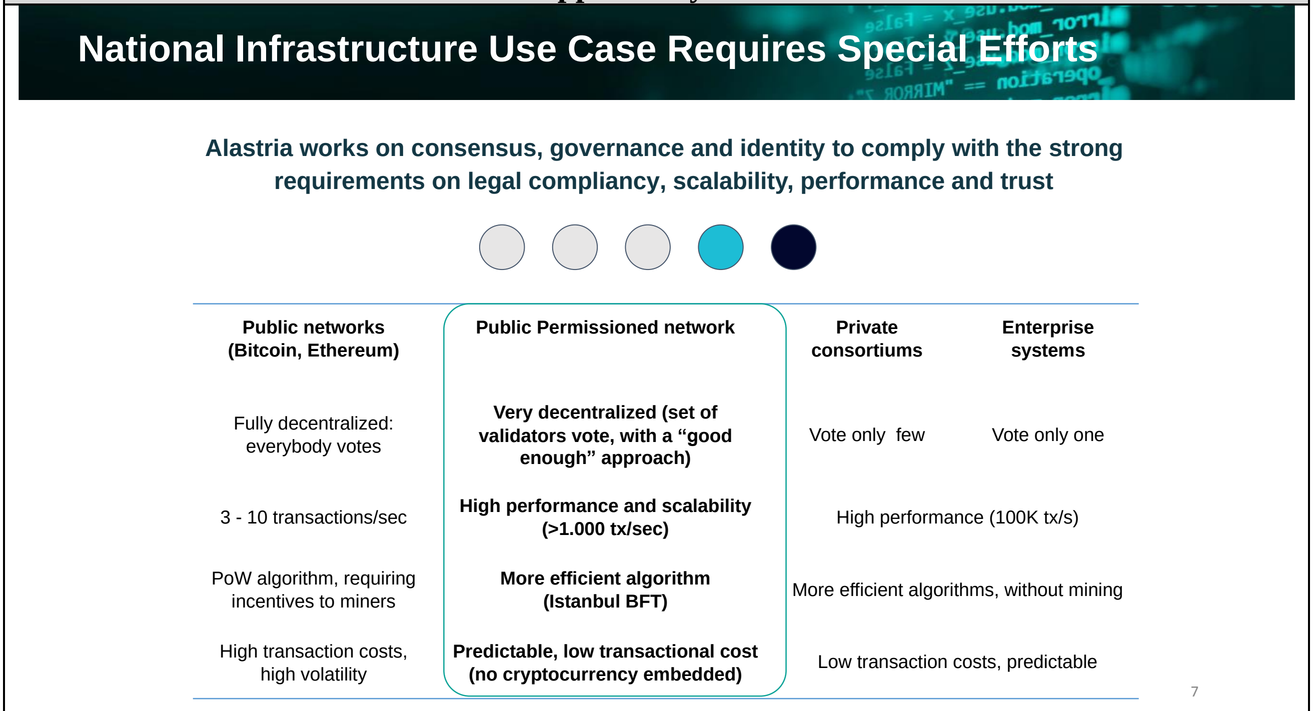
Alastria ID

Section 1: Summary

Use Case Summary			
Use Case ID:	IDM-001	**Use Case Type:**	*Horizontal*
Submission Date:	January 4, 2019	**Is Use Case supporting SDGs**	*Yes*
Use Case Title:	Alastria ID	**Domain:**	*1*
Status of Case	*e.g., Concept, PoC, Pilot, Implementation*	**Sub-Domain**	*Not Applicable*
Contact information of person submitting/ managing the use-case	*Full Name: Ismael Arribas* *Web site:* **https://alastria.io** *standards@alastria.io*		
Proposing Organization	**"Consorcio Red Alastria" Association (**Kingdom of Spain). **G-87936159**		
Short Description	**Alastria can be summarized as an independent, public, permissioned and neutral Blockchain/DLT framework for networks.**		
Long description	*Thanks to the diversity of its stakeholders and associates, Alastria has granted an infrastructure for Self-Sovereign Identity management. As a network it is dully authenticated in the Spanish market and European Union, however the partnership with LAC countries which is a fact of the SDG 17 scope for Alastria is the consequence for being a framework of networks. Alastria is the first multisectoral Association promoted by organizations and institutions for the establishment of a public Blockchain/DLT infrastructure, supporting services with legal effectiveness in the Spanish scope and according with the European regulation.* *The Consortium is open to any organization that wishes to have available a fundamental tool for the development of its own blockchain/DLT strategy with the aim of distributing and organizing products and services.*		
SDG in Focus (when applicable)	*SDG3, SDG4, SDG5, SDG6, SDG7, SDG8, SDG11, SDG 13, SDG16, SDG17.*		
Value Transfer:	**We will transfer claims off-chain with on-chain proofs. Ponderation of attributes by causality. Verified authority to attest and authenticate an attribute.**	**Number of Users:**	First PoC will happen in Spain (>45MM) but this solution aims to establish a global Identity system as an interplanetary badge. European Population and LAC.

Types of Users:	**People, Organizations, Public Administration & Objects (IoT) and processes.**
Stakeholders	*As we are proposing a Self-Sovereign Identity-based interconnected Blockchain Platform(s), with the right Governance, all type of users are also stakeholders*
Data:	*https://github.com/alastria/alastria-identity/wiki* *Privacy by design: unlinkable actions.*
Identification:	*Identification mechanism and rules; ability of participants to be anonymous, etc.* Non-interactive Zero-Knowledge Proof, in essence it refers to a proof construction where one can prove possession of certain information, e.g. a secret key, without revealing that information which needs to be kept confidential, and without any interaction between prover and verifier. **https://snark.network/**
Predicted Outcomes:	**MAIN NET and various PoC with succeed in different verticals like Healthcare, Education, Energy, E-Money and others. eIDAS Bridge Pilot as a reference for the ESSIF (European Self Sovereign Identity Framework)**

Overview of the Business Problem or Opportunity



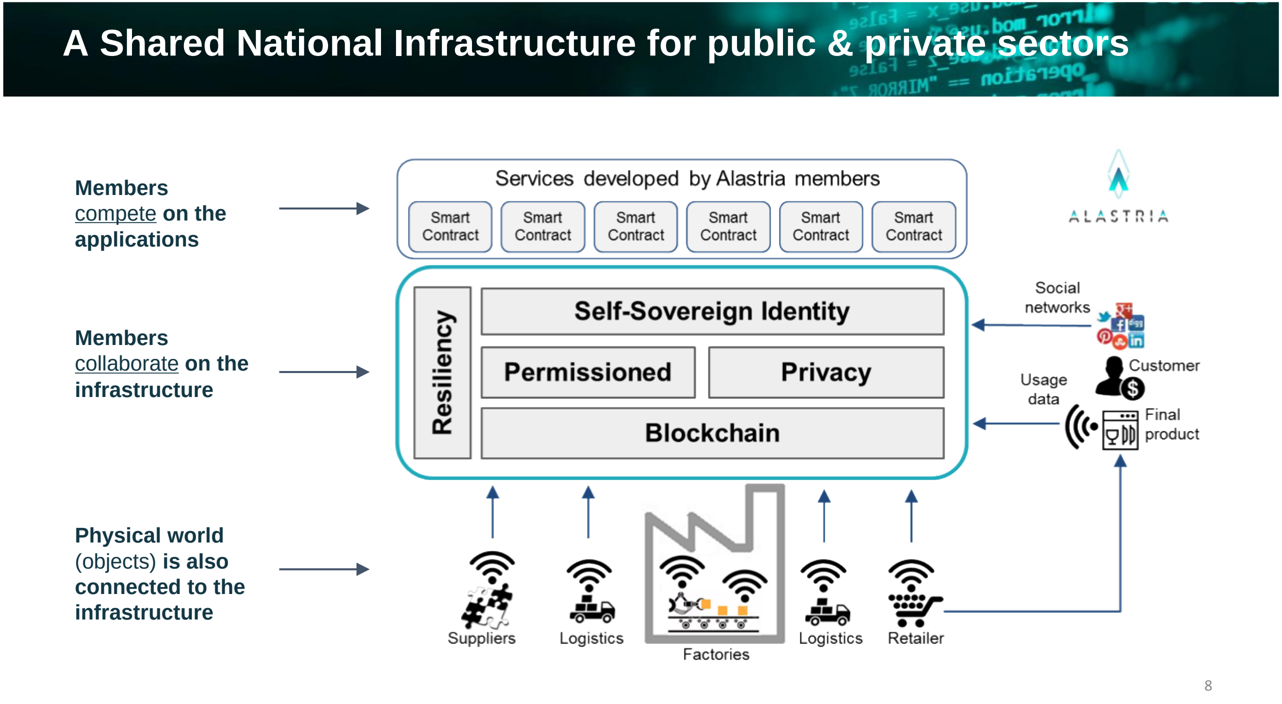
National Infrastructure Use Case Requires Special Efforts

Alastria works on consensus, governance and identity to comply with the strong requirements on legal compliancy, scalability, performance and trust

Public networks (Bitcoin, Ethereum)	Public Permissioned network	Private consortiums	Enterprise systems
Fully decentralized: everybody votes	**Very decentralized (set of validators vote, with a "good enough" approach)**	Vote only few	Vote only one
3 - 10 transactions/sec	**High performance and scalability (>1.000 tx/sec)**	High performance (100K tx/s)	
PoW algorithm, requiring incentives to miners	**More efficient algorithm (Istanbul BFT)**	More efficient algorithms, without mining	
High transaction costs, high volatility	**Predictable, low transactional cost (no cryptocurrency embedded)**	Low transaction costs, predictable	

7

Why Distributed Ledger Technology?



A Shared National Infrastructure for public & private sectors

Members compete on the applications

Members collaborate on the infrastructure

Physical world (objects) is also connected to the infrastructure

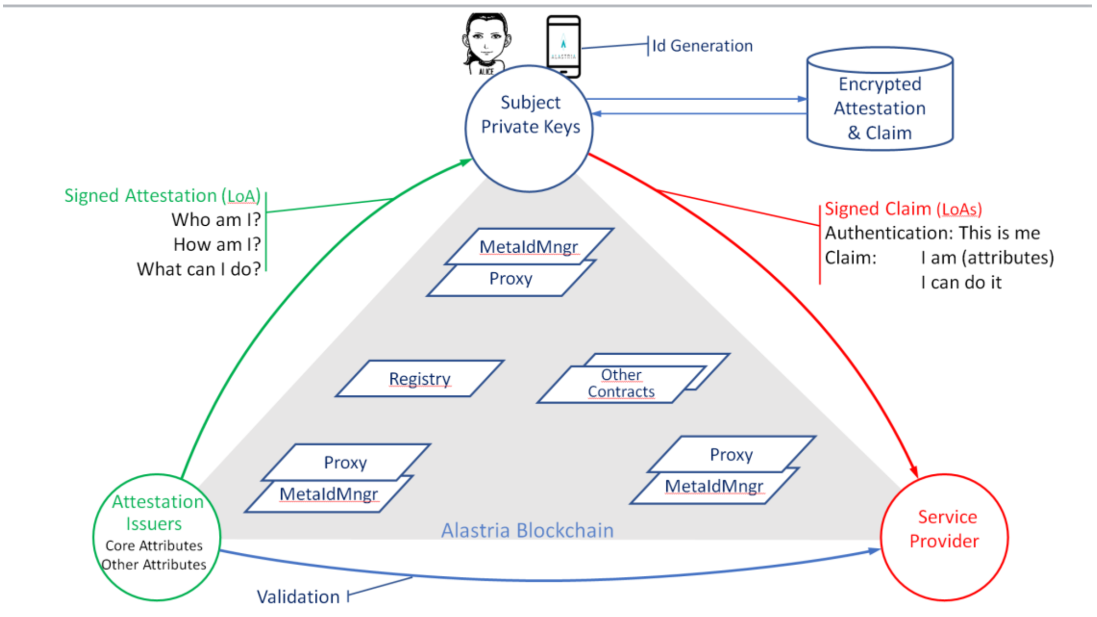
Services developed by Alastria members

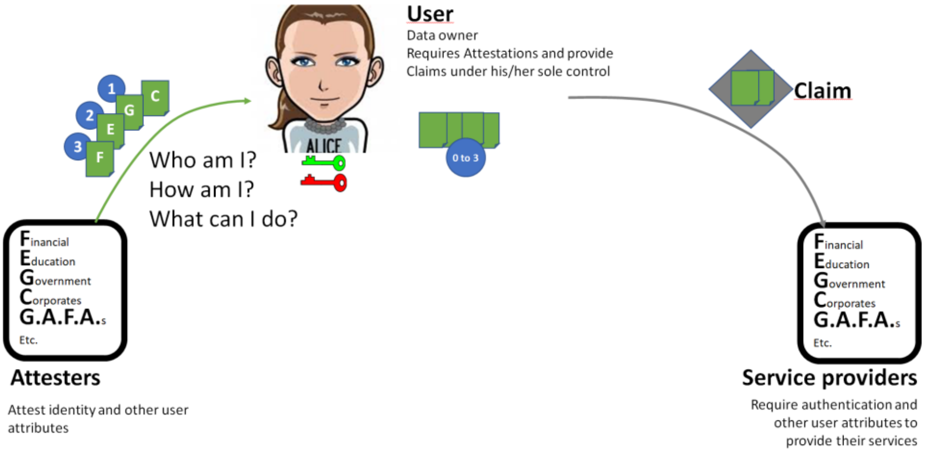
Section 2: Current process

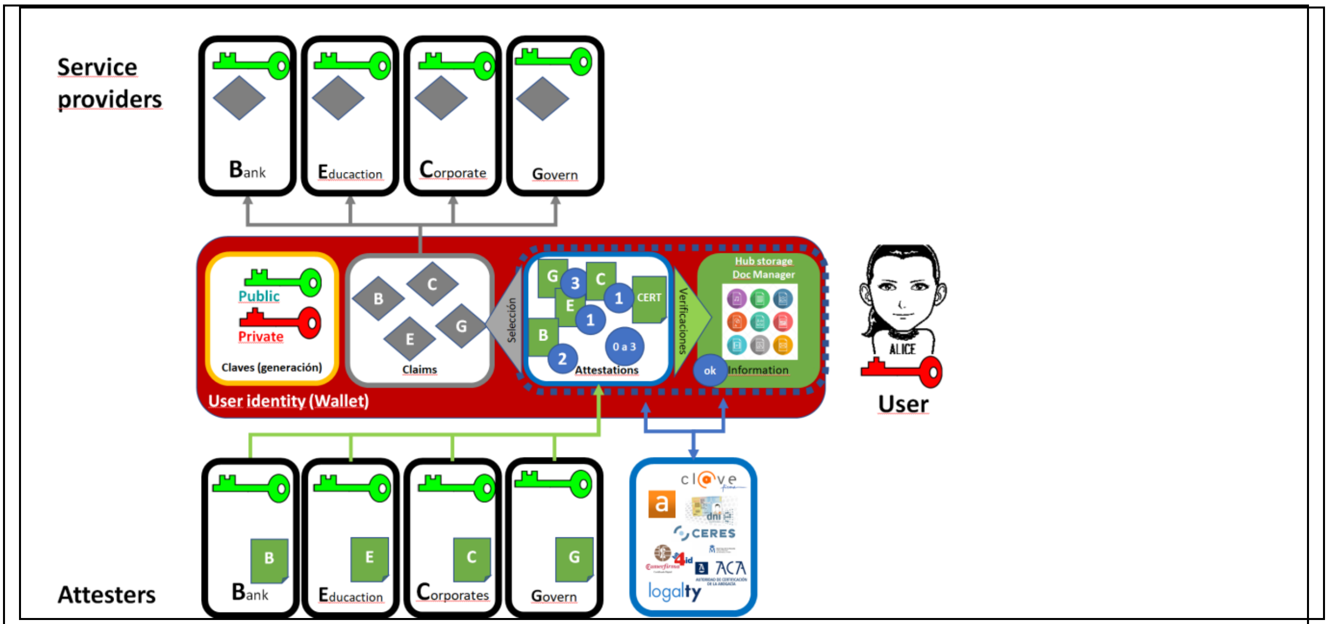
Current Solutions
There are a number of private consortiums and federated ones, but ALASTRIA is moderating the decentralization to a middle point between public and private permissioned infrastructure with all relevant participants for a country or jurisdiction like Public Notary, Corporate Registration Office and listed, medium and small and micro-enterprises, also covenants with other Public administration covering the possibility for a network for frameworks and vice-verse.

Section 2: Current process

Process scheme (as-is) and ROLES / DATA FLOW







Data and information (as-is)		
Data	**Type**	**Description**
1	*Adhesion*	Normal standard document for being a member of Alastria See https://alastria.io/en/become-a-member/

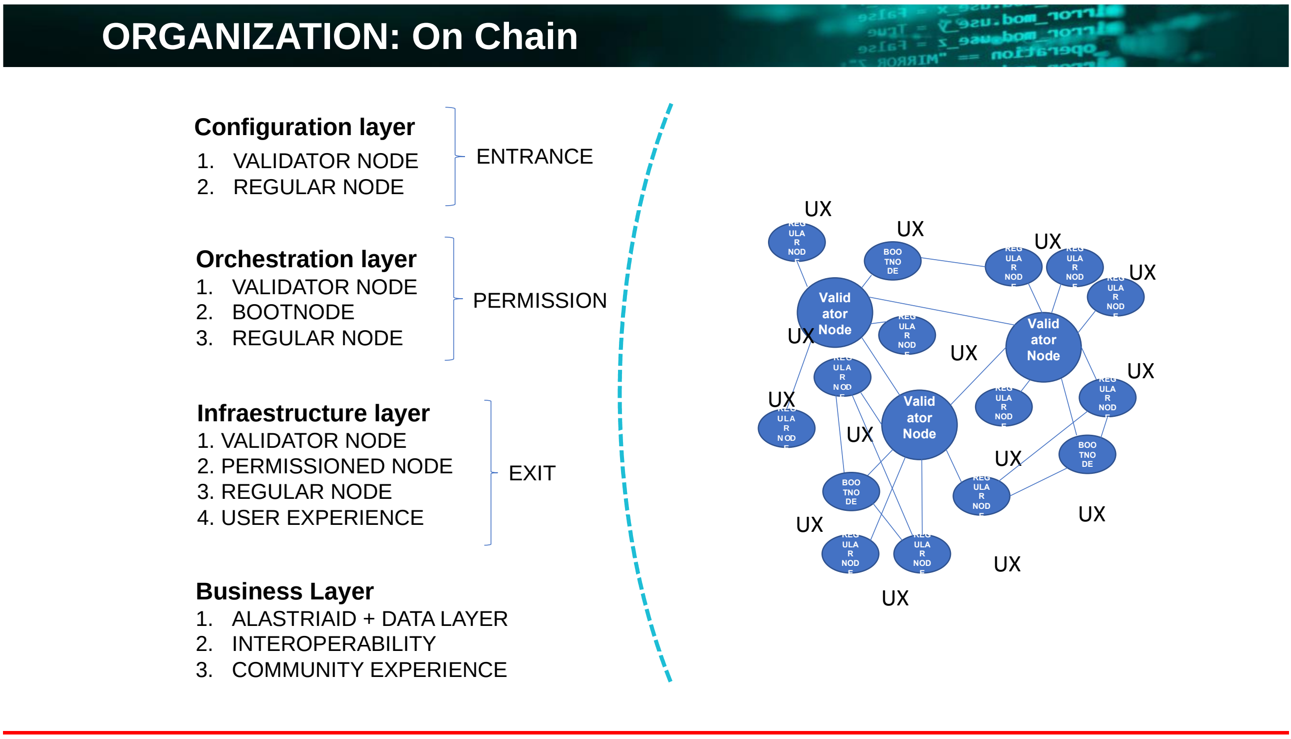
Participants and their roles		
Actor	**Type/Role**	**Description**
1	*Commissions*	Deploy different areas of the infrastructure, technological area, resilience area, trust framework area, standards, sustainability area, risk and cybersecurity processing.
2	*Committees*	Coordination and Implementation of the decision making for administrative proposes.

Other Notes
No.

Section 3: Expected process

Expected Flow (to-be)		
Step	**User Actions**	**System Actions**
1.	Generation	Alastria ID Generation
2.	Authentication	Verification and Validation
3.	Public Keys	Generation, Registration, Revocation and Deletion
4.	Credentials	Issuance, Registration, Revocation and Deletion
5.	Presentations	Issuance, Registration, Confirmation and Deletion.
6.	Identity and Private Key Backup & Recovery	Alastria Backup & Recovery ID.
7.	Signed transactions	Smart contracts and Dapps.

Process scheme (to-be)



ORGANIZATION: On Chain

Configuration layer
1. VALIDATOR NODE
2. REGULAR NODE

ENTRANCE

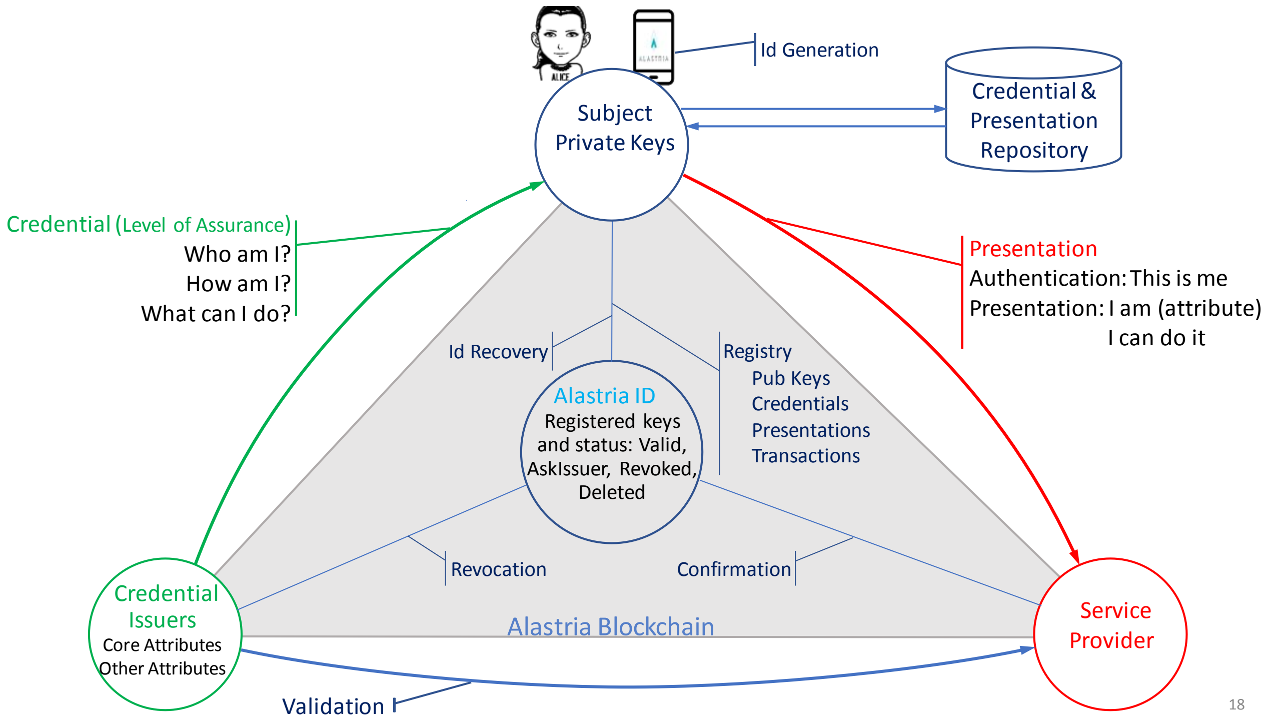
Orchestration layer
1. VALIDATOR NODE
2. BOOTNODE
3. REGULAR NODE

PERMISSION

Infraestructure layer
1. VALIDATOR NODE
2. PERMISSIONED NODE
3. REGULAR NODE
4. USER EXPERIENCE

EXIT

Business Layer
1. ALASTRIAID + DATA LAYER
2. INTEROPERABILITY
3. COMMUNITY EXPERIENCE



Subject Private Keys

Id Generation

Credential & Presentation Repository

Credential (Level of Assurance)
Who am I?
How am I?
What can I do?

Presentation
Authentication: This is me
Presentation: I am (attribute)
I can do it

Id Recovery

Registry
Pub Keys
Credentials
Presentations
Transactions

Alastria ID
Registered keys and status: Valid, AskIssuer, Revoked, Deleted

Revocation

Confirmation

Alastria Blockchain

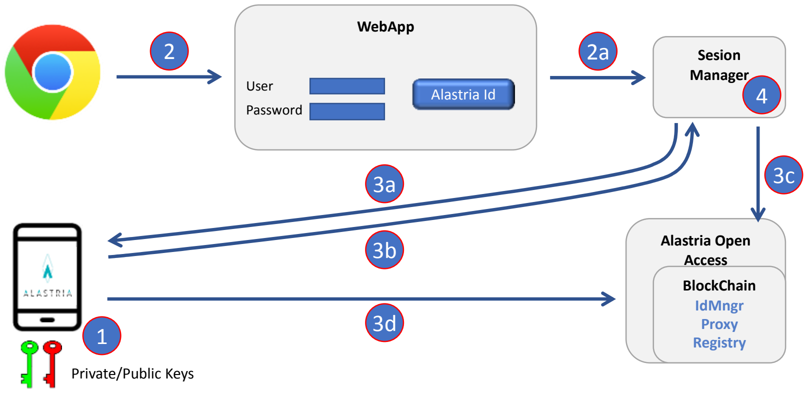
Credential Issuers
Core Attributes
Other Attributes

Service Provider

Validation

18

AlastriaId Generation

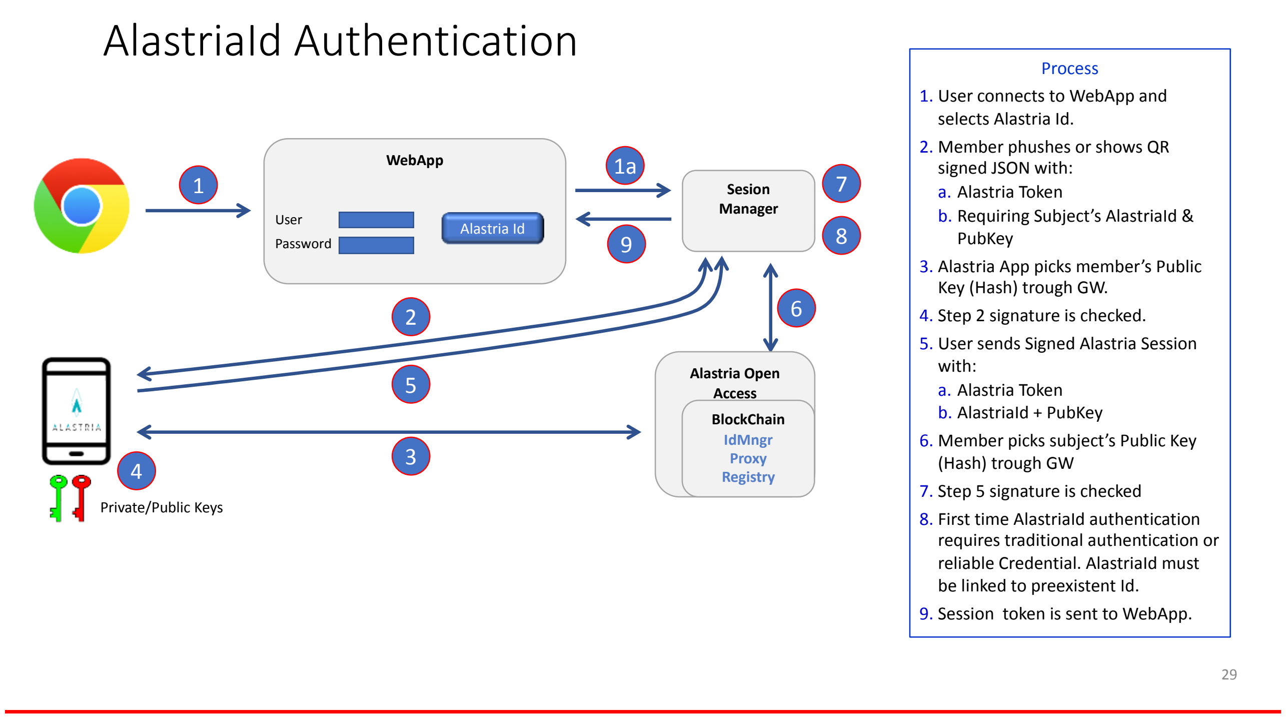


Process

1. Private/Public Key generation on Subject's device
2. Authentication by the current member WebApp.
3. Alastria Id set-up
   a. Members Pushes or shows QR
      i. JSON Alastria Token (AT)
      ii. Requiring KPub
   b. Subject sends signed AT and waits SetUpAlastriaId Event
   c. Member calls setUpAlastriaId
      From: Member
      To: MetaIdentityManager.
      Function: SetUpId (PubKey)
      Returns: AlastriaId
   d. At SetUpAlastriaId Event
      Subject calls CreateAlastriaId
      From: Subject
      To: MetaIdentityManager.
      Function: CreateId (PubKey)
      Returns: AlastriaId
4. At CreatedIdentity Event
   Member links AlstriaId to Subject preexistent Id on its systems.

28

Process scheme (to-be)



AlastriaId Authentication

Process

1. User connects to WebApp and selects Alastria Id.
2. Member phushes or shows QR signed JSON with:
   a. Alastria Token
   b. Requiring Subject's AlastriaId & PubKey
3. Alastria App picks member's Public Key (Hash) trough GW.
4. Step 2 signature is checked.
5. User sends Signed Alastria Session with:
   a. Alastria Token
   b. AlastriaId + PubKey
6. Member picks subject's Public Key (Hash) trough GW
7. Step 5 signature is checked
8. First time AlastriaId authentication requires traditional authentication or reliable Credential. AlastriaId must be linked to preexistent Id.
9. Session token is sent to WebApp.

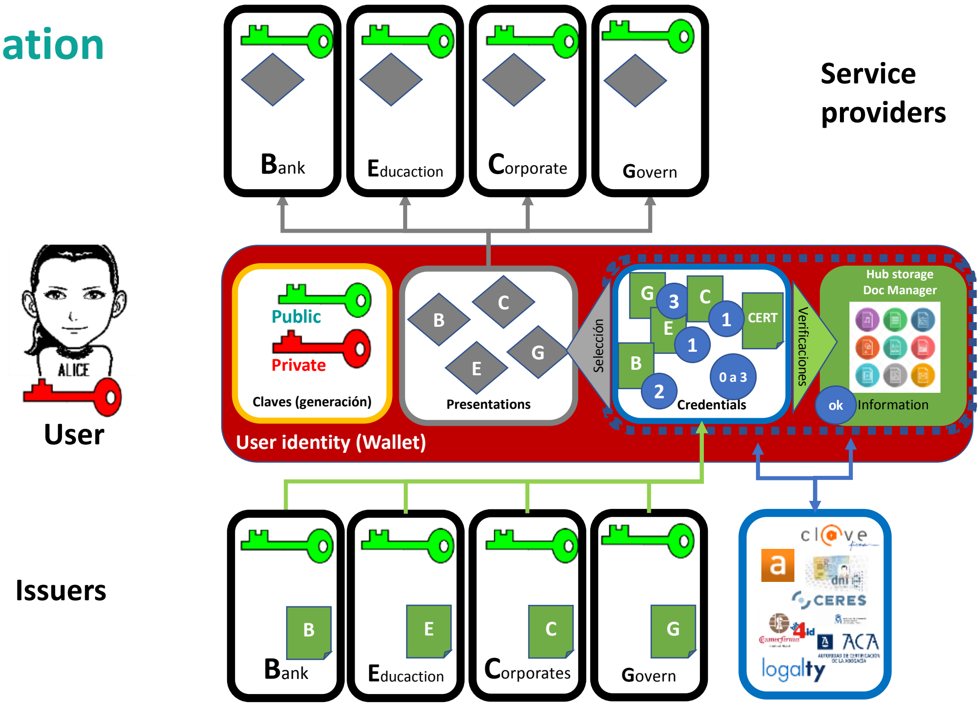
29

Participants and their roles

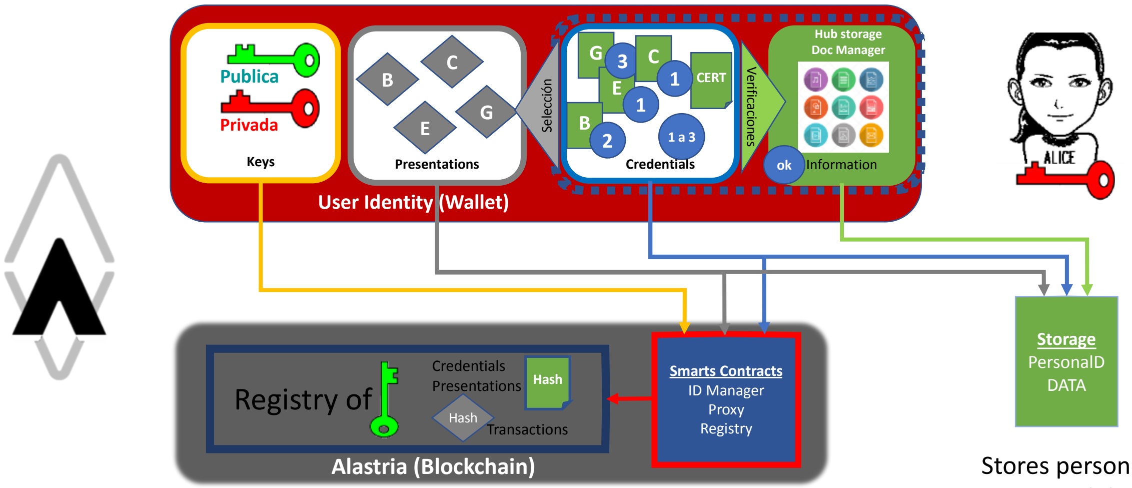
Actor	Type/Role	Description
1	*User*	ID generation
2.	*Credential Issuer*	Attributes and other events.
3.	*Service Provider*	Trust anchoring.
4.	*AlastriaID*	Registry, Recovery, Revocation, Confirmation, Deletion.

Data and information

Information



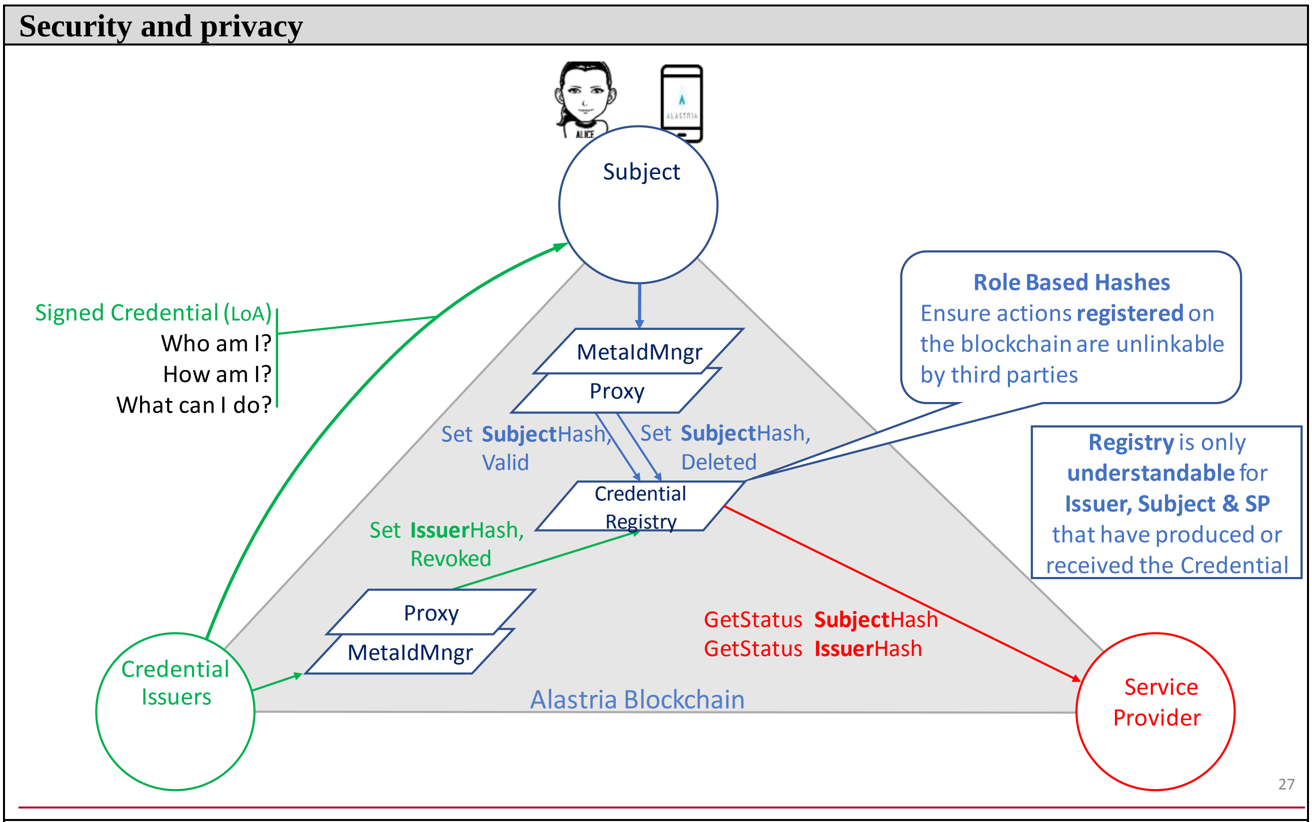
Information repositories



Stores personal
encrypted data

Records evidences (hashes)
never real personal data

Security and privacy



Subject

MetaIdMngr

Proxy

Set **Subject**Hash, Valid

Set **Subject**Hash, Deleted

Credential Registry

Set **Issuer**Hash, Revoked

Proxy

MetaIdMngr

Signed Credential (LoA)
Who am I?
How am I?
What can I do?

Credential Issuers

Alastria Blockchain

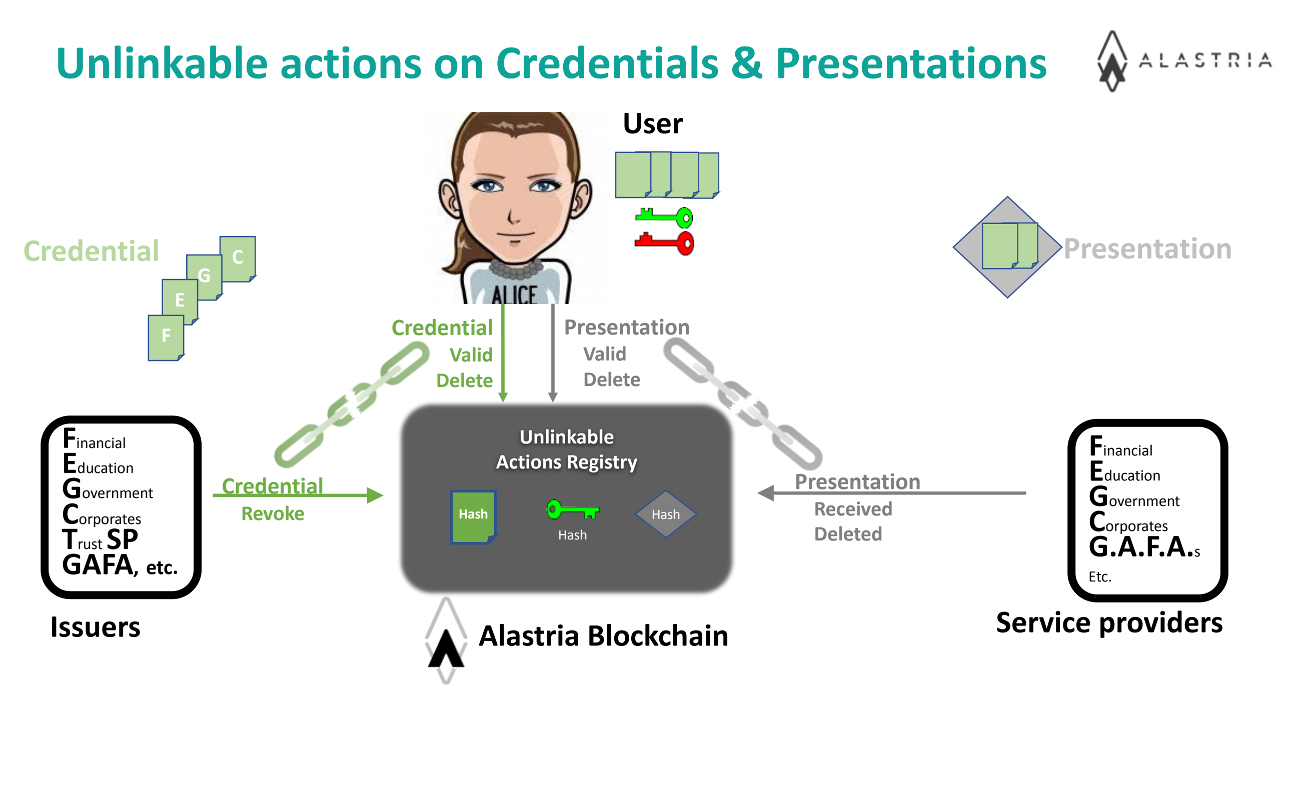
GetStatus **Subject**Hash
GetStatus **Issuer**Hash

Service Provider

Role Based Hashes
Ensure actions **registered** on the blockchain are unlinkable by third parties

Registry is only **understandable** for **Issuer, Subject & SP** that have produced or received the Credential

27



Unlinkable actions on Credentials & Presentations

ALASTRIA

User

Credential

Presentation

Credential
Valid
Delete

Presentation
Valid
Delete

Unlinkable
Actions Registry

Hash

Hash

Hash

Credential
Revoke

Presentation
Received
Deleted

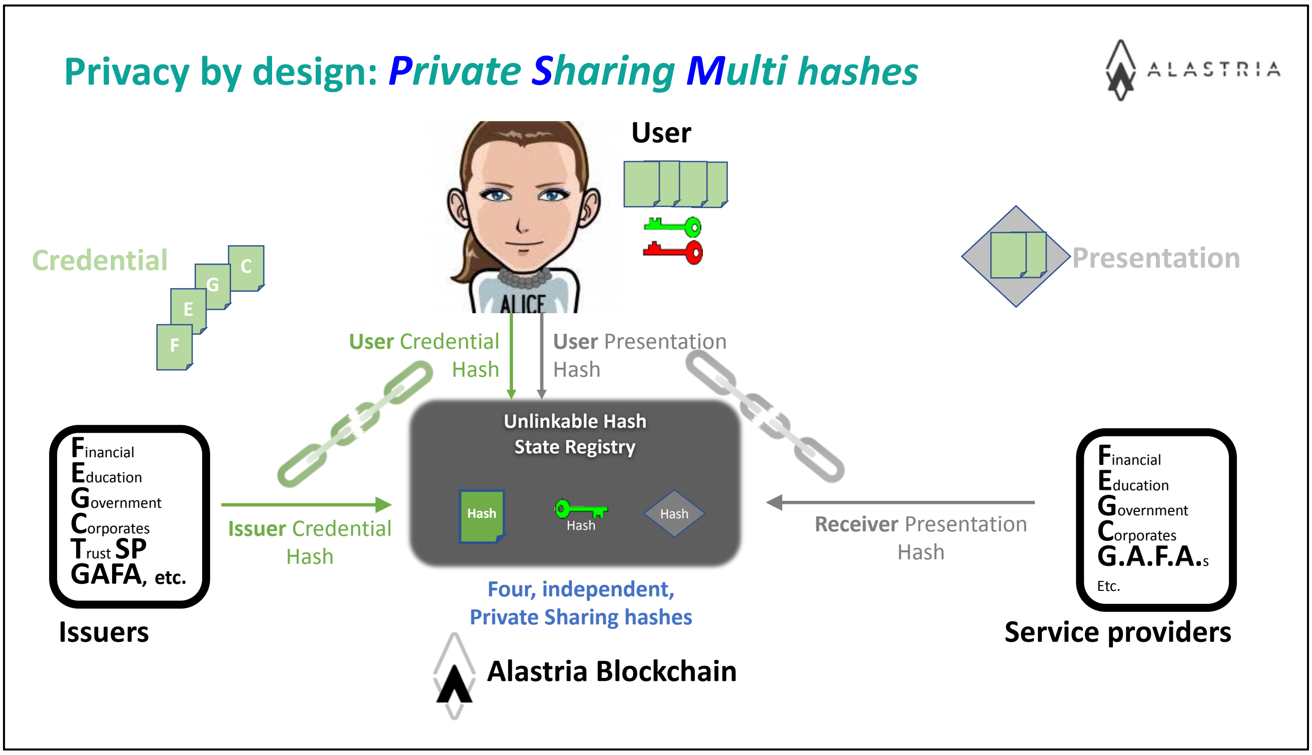
Financial
Education
Government
Corporates
Trust **SP**
GAFA, etc.

Issuers

Alastria Blockchain

Financial
Education
Government
Corporates
G.A.F.A.s
Etc.

Service providers



Privacy by design: *Private Sharing Multi hashes*

Main Success Scenario + expected time line

Various verticals are in production, Restricted MAIN-NET. Three test nets more for the framework of networks. LacChain Mainnet 2019. Testing two projects under European Blockchain Partnership. New Work Item at UNE CTN71/SC307 standard for decentralized ID.

Conditions (pre- or post-)

Public Permission Ecosystems are subject to some specific identification methods.

Performance needs

Extensibility and Scalability priorities. Healthcare PoC with the whole legal system of Spain for vaccines 'process, PoC for Traceability of Agrofood and Seafood, Sustainability transversal PoC for diplomas.

Legal considerations

Trust Framework Commission of Alastria is the tool that is creating all policies for interoperability. Legal and Compliance deployment and other legal checklist maintenance.

Risks

Uncertainty of regulation. Alternative Dispute Resolution must be efficient. Level of Assurance and Level of causalities.

Special Requirements
Not applicable

External References and Miscellaneous
ALASTRIA ID gives a complete compliance with GDPR and eIDAS.

Other Notes
This use case follows W3C Verifiable Credential and is compatible with EIP1812 for interoperability.

Appendix 1:
Domains and subdomains for use cases categorization

Vertical:

1. Finance
    a. Financial management & accounting
    b. International & interbank payments
    c. Clearing and settlement
    d. Reduction of Fraud
    e. Financial messaging
    f. Asset lifecycles and history
    g. Trade finance
    h. Regulatory compliance & audit
    i. AML/KYC
    j. Insurance
    k. Peer-to-peer transactions
2. Healthcare
    a. Pharma
    b. Biotechnology
    c. Medicine
3. Industries
    a. Manufacturing
    b. Energy
    c. Chemical
    d. Retail
    e. Real estate
    f. IT and telco
    g. Supply chain management
    h. Transportation
    i. Agriculture
4. Government and public sector
    a. Taxes
    b. Government and non-profit transparency
    c. Legislation, compliance & regulatory oversight
    d. Voting
    e. Taxation and customs
    f. Intellectual property management
    g. Land Registries

Horizontal:

1. Identity management
2. Security management
    a. Public Key Infrastructure
3. Internet of Things

4. Data processing, storage and management
    a. Data Validation (includes provenance)