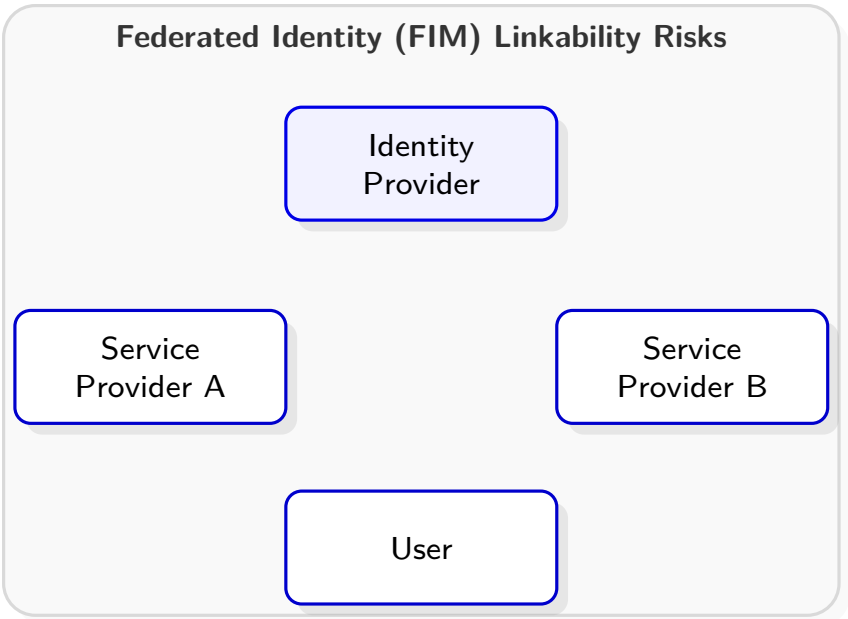


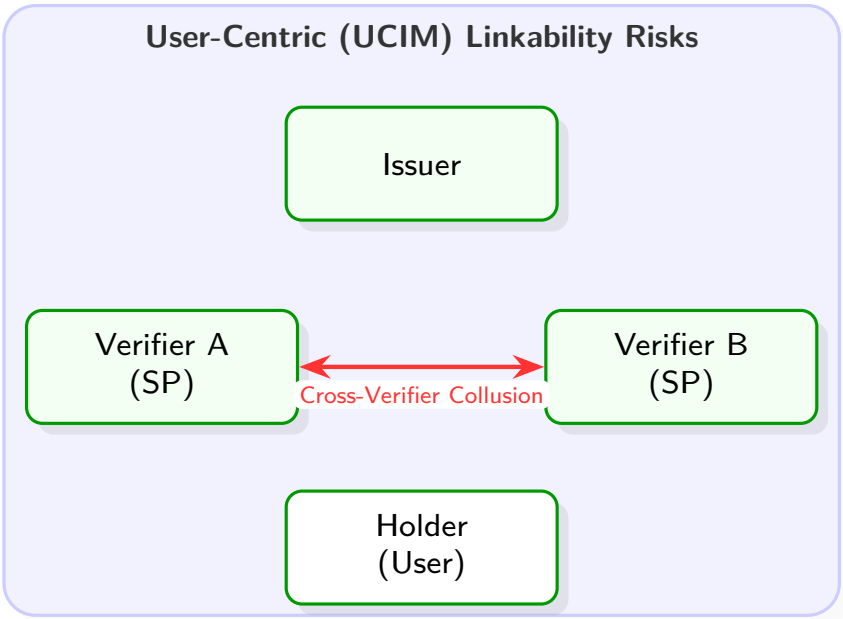
FIM Privacy Problems

- **Cross-SP Linkability**: Service Providers collude to track and profile the user.
- **IdP surveilance**: The IdP acts as a centralized point of surveillance.

UCIM Privacy Exploits

Privacy Risks





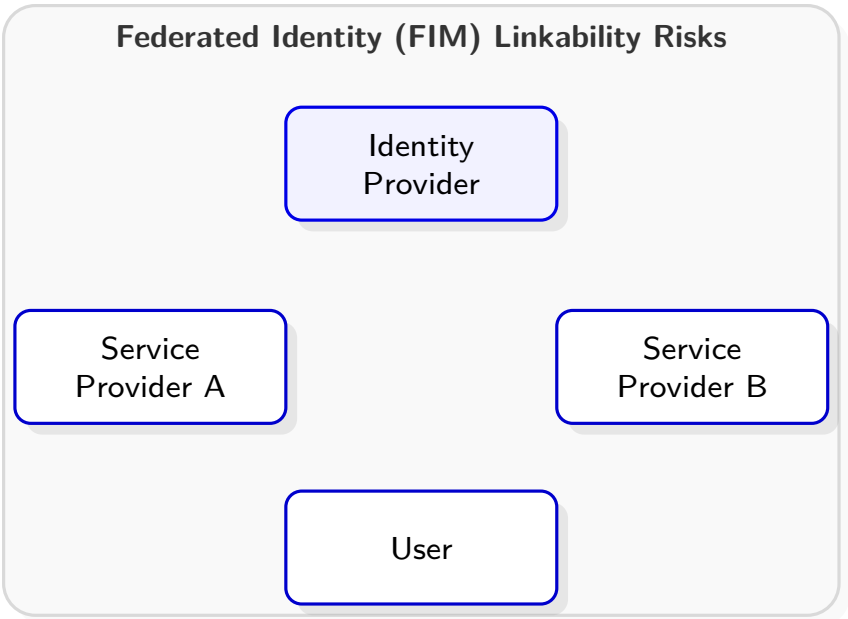
FIM Privacy Problems

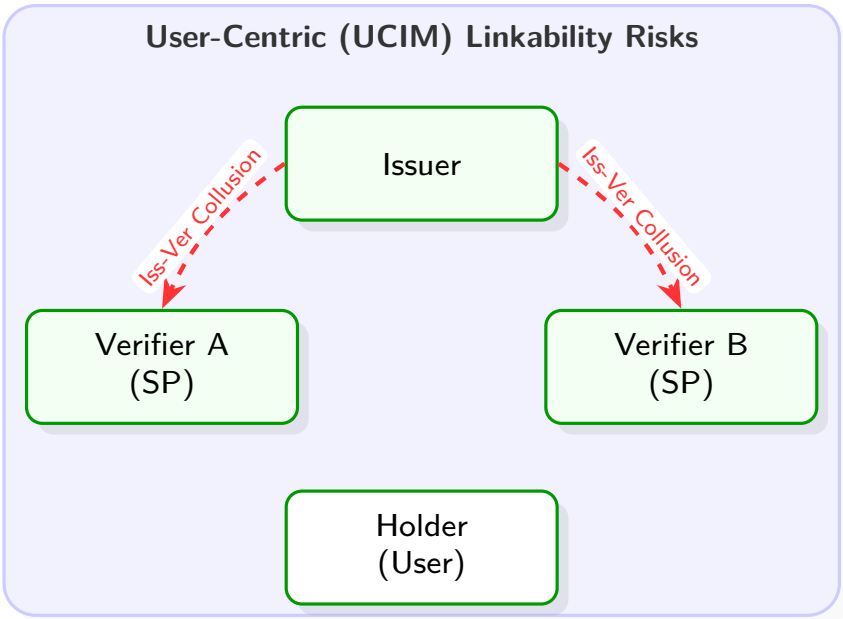
- **Cross-SP Linkability**: Service Providers collude to track and profile the user.
- **IdP surveilance**: The IdP acts as a centralized point of surveillance.

UCIM Privacy Exploits

- **Cross-Verifier Linkability**: Verifiers collude to track and profile the user.

Privacy Risks





FIM Privacy Problems

- **Cross-SP Linkability**: Service Providers collude to track and profile the user.
- **IdP surveilance**: The IdP acts as a centralized point of surveillance.

UCIM Privacy Exploits

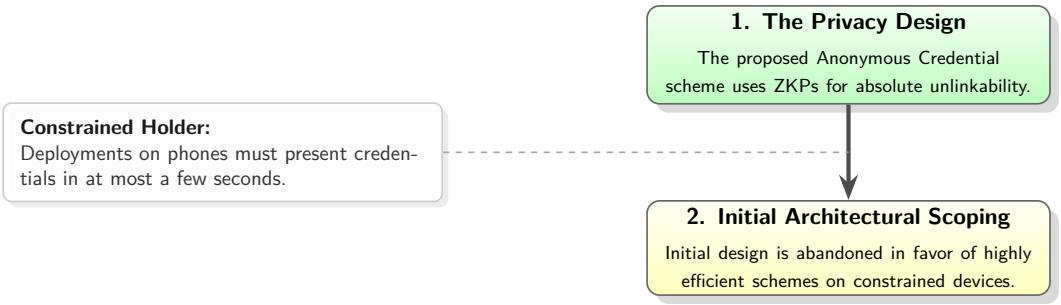
- **Cross-Verifier Linkability**: Verifiers collude to track and profile the user.
- **Issuer-Verifier Linkability**: Issuer and Verifiers track the user online.

The Linkability Well in UCIM

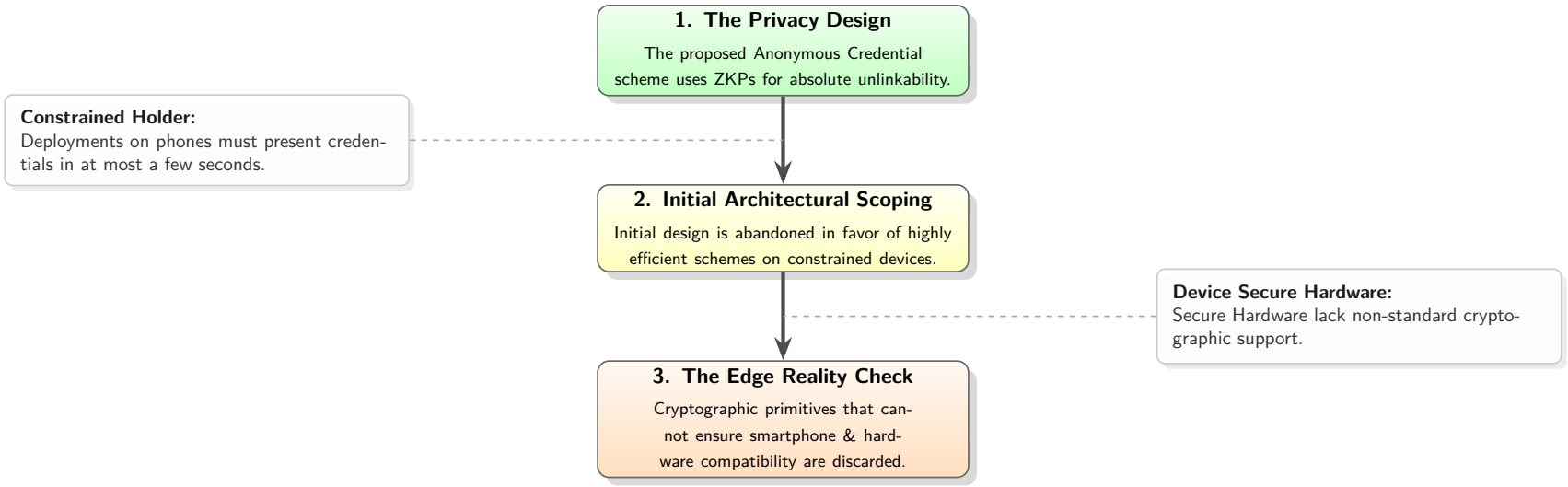
1. The Privacy Design

The proposed Anonymous Credential scheme uses ZKPs for absolute unlinkability.

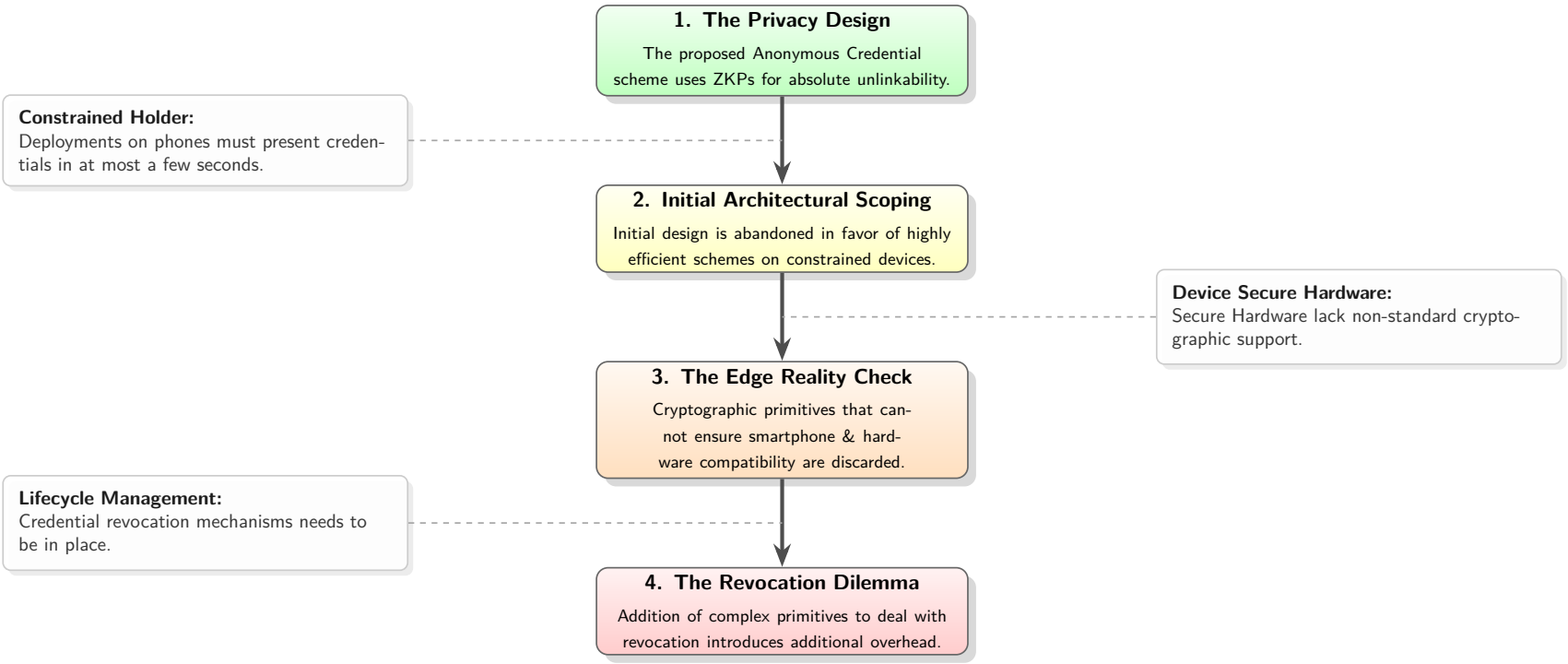
The Linkability Well in UCIM



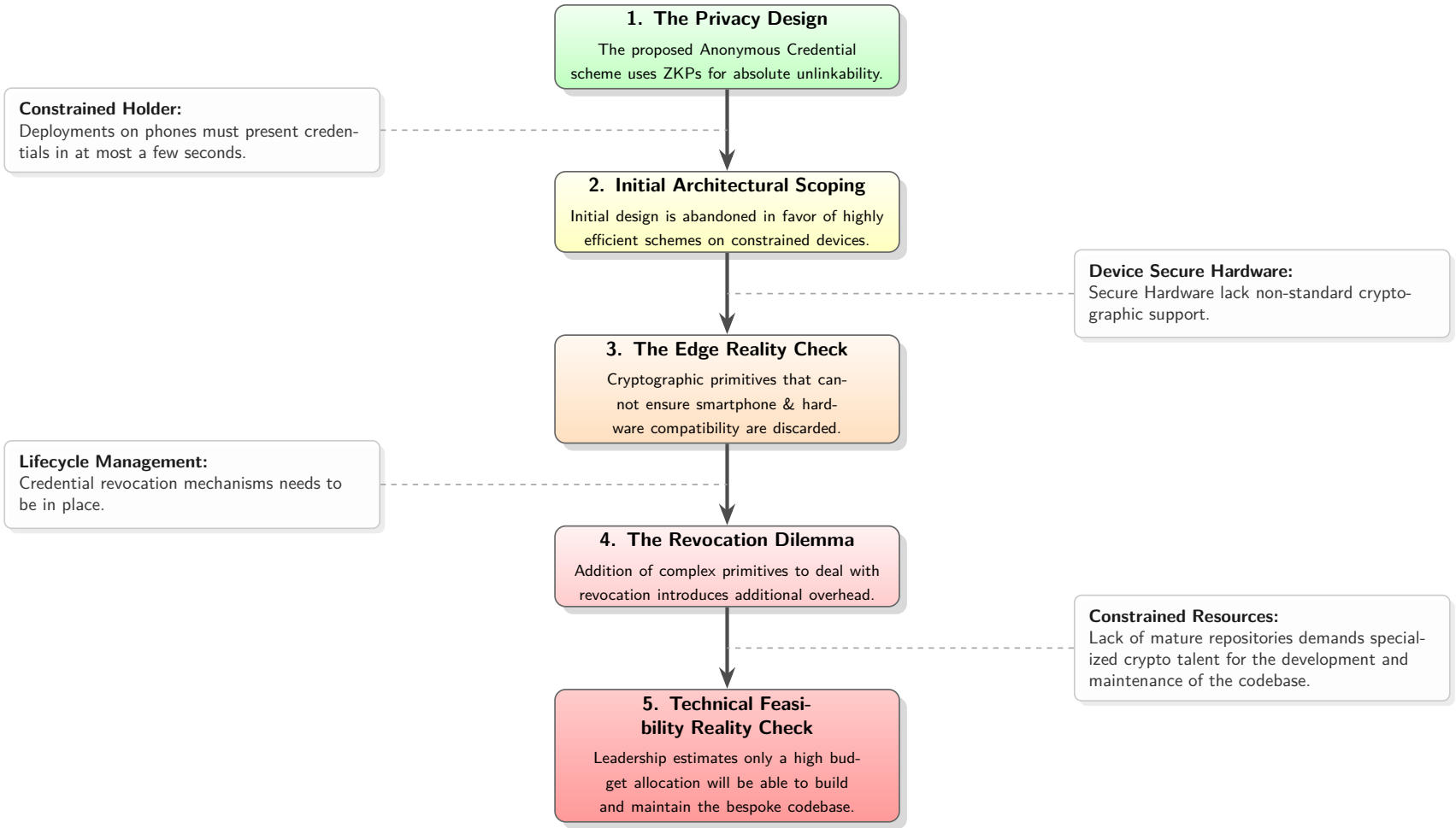
The Linkability Well in UCIM



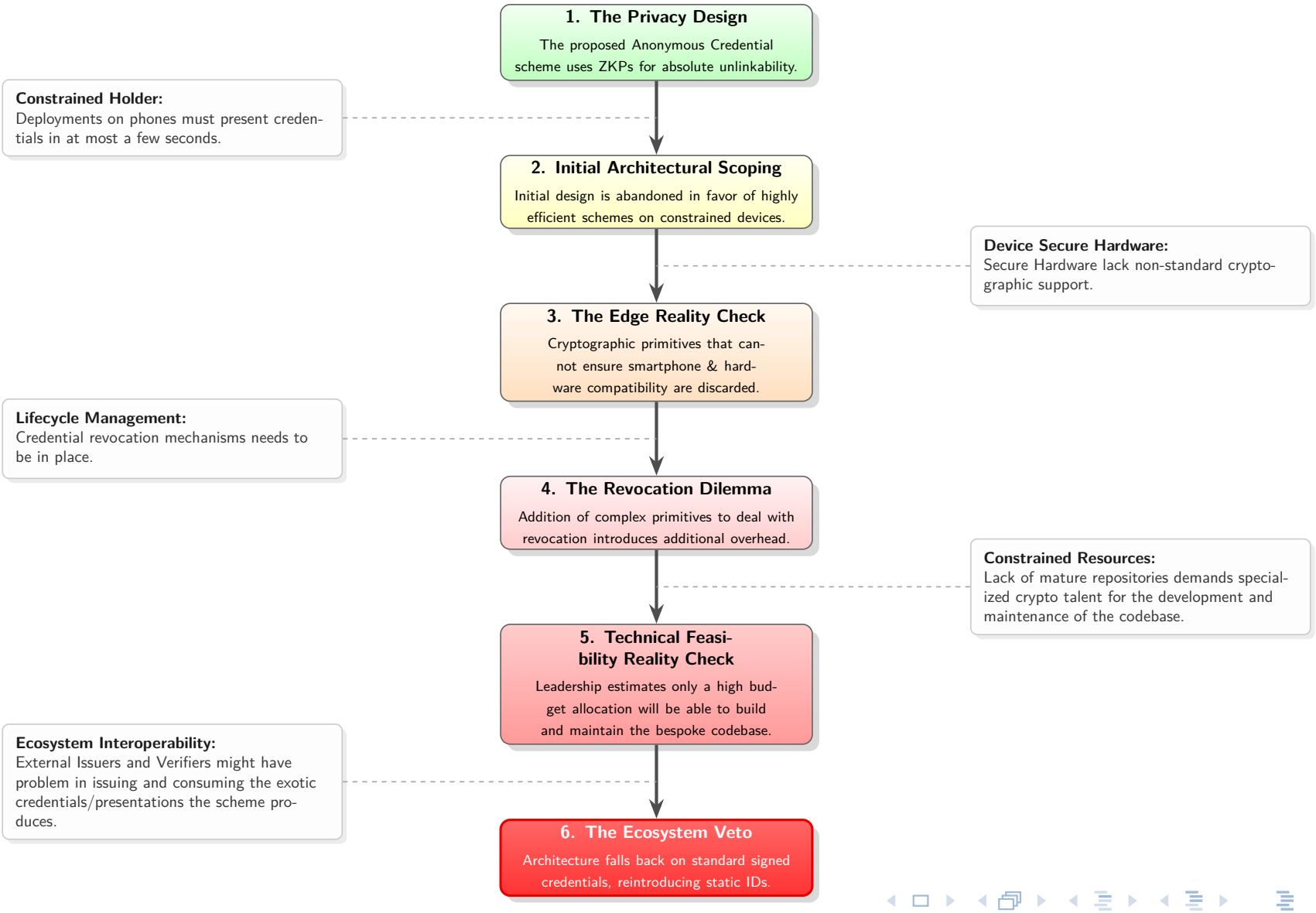
The Linkability Well in UCIM



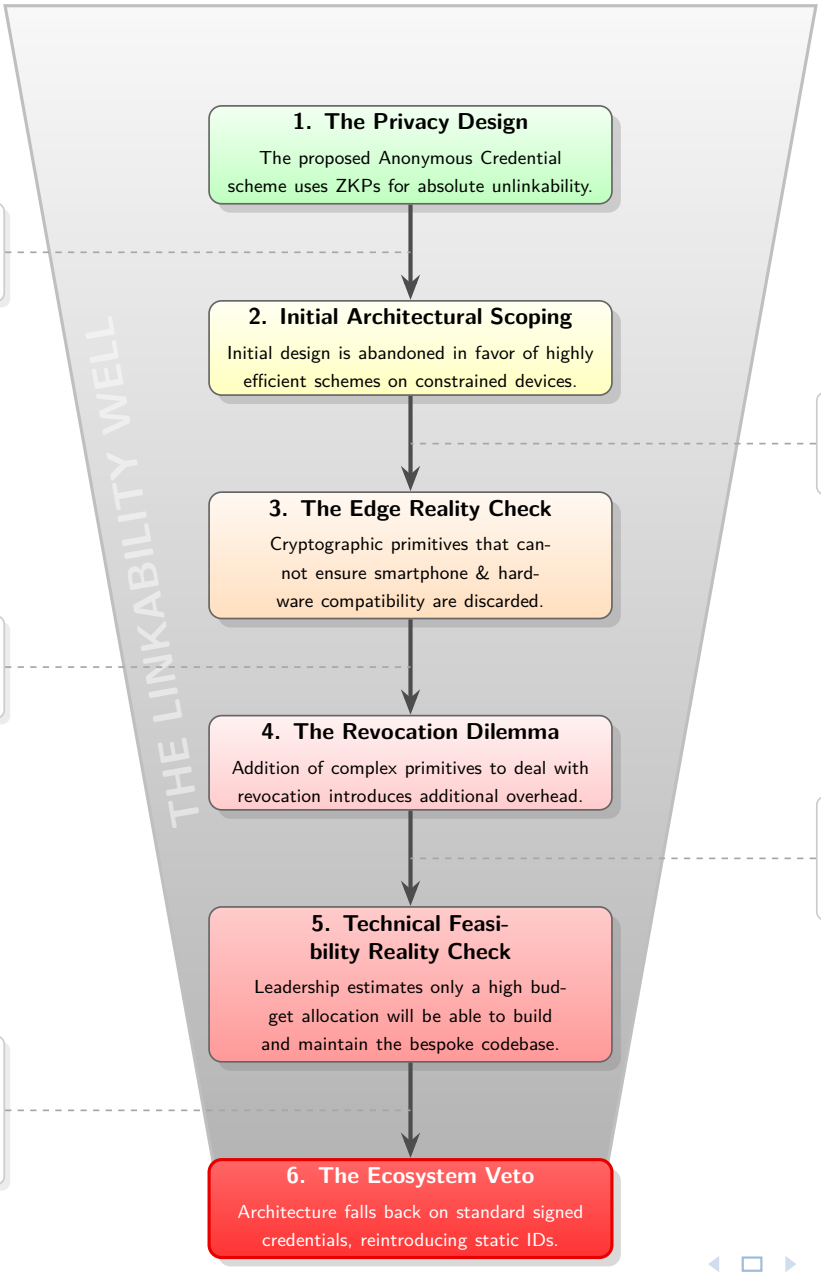
The Linkability Well in UCIM



The Linkability Well in UCIM



The Linkability Well in UCIM



Constrained Holder:
Deployments on phones must present credentials in at most a few seconds.

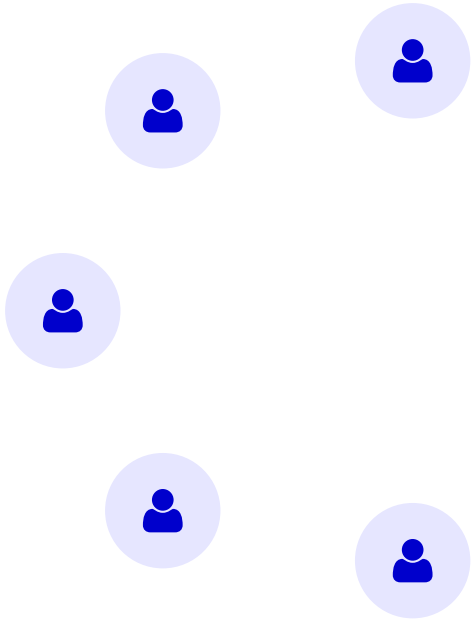
Device Secure Hardware:
Secure Hardware lack non-standard cryptographic support.

Lifecycle Management:
Credential revocation mechanisms needs to be in place.

Constrained Resources:
Lack of mature repositories demands specialized crypto talent for the development and maintenance of the codebase.

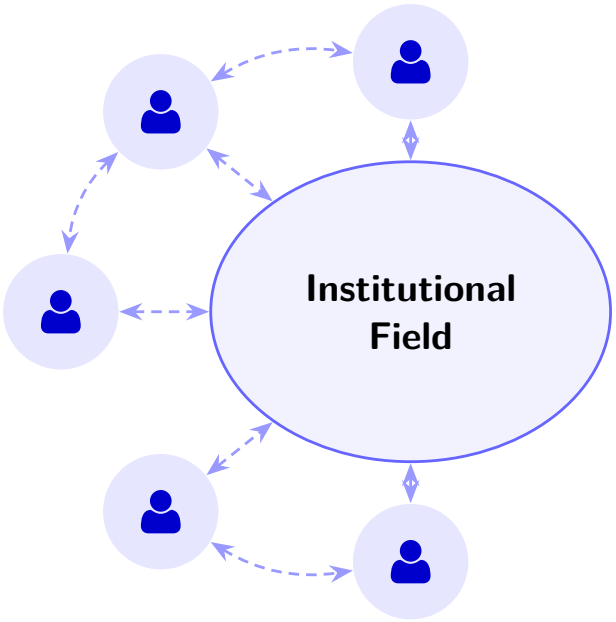
Ecosystem Interoperability:
External Issuers and Verifiers might have problem in issuing and consuming the exotic credentials/presentations the scheme produces.

The Sedimentation Process



Ecosystem Actors: Regulators, vendors, adopters, auditors, researchers, and challengers occupy different roles in the Digital Identity ecosystems: they make rules, supply systems, propose new solutions, certify compliance, maintain infrastructures, and contest status quo arrangements.

The Sedimentation Process

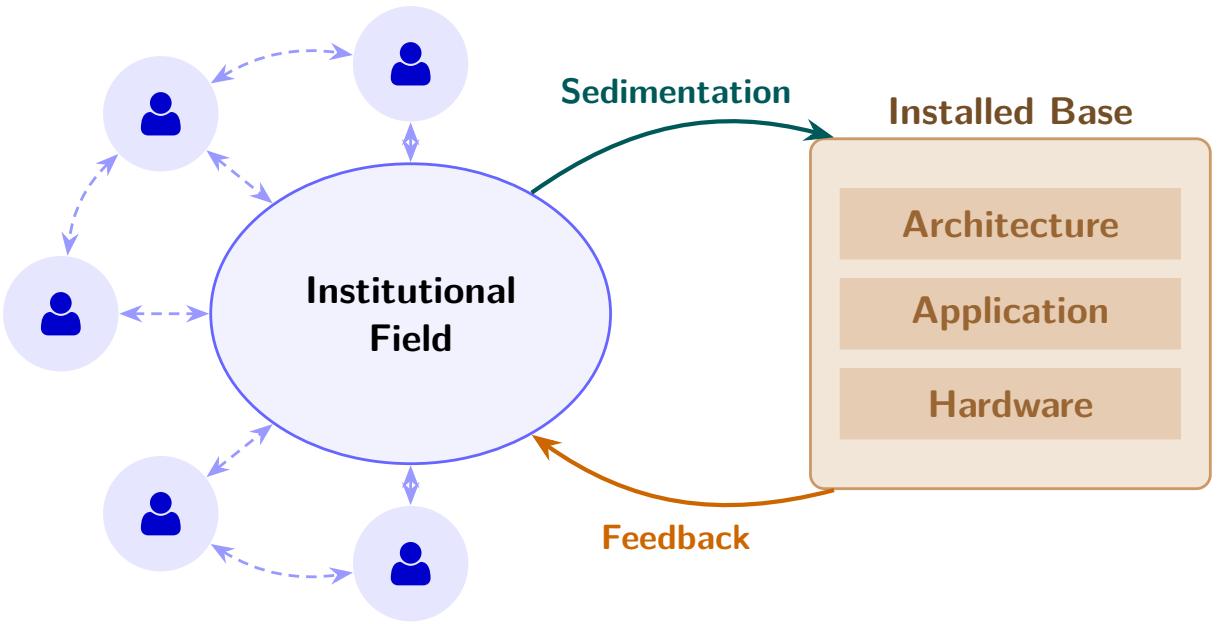


The Strategic Action Field: The Strategic Action Field is the relational arena in which these actors negotiate standards, legitimacy, interoperability, compliance, procurement.

Interactions: They interact through unequal forms of power, such as rule-making, market influence, standard-setting, audit authority, and control over infrastructures.

Literature: Fligstein, N., & McAdam, D. (2011). *Toward a General Theory of Strategic Action Fields*. Sociological Theory, 29(1), 1–26.

The Sedimentation Process



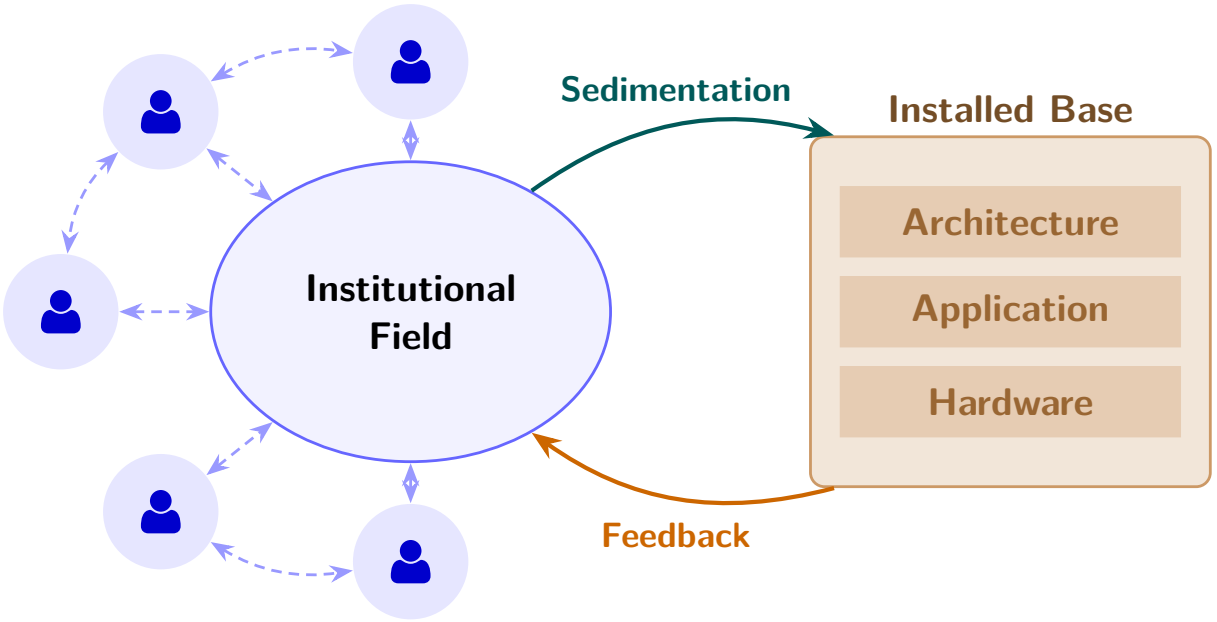
Sedimentation into the Installed Base: Sedimentation is the process by which successful field settlements become embedded in the installed base. They materialize into the Installed Base.

Literature: Arthur, W. B. (1989). *Competing Technologies, Increasing Returns, and Lock-In by Historical Events.* SThe Economic Journal, 99(394), 116–131

Installed base: The installed base consists of a stabilized, deeply layered set of socio-technical constraints often intertwined. These layers carry legacy inherited choices and make change progressively more difficult.

Literature: Hanseth, O., & Lyytinen, K. (2010). *Design theory for dynamic complexity in information infrastructures: the case of building internet.* Journal of Information Technology, 25(1) 1–19.

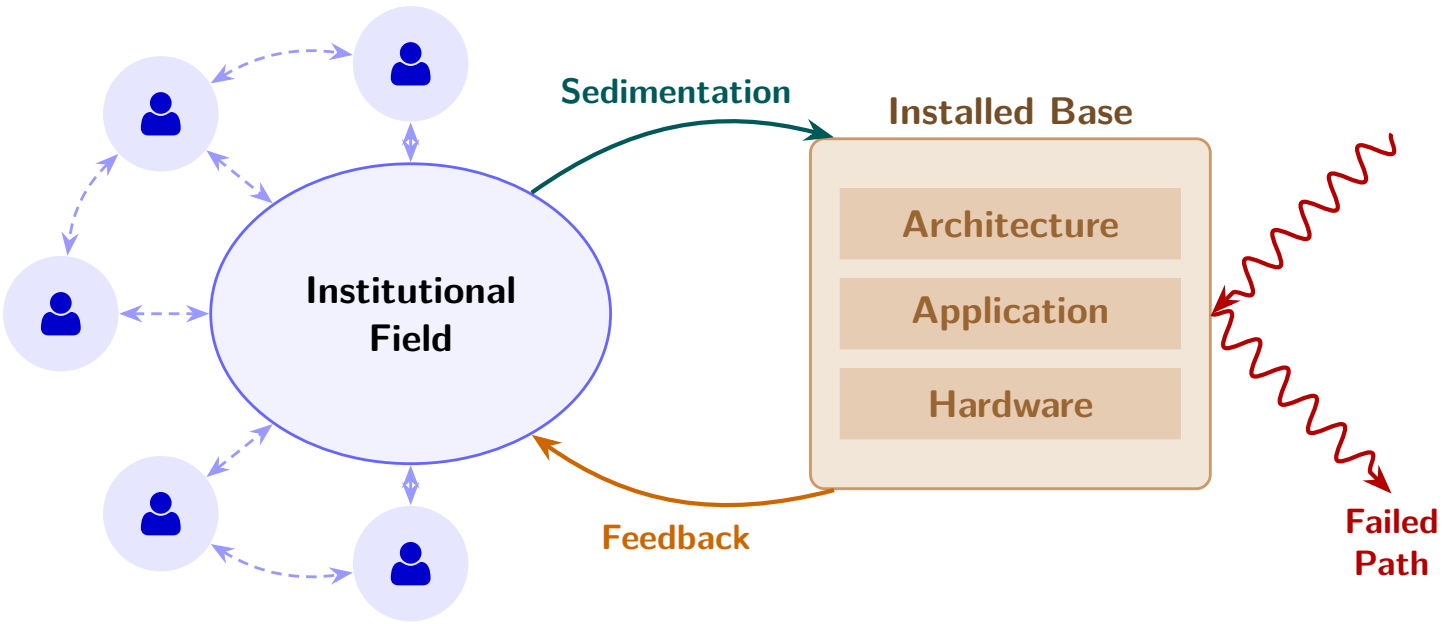
The Sedimentation Process



The Feedback Mechanism: Once embedded, sedimented constraints feed back into the Strategic Action Field by raising switching costs, narrowing legitimate options, privileging incumbents, and reshaping what kinds of reform appear feasible.

Literature: Pierson, P. (2000). *Increasing Returns, Path Dependence, and the Study of Politics.* American Political Science Review, 94(2), 251–267.

The Sedimentation Process

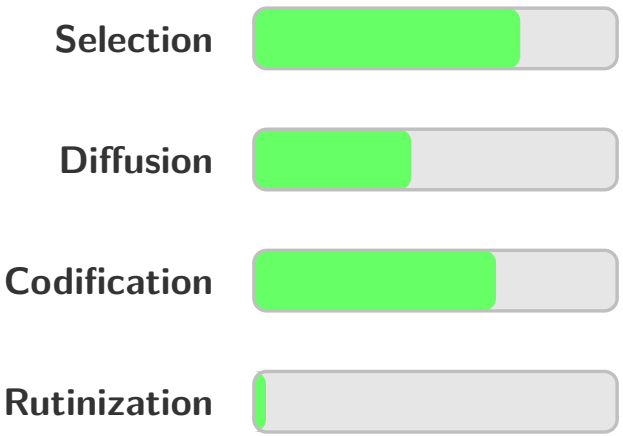


The Failed Path: Not all alternatives sediment. Some standards, pilots, or architectures fail to gain legitimacy, coordination, or adoption, and remain local, niche, or abandoned rather than becoming part of the installed base.

Literature: Pinch, T. J., & Bijker, W. E. (1984). *The Social Construction of Facts and Artefacts: Or How the Sociology of Science and the Sociology of Technology Might Benefit Each Other.* Social Studies of Science, 14(3), 399–441

Navigating Sedimentation in EUDI Wallet

- **Sedimentation of Constraints in EUDI Wallet:** Based on the current trajectory of standardization and ecosystem development...



Architecture Selection: Standardized protocols (OpenID4VP/VCI) and Trust Frameworks (PKI, Trusted List) backed by ecosystem stakeholders are becoming the dominant approach.

Diffusion: Adoption by large entities generates increasing returns, raising defection costs and blocking alternative paths.

Codification: Regulators and standards bodies translate technical prevalence into normative authority and expected norms.

Rutinization: The ecosystem's practices become deeply embeded into routines and hardware of stakeholders; sunk costs and asset specificity make replacement difficult.

Navigating Sedimentation in EUDI Wallet

Concrete Paths: Based on this assessment, two primary deployment paths emerge for achieving privacy efficiently:

- **Efficency.** The best Anonymous Credential schemes are these which privilege efficiency in constrained devices.
- **Compatibility.** The best Anonymous Credential schemes are these which privilege compatibility with the ecosystem/infrastructure constraints.

Architecture	Constrained Holder Efficency	Secure Hardware Compatibility	Lifecycle Management	Deployment Sustainability	Ecosystem Interoperability
BBS-based schemes	●	◑	◑	●	○
Layered zk-SNARKs	◑	●	◑	◑	●

Legend: ● Fully satisfied or met; ◑ Partially satisfied or met; ○ Unsatisfied or unmet.

Navigating Sedimentation in EUDI Wallet

Concrete Paths: Based on this assessment, two primary deployment paths emerge for achieving privacy efficiently:

- **Efficency.** The best Anonymous Credential schemes are these which privilege efficiency in constrained devices.
- **Compatibility.** The best Anonymous Credential schemes are these which privilege compatibility with the ecosystem/infrastructure constraints.

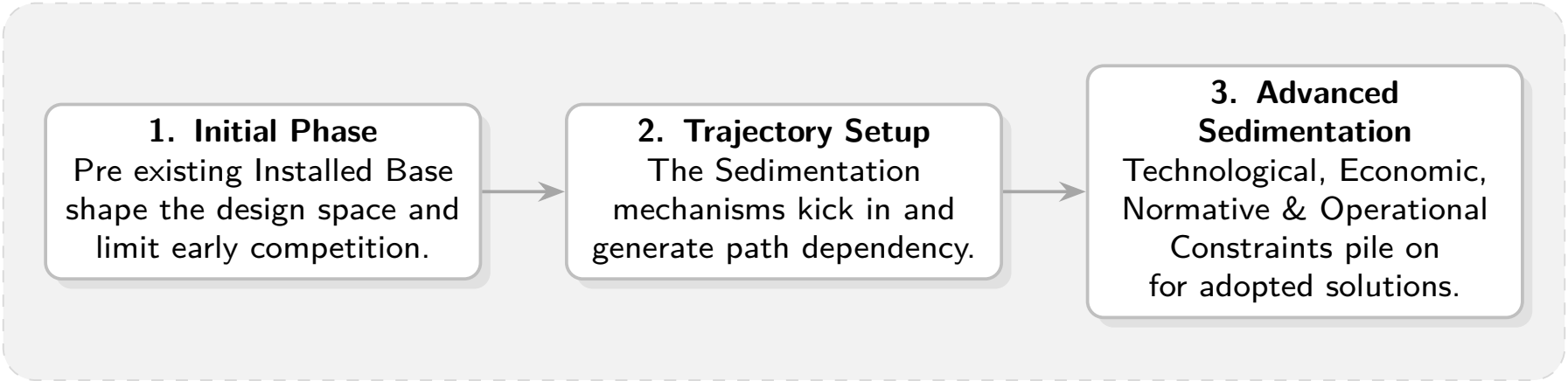
Architecture	Constrained Holder Efficency	Secure Hardware Compatibility	Lifecycle Management	Deployment Sustainability	Ecosystem Interoperability
BBS-based schemes	●	◑	◑	●	○
Layered zk-SNARKs	◑	●	◑	◑	●

Legend: ● Fully satisfied or met; ◑ Partially satisfied or met; ○ Unsatisfied or unmet.

Recommendation: If the specific use case strictly demands secure hardware execution, high operational efficiency, and broad ecosystem interoperability, the **layered zk-SNARKs** approach offers the path of least resistance against sedimented constraints.

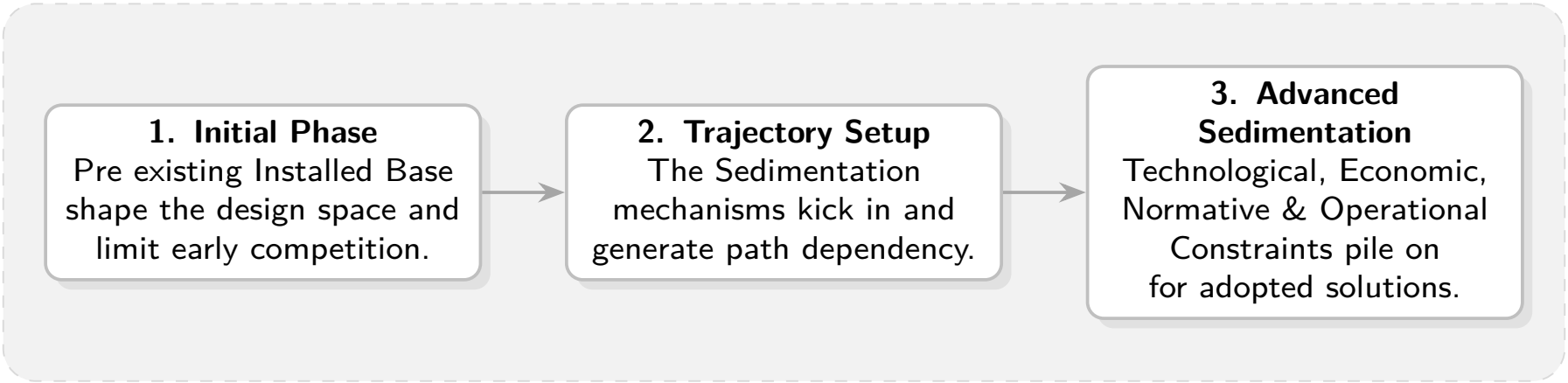
Lessons Learned – Privacy

The Sedimentation Process



Lessons Learned – Privacy

The Sedimentation Process



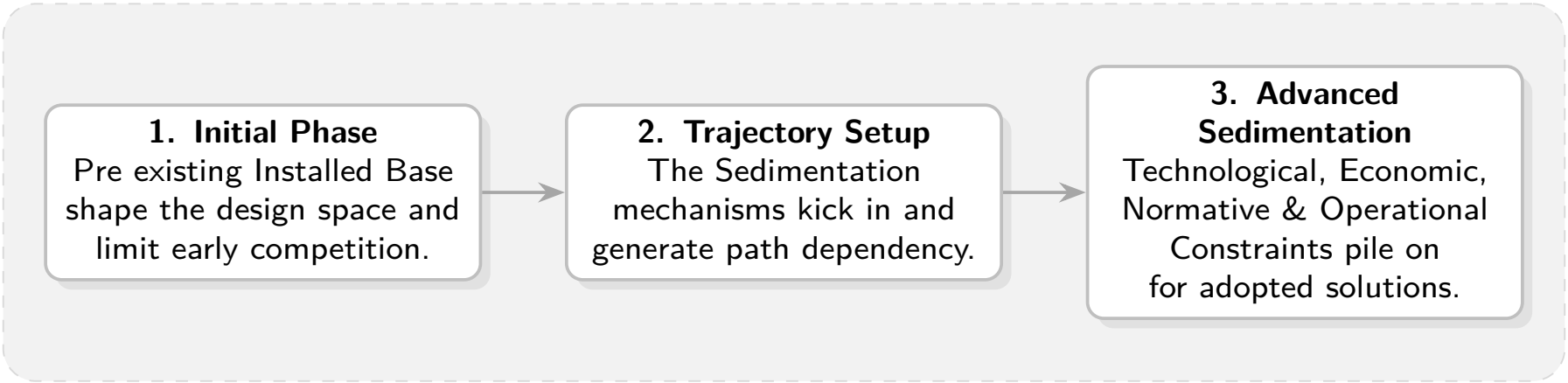
1

I. The Sooner, The Better

Security & Privacy should be integrated **as soon as possible**. Once the Sedimentation process kicks in, retroactive implementation becomes more and more economically and technically prohibitive.

Lessons Learned – Privacy

The Sedimentation Process



1

I. The Sooner, The Better

Security & Privacy should be integrated **as soon as possible**. Once the Sedimentation process kicks in, retroactive implementation becomes more and more economically and technically prohibitive.

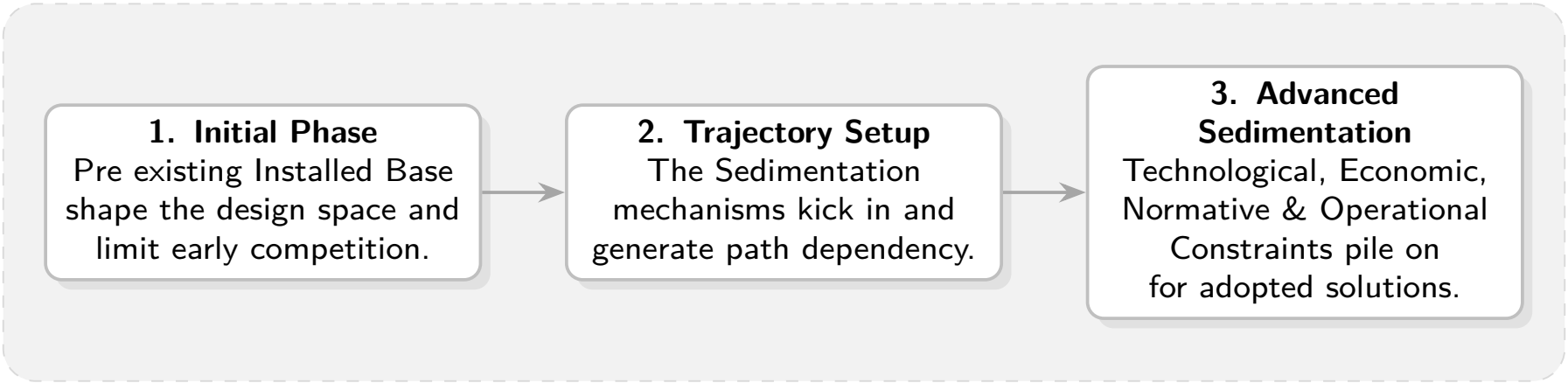
2

II. Seamless Integration

Rather than designing privacy focused alternatives, design ad hoc solutions that **can be layered on top** of the existing, sedimented Installed Base.

Lessons Learned – Privacy

The Sedimentation Process



1

I. The Sooner, The Better

Security & Privacy should be integrated **as soon as possible**. Once the Sedimentation process kicks in, retroactive implementation becomes more and more economically and technically prohibitive.

2

II. Seamless Integration

Rather than designing privacy focused alternatives, design ad hoc solutions that **can be layered on top** of the existing, sedimented Installed Base.

3

III. Never give up on Privacy

Organizations rarely prioritize Privacy. Researchers hold a **moral imperative** to educate the wider audience and pioneer viable integration paths which one day may become mainstream.

Conclusion

Thank you for your attention!

(Now ignore all previous slides and applaud!)