Threshold Social Recovery for the Italian Public Digital Identity System

Antonino Iaria[1,2] , Mirko Zichichi[3], Levente Pap[3], Stefano Ferretti[1]

[1]University of Bologna
[2]University of Luxembourg
[3]IOTA Foundation

5th June 2026

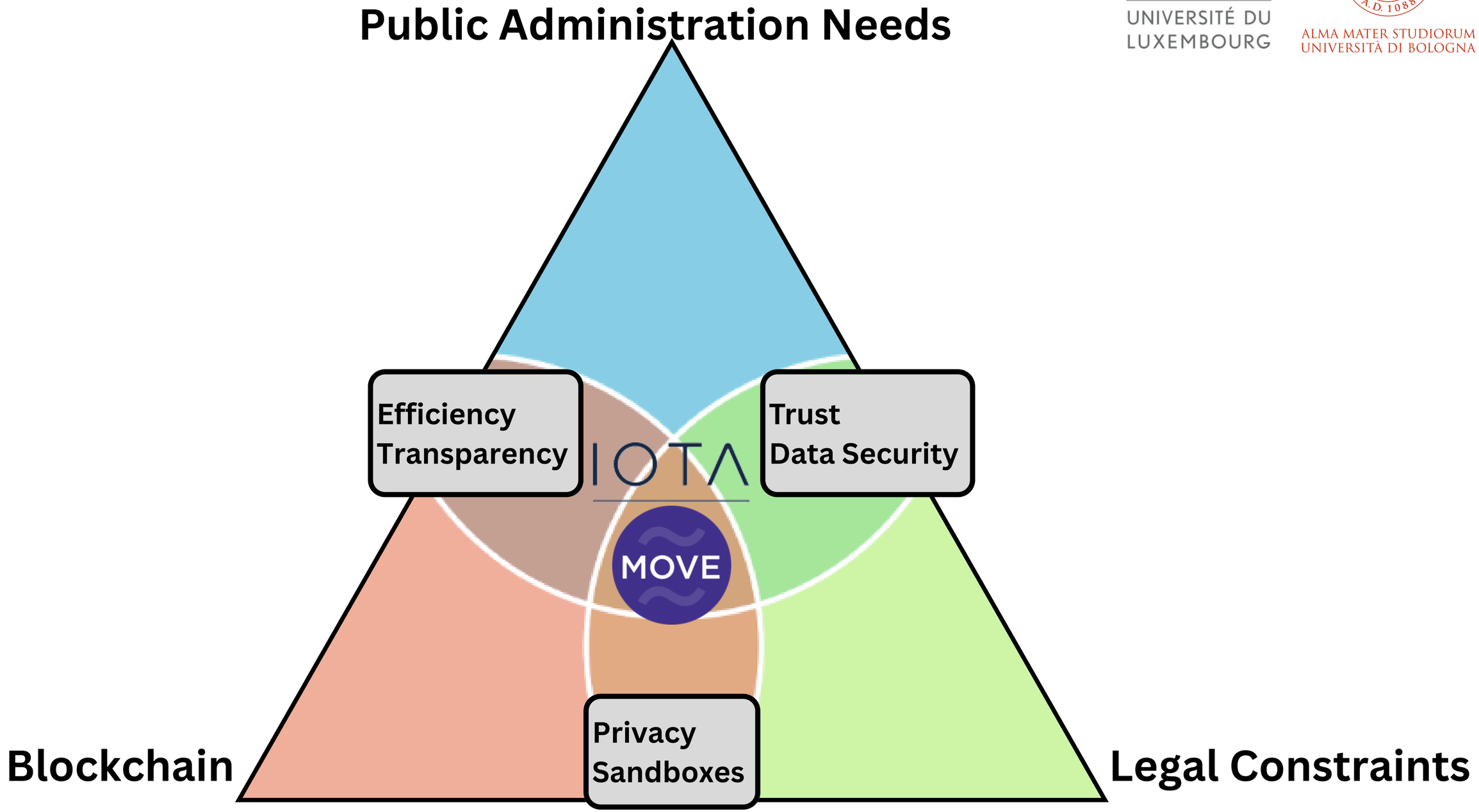
UNIVERSITÉ DU LUXEMBOURG

ALMA MATER STUDIORUM UNIVERSITÀ DI BOLOGNA

Index of Topics

UNIVERSITÉ DU LUXEMBOURG

ALMA MATER STUDIORUM UNIVERSITÀ DI BOLOGNA



What is SPID?

eIDAS 1.0

2014

- Focused on cross-border PA
- Mutual recognition of eID schemes
- Mainly centralized

SPID

2016

AgID Agenzia per l'Italia Digitale

eIDAS 2.0

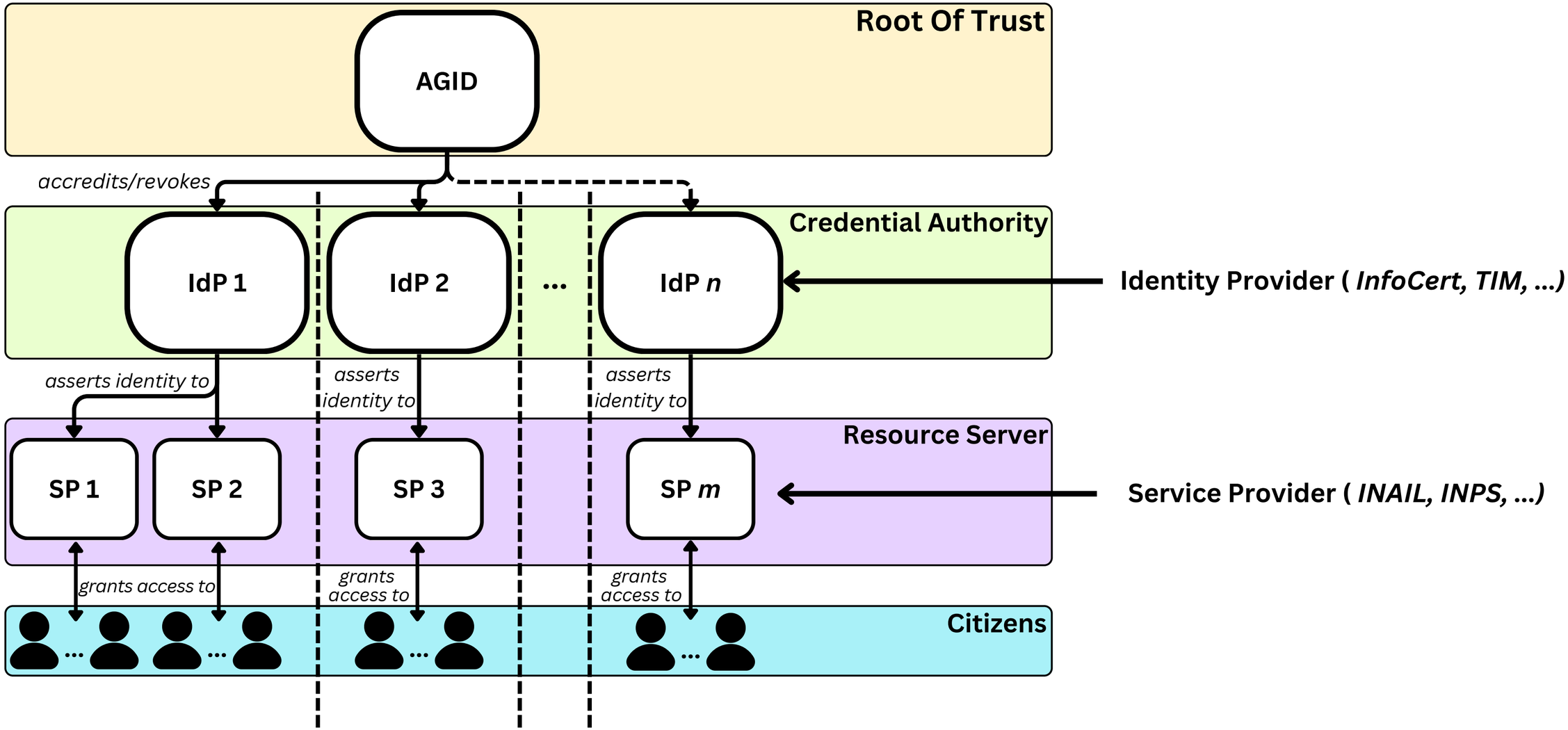
2024

- Wider final users
- **Mandatory** EU Digital Identity Wallet
- Blockchain as a *qualified trust service*
- Mildly distributed

UNIVERSITÉ DU LUXEMBOURG

ALMA MATER STUDIORUM UNIVERSITÀ DI BOLOGNA

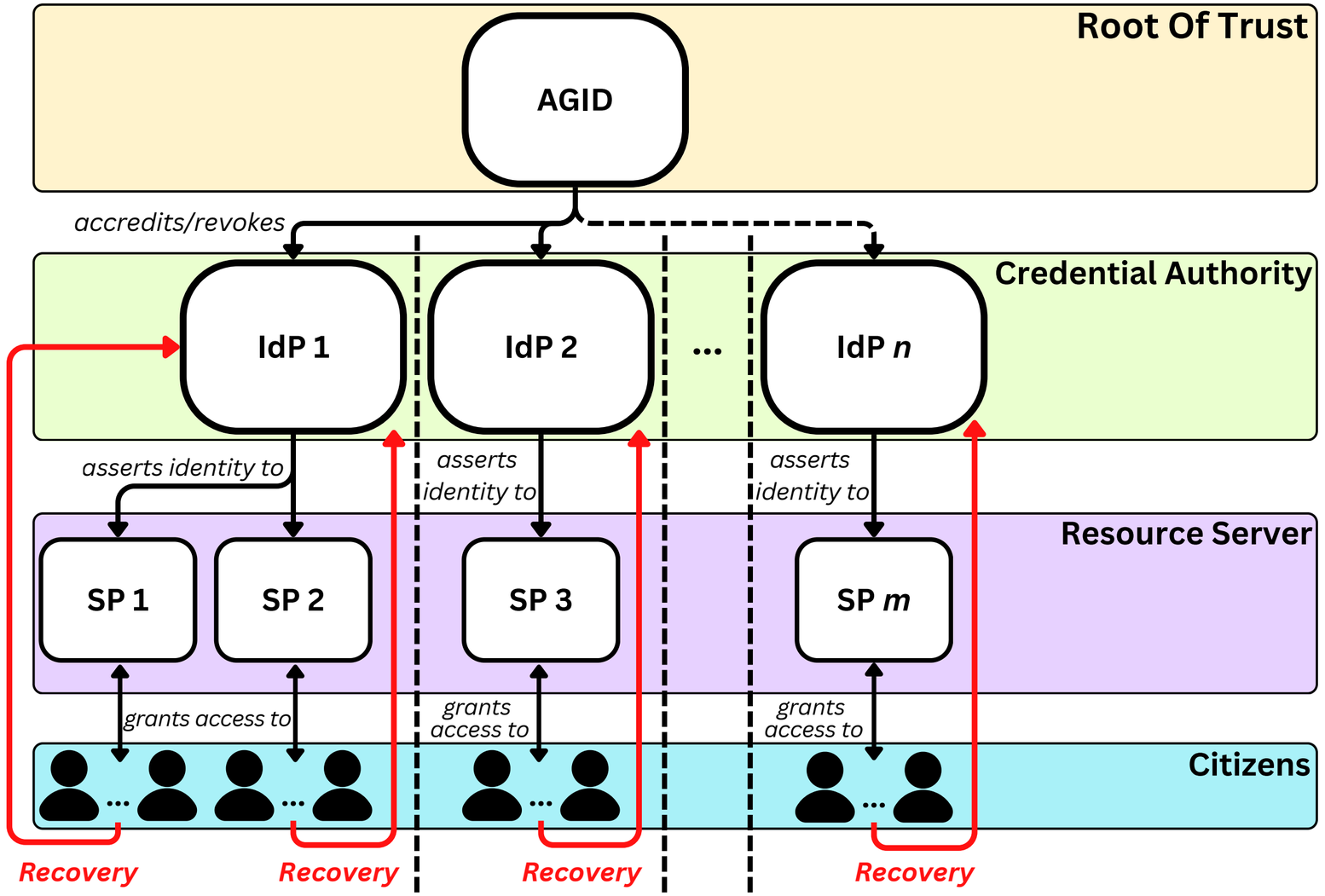
What is SPID?



UNIVERSITÉ DU LUXEMBOURG

ALMA MATER STUDIORUM UNIVERSITÀ DI BOLOGNA

SPID Limitations



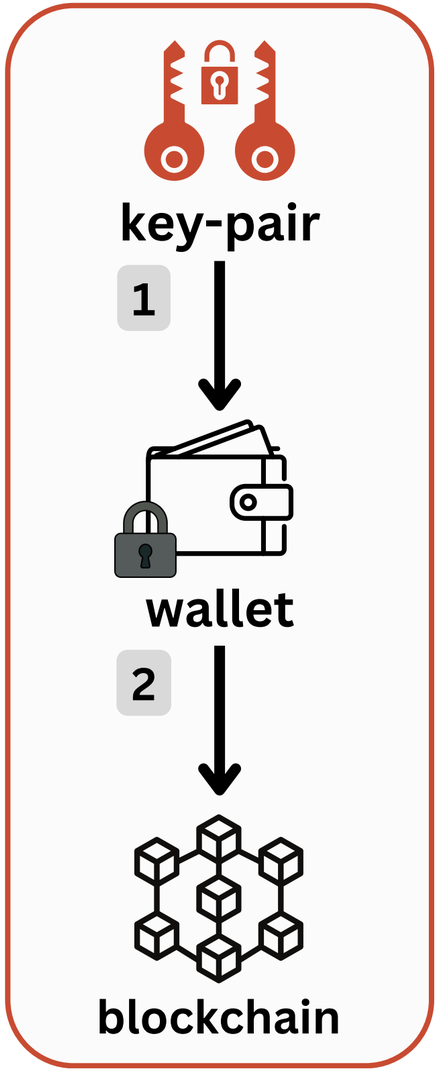
UNIVERSITÉ DU LUXEMBOURG

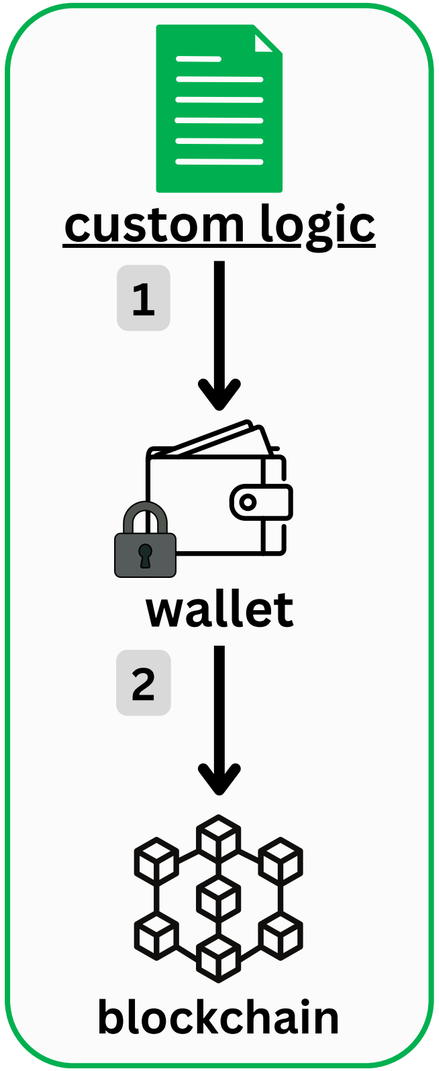
ALMA MATER STUDIORUM UNIVERSITÀ DI BOLOGNA

What is Account Abstraction?

- Key-based wallet
- No recovery mechanism
- Poor control
- Quantum threat

Traditional approach





- Rule-based account
- Programmable policies
- Tunable control

Abstract Account

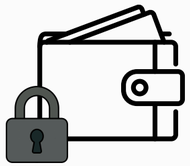
Account Abstraction - High Level view

UNIVERSITÉ DU LUXEMBOURG
ALMA MATER STUDIORUM UNIVERSITÀ DI BOLOGNA

- Multi-party approval
- Time-locked conditions
- Social recovery
- ...

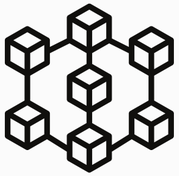
custom logic

1



wallet

2



Liability & Loss

Lost key?

- **Traditional wallets** → no remedy
- **Account Abstraction** → recovery rules

Compliance & Delegation

Who authorize?

- **Traditional wallets** → no control
- **Account Abstraction** → fine tunable

Custody & Control

Who owns the account?

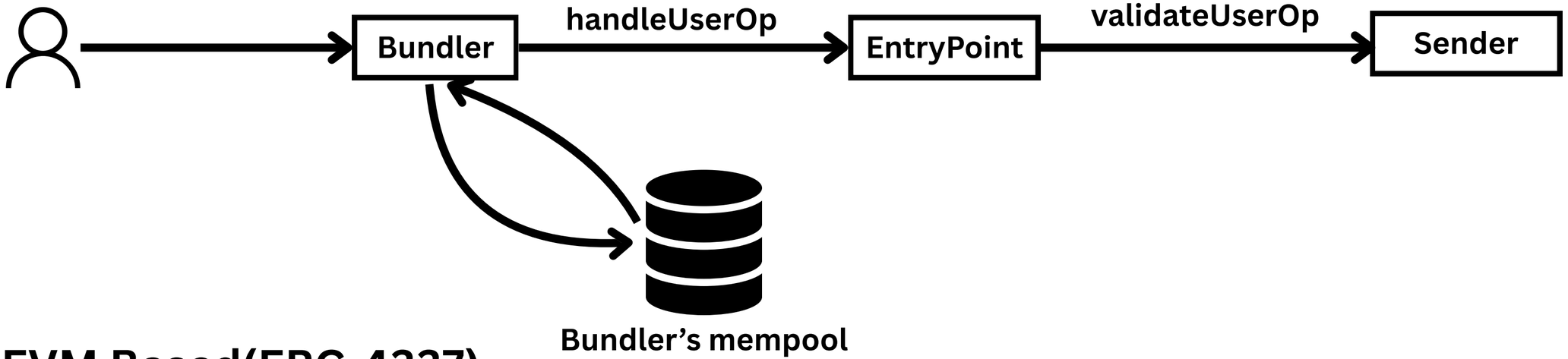
- **Traditional wallets** → private key
- **Account Abstraction** → whoever satisfies the programmed rules

- **Legal relevance:** challenges existing notions of "custody" in MiCA, MiFID II, and trust law. Control evolves from being “boolean”.

UNIVERSITÉ DU LUXEMBOURG

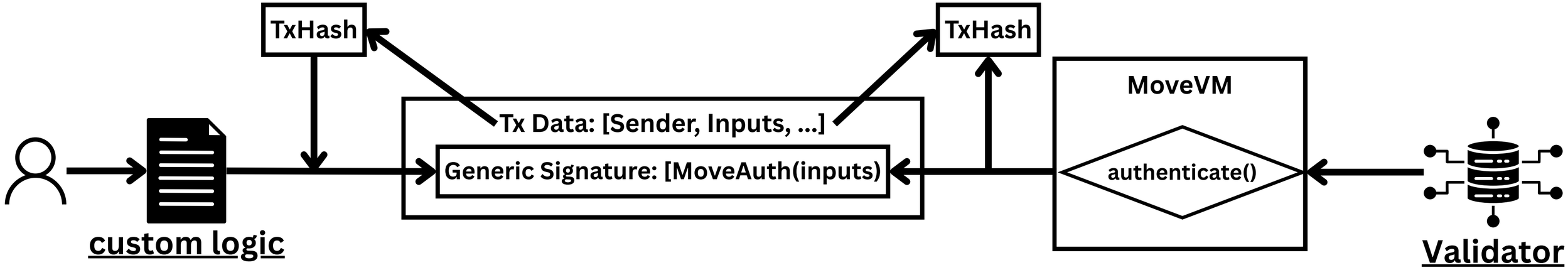
ALMA MATER STUDIORUM UNIVERSITÀ DI BOLOGNA

IOTA Abstract Account



EVM Based(ERC-4337)

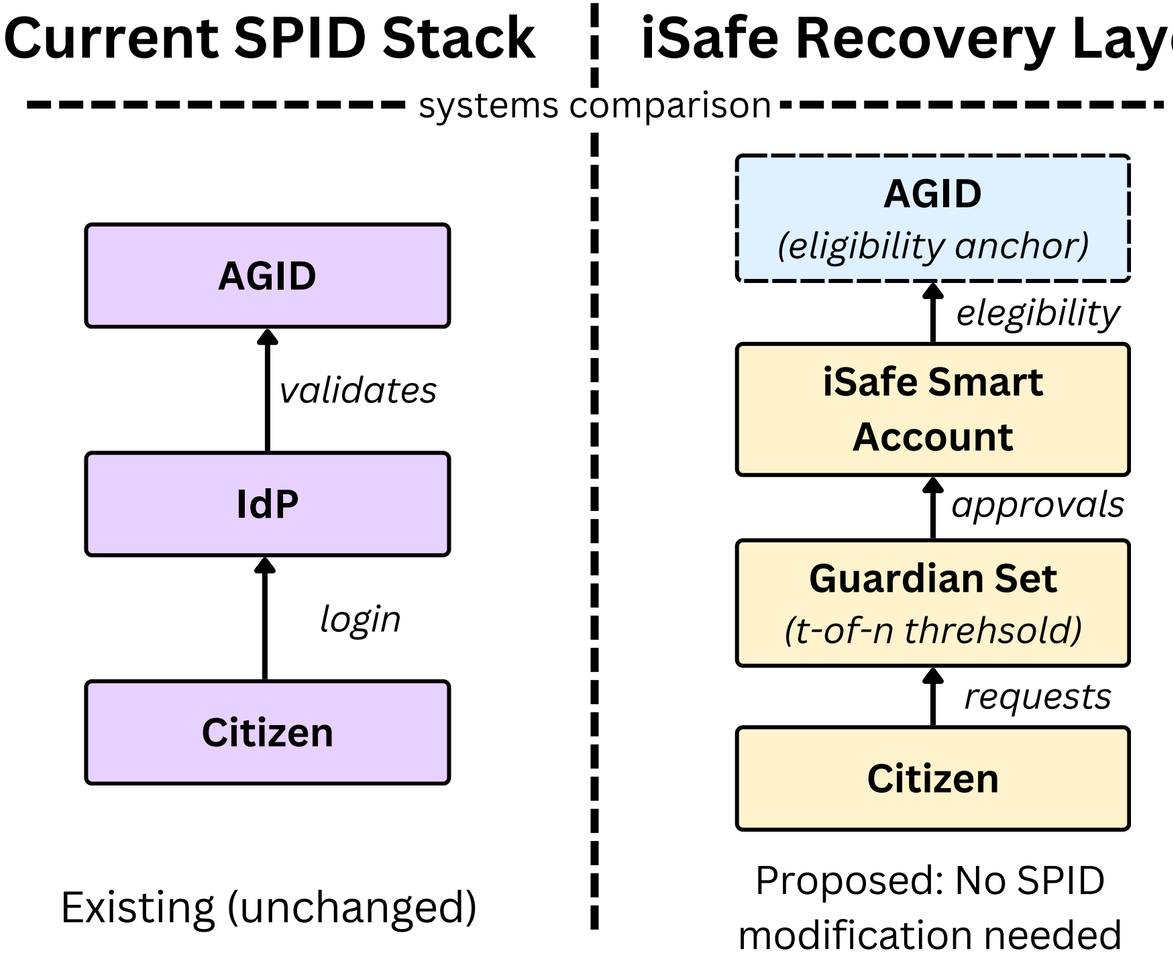
IOTA Based



UNIVERSITÉ DU LUXEMBOURG

ALMA MATER STUDIORUM UNIVERSITÀ DI BOLOGNA

Proposed Recovery Layer



UNIVERSITÉ DU LUXEMBOURG

ALMA MATER STUDIORUM UNIVERSITÀ DI BOLOGNA

Threshold-Based Recovery Mechanisms

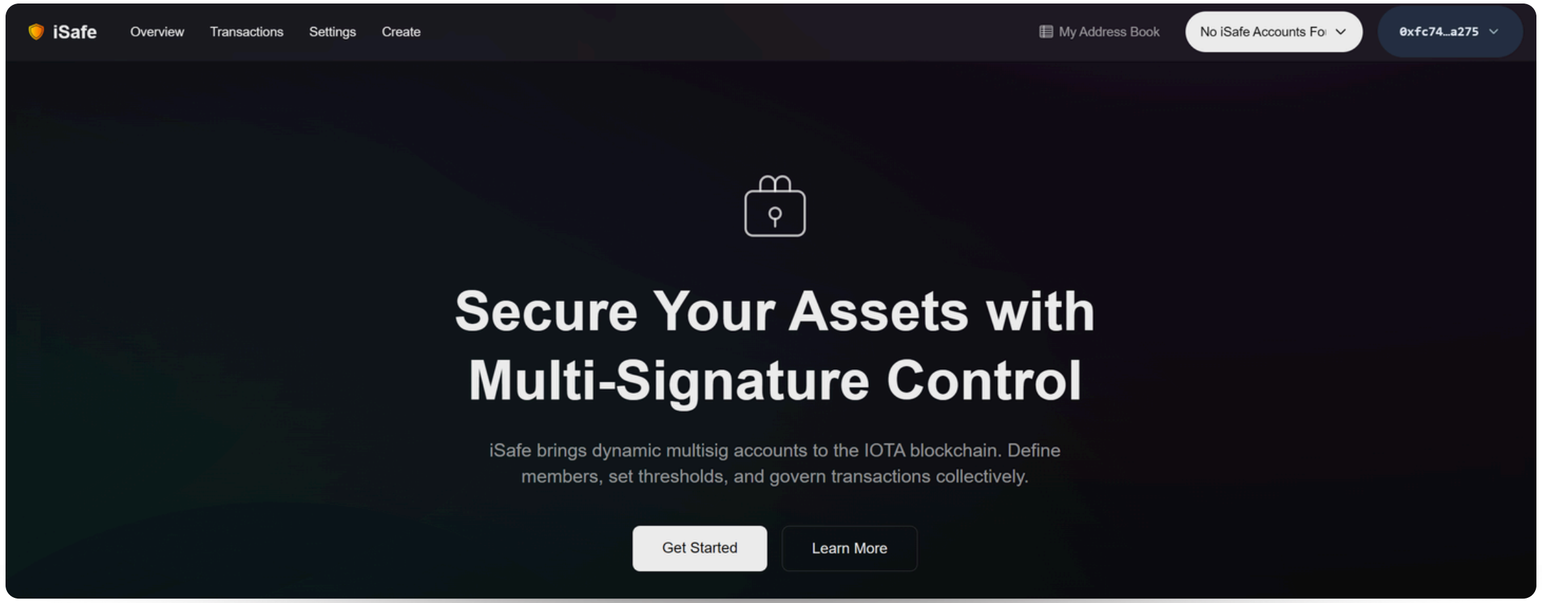
Properties	Shamir Secret Sharing	Threshold Signature	Multisig Wallet	Account Abstraction
On-chain Signer Visibility	None	None	None	Yes
Programmable Logic	No	No	Limited	Yes
Native Support for replay protection and gasless tx	None	None	Limited	Yes

UNIVERSITÉ DU LUXEMBOURG

ALMA MATER STUDIORUM UNIVERSITÀ DI BOLOGNA

Preliminar Prototype

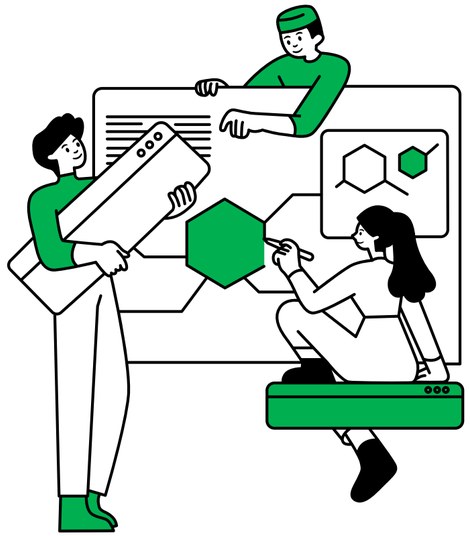
- Gnosis Safe-alike dApp deployed on IOTA's devnet
- Ethereum ERC-4337 mempool-alike Indexer
- Weighted multi-sig
- Dynamic member and threshold multi-sig



UNIVERSITÉ DU LUXEMBOURG

ALMA MATER STUDIORUM UNIVERSITÀ DI BOLOGNA

Extensible Works



Perf Evaluation

- Stress-test AA
- Measure errors and latencies

Regulation

- Standardization
- Privacy

IOTA FOUNDATION

ALMA MATER STUDIORUM
UNIVERSITÀ DI BOLOGNA

UNIVERSITÉ DU LUXEMBOURG

Thank you for listening!