SSI Implementation

Practical Experience From Alastria

About Alastria

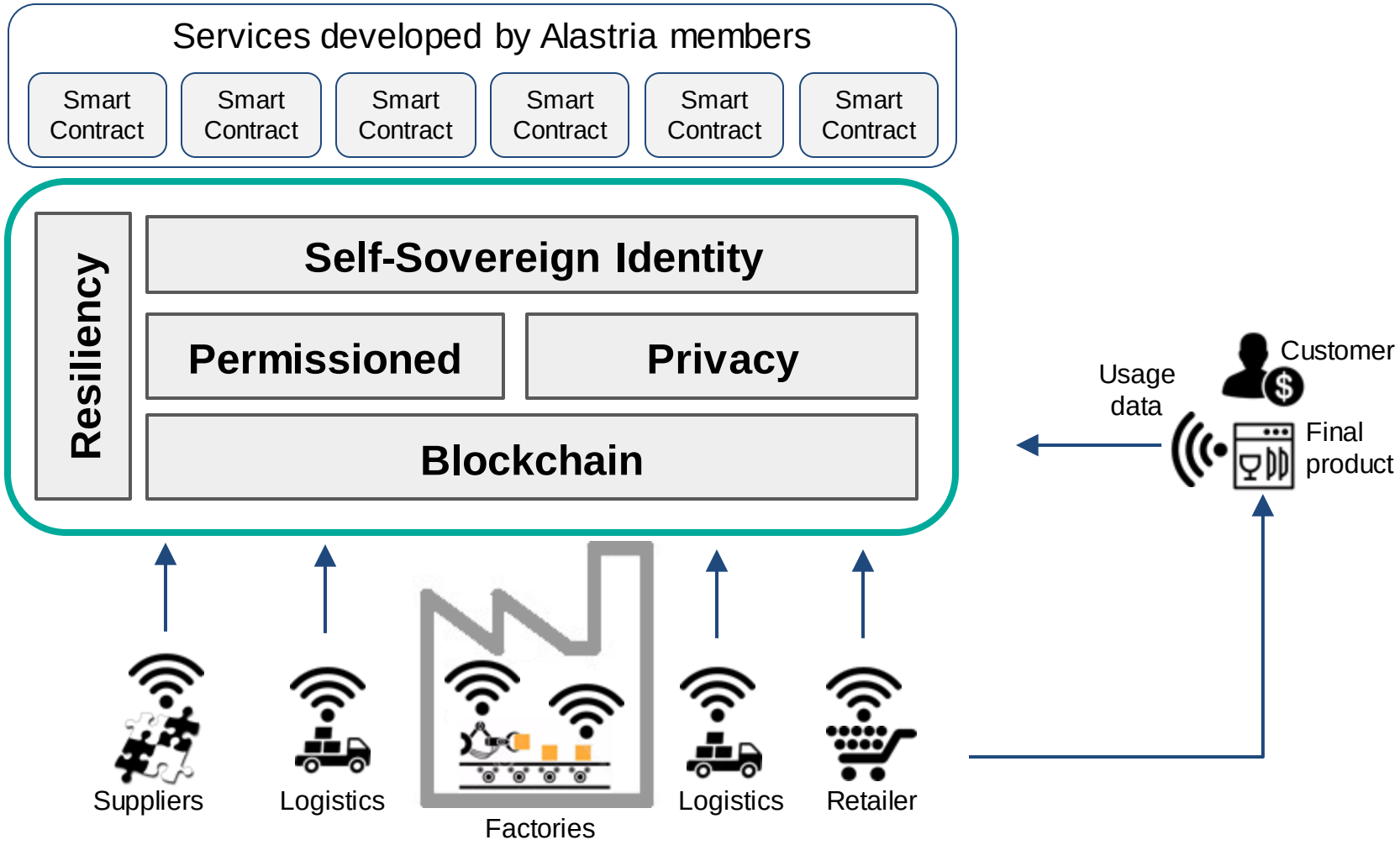
Alastria is a non-profit association that **promotes the digital economy by means of the development of distributed/Blockchain technologies.**

They've built a **multi-sectoral organization** that generates and shares knowledge with a collaborative spirit, evolving with a common vision and purpose

National Blockchain Network

Members **compete** on the applications

Members **collaborate** on the infrastructure



More 100 nodes

More 2 years up & running

Join the Alastria Webinar

ALASTRIA

Problems with Identity

ALASTRIA

Different standards across organizations

Lack of interoperability or portability

Too many! At least one for every organization

Inaccurate & outdated

Audit and traceability requirements

Limited user control

An increased volume in cybercrime, trust, fraud and security issues

Lack of single citizen view with inconsistent data across entities

Repetitive and expensive processes

Dependent on physical proofs and manual processes

Not trusted

Data privacy regulations

European e-identity

… control over our personal data which still have far too rarely today. Every time an App or website asks us to create a new digital identity or to easily log on via a big platform,
we have no idea what happens to our data in reality.

That is why the Commission will soon propose a secure European e-identity.

One that we trust and that any citizen can use anywhere in Europe to do anything from paying your taxes to renting a bicycle. A technology where we can control ourselves what data and how data is used

President von der Leyen's speech
State of the Union 2020 - 16th of September 2020

Why using Blockchain for Digital Identity

ALASTRIA

TRANSPARENCY

The use of the public/private key pair infrastructure allows the possibility of **signing and verifying the origin of the credentials without needing a third party.**

INMUTABILITY

Registering in Blockchain the hashes of the credentials, as well as the events of their issuance, presentation and revocation, assures us that they cannot be altered, **making it GDPR compliant and being completely user-centric.**

DECENTRALIZATION

Thanks to the implementation of Smart Contracts (self-executing programs in Blockchain networks) **the system does not need third parties** that act as intermediaries and who can read/use user data.

CURRENT MODEL OF IDENTITY

The **"Self Sovereign" or self-managed identity** is a model for managing digital identities being the user the sole owner of his data and having full control over it.

SELF-SOVEREIGN IDENTITY

What’s AlastriaID

Collaboration, Interoperability & internationalization

Open Source model contributed by more than 200 members

Alastria ID

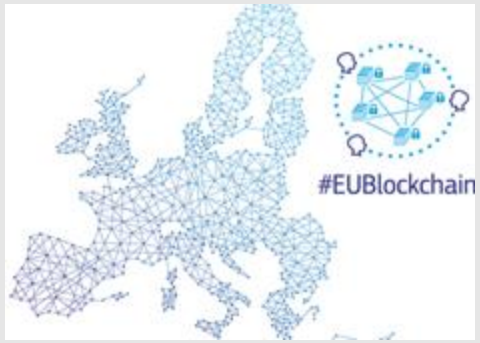
Three cornerstones:

- Functional-UX
- Technical
- Legal

UNE 71307 approved

Contributed to JTC19

Standardization



European Initiatives

EBP: *European Blockchain Partnership (Member States)*

EBSI: *European Blockchain Services Infrastructure*

ESSIF: *European Self-Sovering Identity Framework*

eIDAS: *eIDAS Bridge project*

Projects

- Dalion, Digitalis, Cabo Verde,…: Projects using Alastria ID
- Validated Id, uPort, Everis, Vottun,…: Alastria ID Compliant Wallets
- LACCHAIN - DAVID19: sponsored by Banco Interamericano de Desarrollo

The Roles & Needs. Example: renting a car

Personal User data is under the exclusive User control

1 User requests attested data from Issuers

2 Issuer sends attested data as digitally signed Verifiable Credentials

3 SP requests required data as a Presentation Request

4 User sends required data as a digitally signed Verifiable Presentation for a given **Purpose (rent a car)**

Issuers

Can attest identity and other user attributes

User

Service Providers

Require authentication and other user attributes to provide their services

Driving License from Trafic Auth.

Credit Card from a Bank

Over 25 years old from Town Hall

Personal User data is under the exclusive User control in a personal repository or wallet managed form his mobile or any other device.
Credentials can be reused at will.

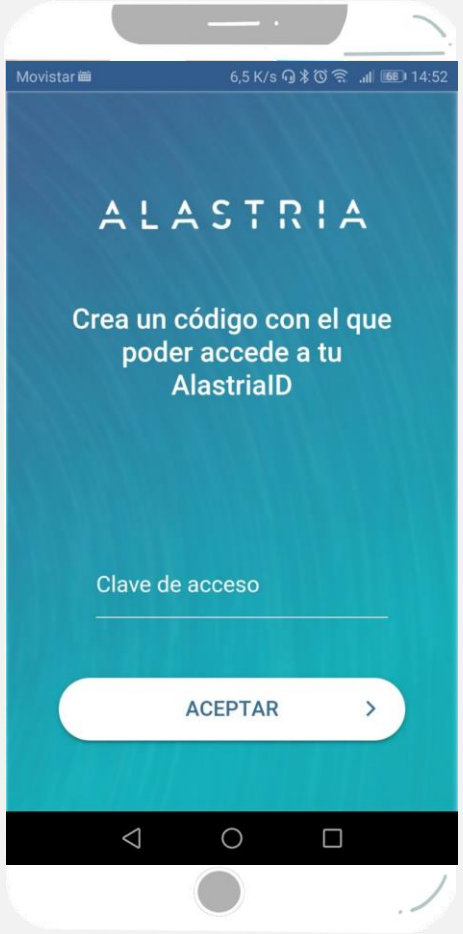
Data can be self attested or attested by an appropriate Issuer to increase confidence.

Each Issuer, the User and the SP have a Distributed Identifier, DID.

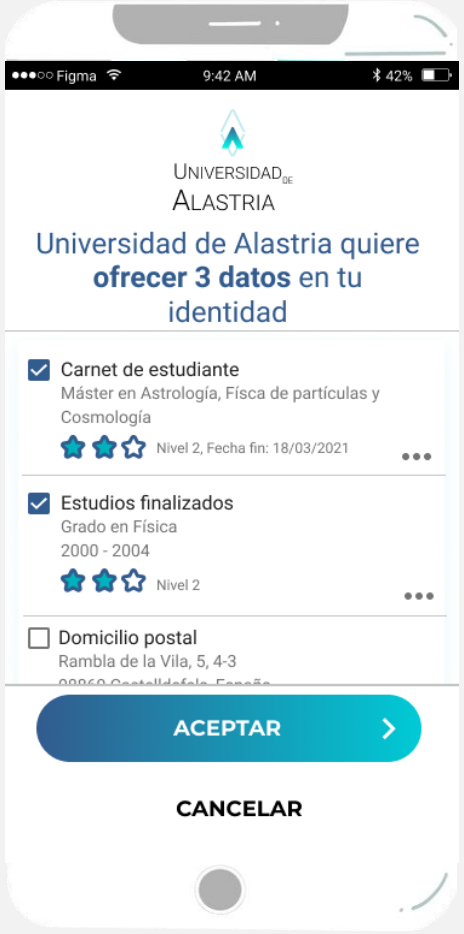
Prívate Keys are used to keep exclusive control over their DID

Easy to use mobile app

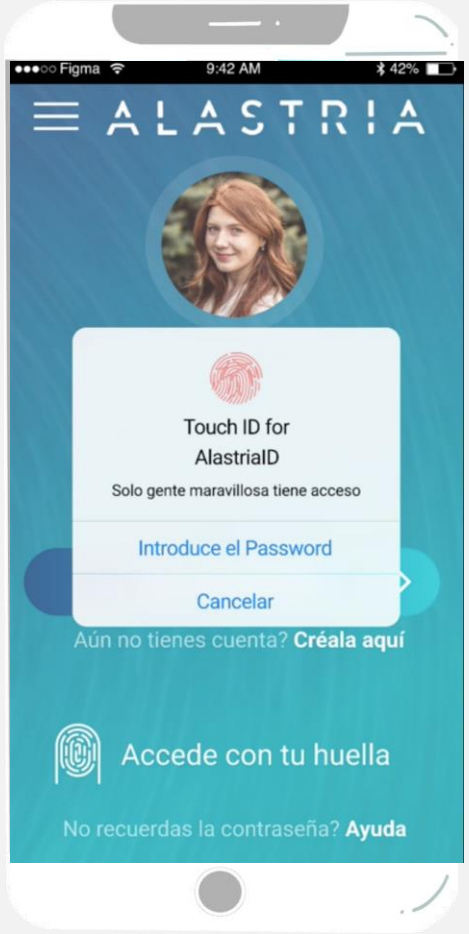
Personal data under exclusive user control



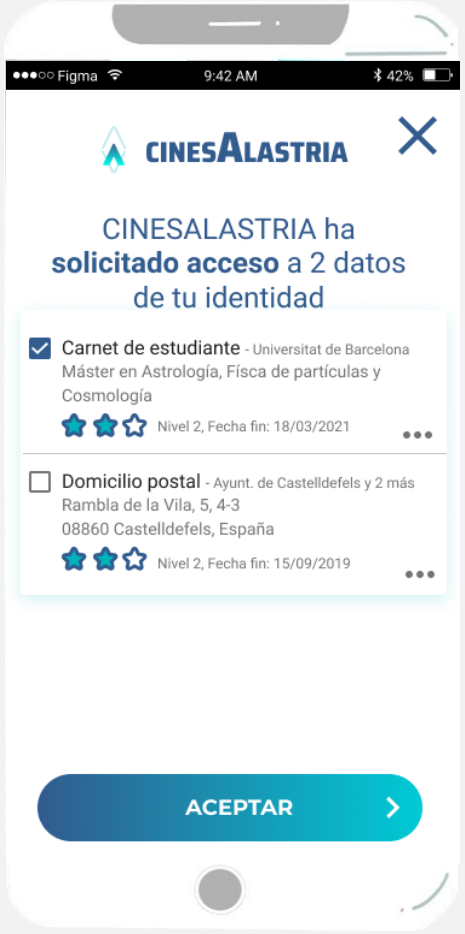
Id Generation



Credentials



Authentication



Presentations

Alastria Id – Credentials

Header:
- @context: http://schema.org
- @type: Person
- NetworkId: AlastriaTestNet01 → Network identification

Subject:
- SubjectAlastriaID: SubjectDID → Mandatory Subject's Alastria Id

AttributeData:
- @LevelOfAssurance: 3 → Level of Assurance
- **DrivingLicense: Type B2 (Car)**

IssuanceDates:
- InitialValidityDate: 2018-04-20/12:00 → Mandatory Initial Validity Date
- EndValidityDate: 2023-04-20/12:00 → Optional End Validity Date

Issuer:
- IssuerURL: IssuerURL
- IssuerAlastriaID: IssuerDID → Mandatory Issuer's AlastriaId
- IssuerPubKey: CurrentIssuerPubKey
- IssuerSignature: IssuerSignature → Mandatory Issuer Signature (with current Private Key)

Credential

W3C

Alastria Id – Presentations

Presentation

Header:
@context: http://schema.org
@type: Person
Subject:
SubjectAlastriaID: SubjectDID
AttributeData:
@LevelOfAssurance: 3
DrivingLicense: B2
IssuanceDates:
InitialValidityDate: 2018-04-20/12:00
EndValidityDate: 2023-04-20/12:00
Issuer:
IssuerURL: IssuerURL
IssuerAlastriaID: IssuerDID
IssuerPubKey: CurrentIssuerPubKey
IssuerSignature: **IssuerSignature1**

Credential 1
Credential …
Credential N

IssuerSignature: **IssuerSignature…**

IssuerSignature: **IssuerSignatureN**

More than a simple Credential list.

1 to N Credentials from (different) issuers, including their original digital signatures.

PresentationDates:
InitialPresentationDate: 2018-04-20/12:00
EndPresentationDate: 2023-04-20/12:00

Mandatory Presentation Initial Validity Date
Optional Presentation End Validity Date

Recipient:
RecipientAlastriaID: ServiceProviderDID

Mandatory Service Provider Alastria ID

Purpose:
ProcessHash: Hash of the process description & permanent link to it

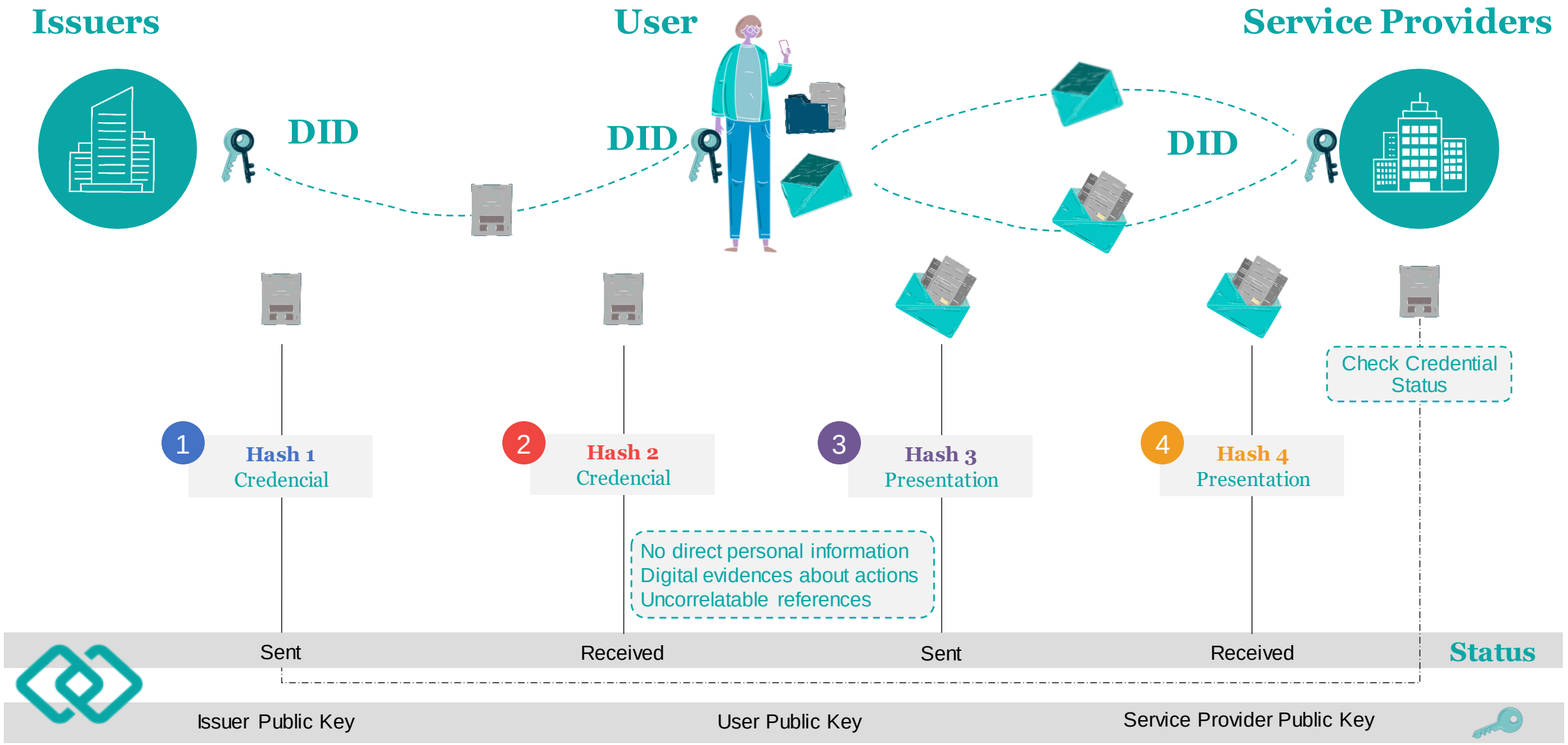
Business Process or purpose, linking the user consent to the purpose

Signature:
SubjectPubKey: CurrentSubjectPubKey
SubjectSignature: **SubjectSignature**

Optional current Subject's Public Key.
Mandatory Subject's Signature (done with current Private Key).

Personal data life cycle

After receiving a Credential and Sending a Presentation



Credentials issuance

Private Sharing Multihashes: avoiding correlation

Header:
@context: http://schema.org
@type: Person

Subject:
did:ala:quor:redt:f7f3b448ee5103ab848c217f8a899a357818c9409fd33d6fd83a6abcd76e3ea3

AttributeData:
@LevelOfAssurance: 2
Passport: **73749768V**

IssuanceDates:
InitialValidityDate: 2020-04-20/12:00
EndValidityDate: 2025-04-20/12:00

Issuer:
IssuerAlastriaID: IssuerProxyAddress
IssuerURL: AskIssuerURL

TUlJQ0lqQU5CZ2txaGtpRzl3MEJBUUVGQUFPQ0FnOEFNSUlDQ2dLQ0FnRUFvWWpiemtNbXNzNkJVL2VDQllocwozYkZSQlZsZE05RGxhTTdXaFBaRWdtWWw3QzFPYjBrbUVQRzJPL0dhTm9CT253cHRIeWt6dnBZUzQycnIvRDhJCjBMZUovMmR6MHVTdFF2NmtRREIEbU5SVHRoVzlzcGN1QnNxVzNlMWJSeWYwSnJMOG90MVg4TTRrME5HVTd3NTAKOGh0UHpSWlhSUzJab252OEcvTjM1ZVBEVjVYZjVtcmNPUE9lYmNvbm5kWEhScWZMbHlYQ3hDUzV4MHFsSkdYMQpkL29lMlhvcDdWZkJQL1VocnJtTm1zdFpzQkV2TDNmMzMrYTQ4Mnh1Q1R2UElRY3Y2Mk4zbGFSMndLT0pOOUNwCkZPcHFqd1I4Y2o5b0xqYkNSSGQ1VC8rYmdjNkRPL1hWenI5REFQVmFZTFp2bThwdU1oaGdja05JamdQT2ZXc1YKeUkrL0cxenVVSDVjYUZNaE1hUzk1TTJhMVhOSXdKNXNGMjVQRnBzdHRJckZYQytiMEpTMzI1bWs1cXZ6Q2dudQowRHJXVDJWUEJOanc0cnZtaEJQbkZiL0pkWHk1ZTVaSXB4dEdScHZLWWNCeERrNnlxZ3Q5U0MvZTgxK3RxQ3JGClNROWNHMVFDVi9Cblp3NGNkMUpIZTMvQUhvdDFZZVdqYjhZcElGaWZKN1d4RmIwZzlHSVlKWlRoM2RDOWhyTk8KZlNzSW9PTCtaQXlORnA0M3UwRkpUN3F0QzdDdHhQdkpudC9oOEFDRTA3ZXdna3EzTTBPem1UMlJOSWYwSGh5UwpNandkSWhsWThRR0dvVjMrekR1OW5UeDYzdHZ2YUJpa1B3dFp1Q3o3NmlwV2I1S3Q2U0E4MGZzTi9RT3REZmxtCkJ3amxUNlV2b2I2Z0s4QzdpSXJ3UUdVQ0F3RUFBUT09

Hashed Data

Header:
@context: http://schema.org
@type: Person

Subject:
did:ala:quor:redt:f7f3b448ee5103ab848c217f8a899a357818c9409fd33d6fd83a6abcd76e3ea3

AttributeData:
@LevelOfAssurance: 2
Passport: **73749768V**

IssuanceDates:
InitialValidityDate: 2020-04-20/12:00
EndValidityDate: 2025-04-20/12:00

Issuer:
IssuerAlastriaID: IssuerProxyAddress
IssuerURL: AskIssuerURL

TUlJQ0lqQU5CZ2txaGtpRzl3MEJBUUVGQUFPQ0FnOEFNSUlDQ2dLQ0FnRUFvWWpiemtNbXNzNkJVL2VDQllocwozYkZSQlZsZE05RGxhTT [...*

did:ala:quor:redt:5e13fc2d332a06bb66fd109006e163a9820bb7848ff4a102c0b20bdf88ea57f4

1
c80bb30d8ce77ec1ca9dba8b8f8e24e32ff2d9685aa6b3101ee6331480c3e408

DID
Identifier on Blockchain

1

Santander completes the credential data following the AlastriaID scheme

2

Santander signs all the credential data with its private key, obtaining an alphanumeric code

3

The alphanumeric code obtained by signing the data is added to the credential fields as well as the Issuer's DID

4

The hash* obtained is recorded on Blockchain

* A hash is a mathematical algorithm that transforms any arbitrary block of data into a new character string with a fixed length

Credential Hashes: two different hashes

1st Hash: Issuer

Hashed Data

Header:
@context: http://schema.org
@type: Person

Subject:
did:ala:quor:redt:f7f3b448ee5103ab848c217f8a899a357818c9409fd33d6fd83a6abcd76e3ea3

AttributeData:
@LevelOfAssurance: 2
Passport: **73749768V**

IssuanceDates:
InitialValidityDate: 2020-04-20/12:00
EndValidityDate: 2025-04-20/12:00

Issuer:
IssuerAlastriaID: IssuerProxyAddress
IssuerURL: AskIssuerURL
IssuerSignature: IssuerSignature

did:ala:quor:redt:5e13fc2d332a06bb66fd109006e163a9820bb7848ff4a102c0b20bdf88ea57f4

DID:
Identifier on Blockchain

2nd Hash: Subject

Hashed Data

Header:
@context: http://schema.org
@type: Person

Subject:
did:ala:quor:redt:f7f3b448ee5103ab848c217f8a899a357818c9409fd33d6fd83a6abcd76e3ea3

AttributeData:
@LevelOfAssurance: 2
Passport: **73749768V**

IssuanceDates:
InitialValidityDate: 2020-04-20/12:00
EndValidityDate: 2025-04-20/12:00

Issuer:
IssuerAlastriaID: IssuerProxyAddress
IssuerURL: AskIssuerURL
IssuerSignature: IssuerSignature

did:ala:quor:redt:f7f3b448ee5103ab848c217f8a899a357818c9409fd33d6fd83a6abcd76e3ea3

DID:
Identifier on Blockchain

1 c80bb30d8ce77ec1ca9dba8b8f8e24e32ff2d9685aa6b3101ee6331480c3e408

2 728356b4d1fa5c63fe5a4de71f71113e5068c8115409c3cdedfbb7d3579f4bfe

Presentation Hashes: two different hashes

3rd Hash: User

Hashed Data

Header:
@context: http://schema.org
@type: Person
Subject:
SubjectAlastriaID: SubjectProxyAddress
AttributeData:
@LevelOfAssurance: 2
address:
@type: PostalAddress,
addressLocality: Seattle,
addressRegion: WA,
postalCode: 98052,
streetAddress: 20341 Whitworth Institute
IssuanceDates:
InitialValidityDate: 2018-04-20/12:00
EndValidityDate: 2023-04-20/12:00
Issuer:
IssuerURL: IssuerURL
IssuerAlastriaID: IssuerProxyAddress
IssuerPubKey: CurrentIssuerPubKey
IssuerSignature: IssuerSignature

Credential 1
Credential ...
Credential N

IssuerSignature: IssuerSignature
IssuerSignature: IssuerSignature

ClaimDates:
InitialClaimDate: 2018-04-20/12:00
EndClaimDate: 2023-04-20/12:00
Recipient:
RecipientAlastriaID: RecipientProxyAddress
Purpose:
ProcessHash: Hash of the process name & description
Signature:
SubjectPubKey: CurrentSubjectPubKey
SubjectSignature: SubjectSignature

did:ala:quor:redt:f7f3b448ee5103ab848c217f8a899a357818c9409fd33d6fd83a6abcd76e3ea3

DID:
Identifier on Blockchain

4th Hash: Service Provider

Hashed Data

Header:
@context: http://schema.org
@type: Person
Subject:
SubjectAlastriaID: SubjectProxyAddress
AttributeData:
@LevelOfAssurance: 2
address:
@type: PostalAddress,
addressLocality: Seattle,
addressRegion: WA,
postalCode: 98052,
streetAddress: 20341 Whitworth Institute
IssuanceDates:
InitialValidityDate: 2018-04-20/12:00
EndValidityDate: 2023-04-20/12:00
Issuer:
IssuerURL: IssuerURL
IssuerAlastriaID: IssuerProxyAddress
IssuerPubKey: CurrentIssuerPubKey
IssuerSignature: IssuerSignature

Credential 1
Credential ...
Credential N

IssuerSignature: IssuerSignature
IssuerSignature: IssuerSignature

ClaimDates:
InitialClaimDate: 2018-04-20/12:00
EndClaimDate: 2023-04-20/12:00
Recipient:
RecipientAlastriaID: RecipientProxyAddress
Purpose:
ProcessHash: Hash of the process name & description
Signature:
SubjectPubKey: CurrentSubjectPubKey
SubjectSignature: SubjectSignature

did:ala:quor:redt:4031899d20a4965636b75bbd34758c91c250d9ce9b1febe8c897e642930c4744

DID:
Identifier on Blockchain

3

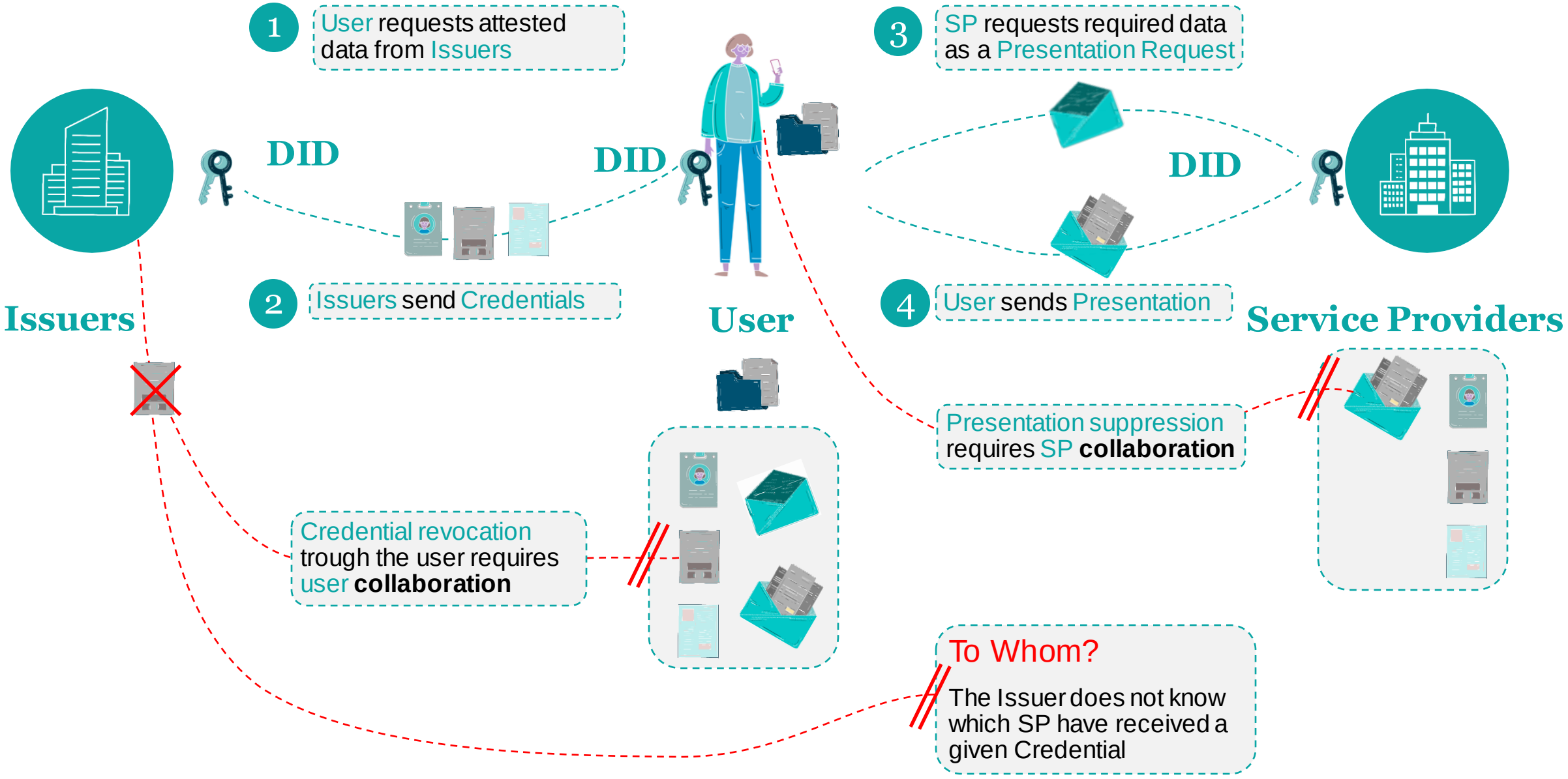
```
34f3c53d0b1d4dbdd56483
2b4e83382fd647ba994f15
886034fd071c14ffd4fd
```

4

```
379ab3ca5b592487234adb
821b9edea8850544c7cb71
fea4d1844015836eabd2
```

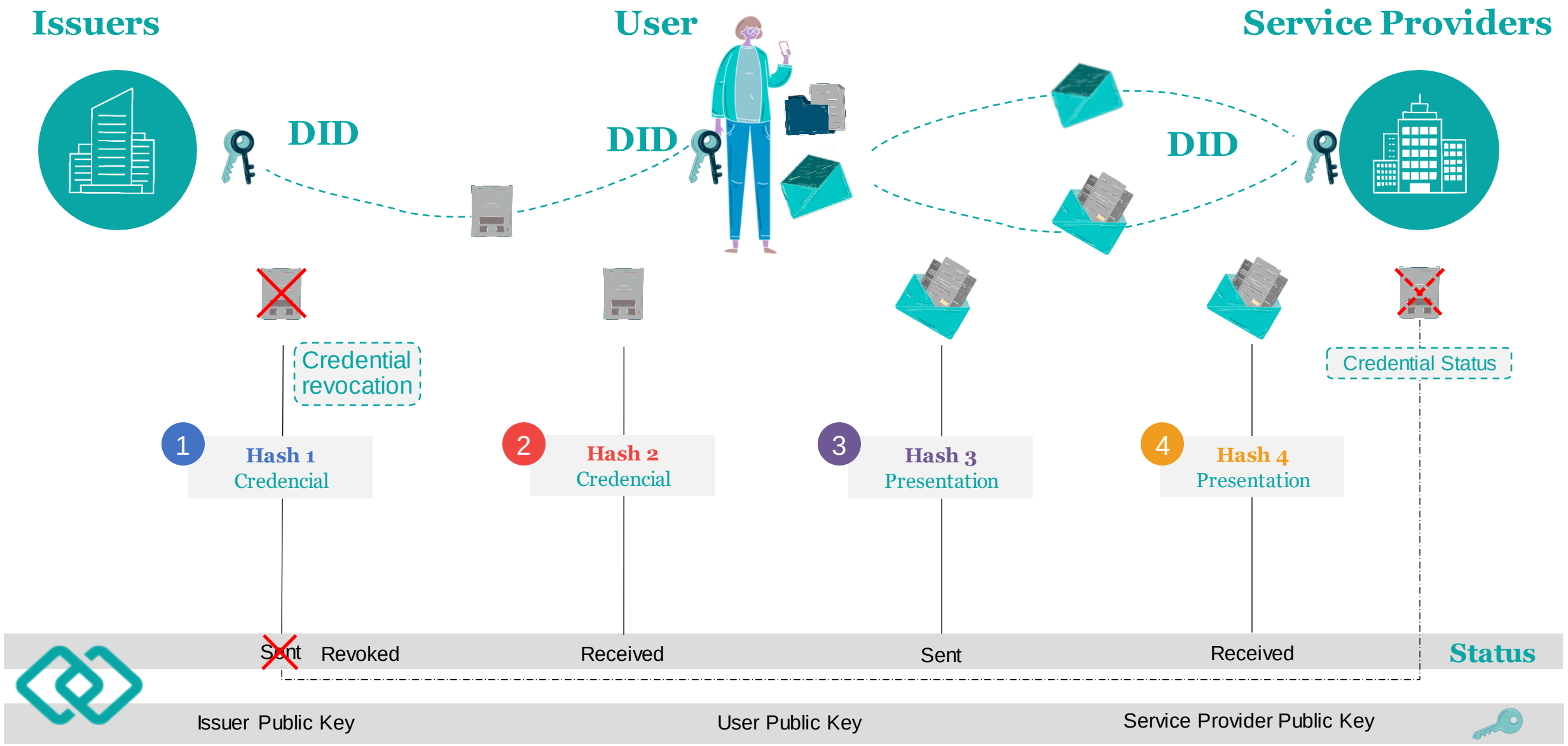
Personal data life cycle

Issuer Credential Revocation and User Presentation Suppression



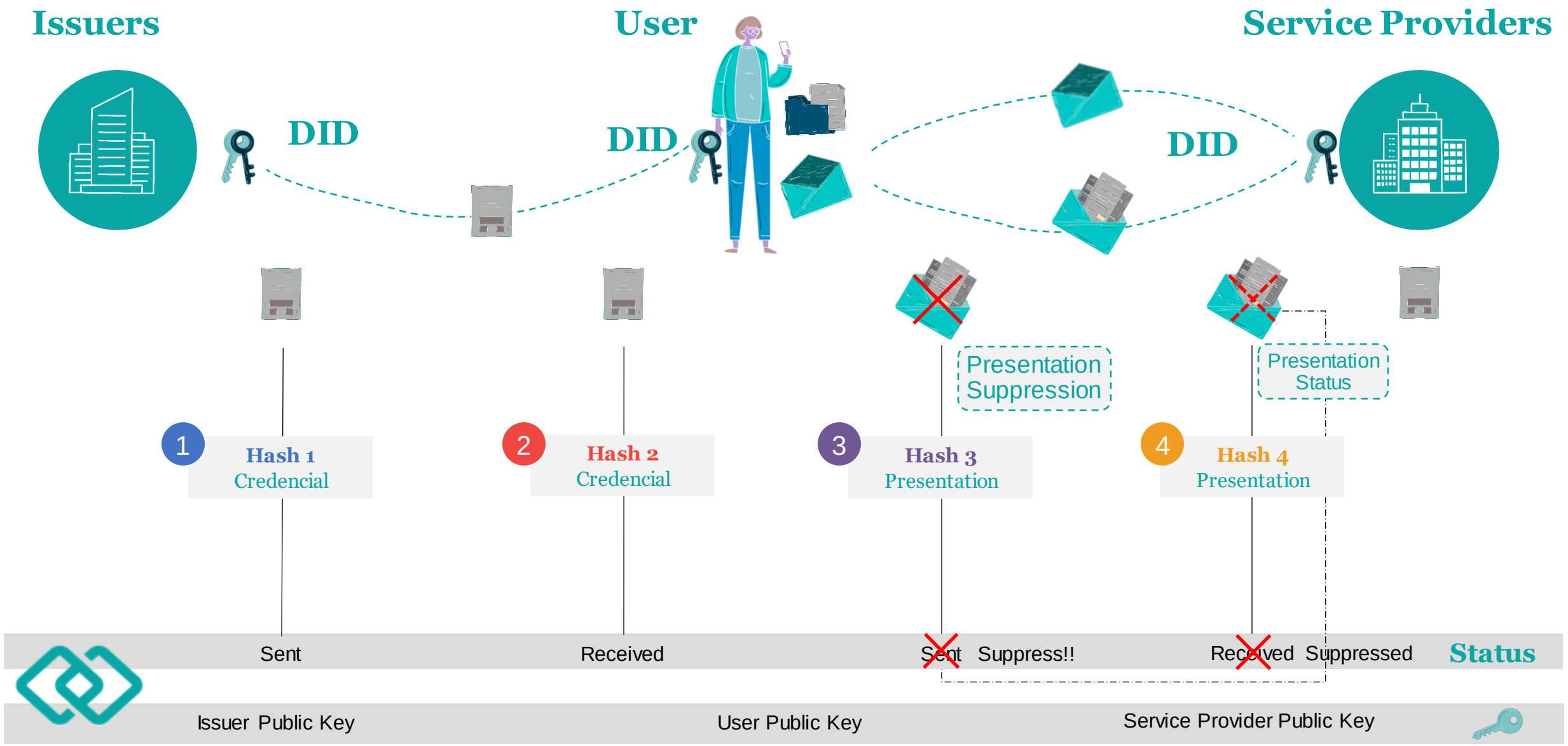
Personal data life cycle

When the Issuer revokes a Credential



Personal data life cycle

When the user Request the Suppression of a Presentation



Technical Overview

Available SW and documentation

Implemented by projects

Demo Wallet

Uses embedded Library

Demo Entity

Uses Swagger Services

Implemented by Alastria

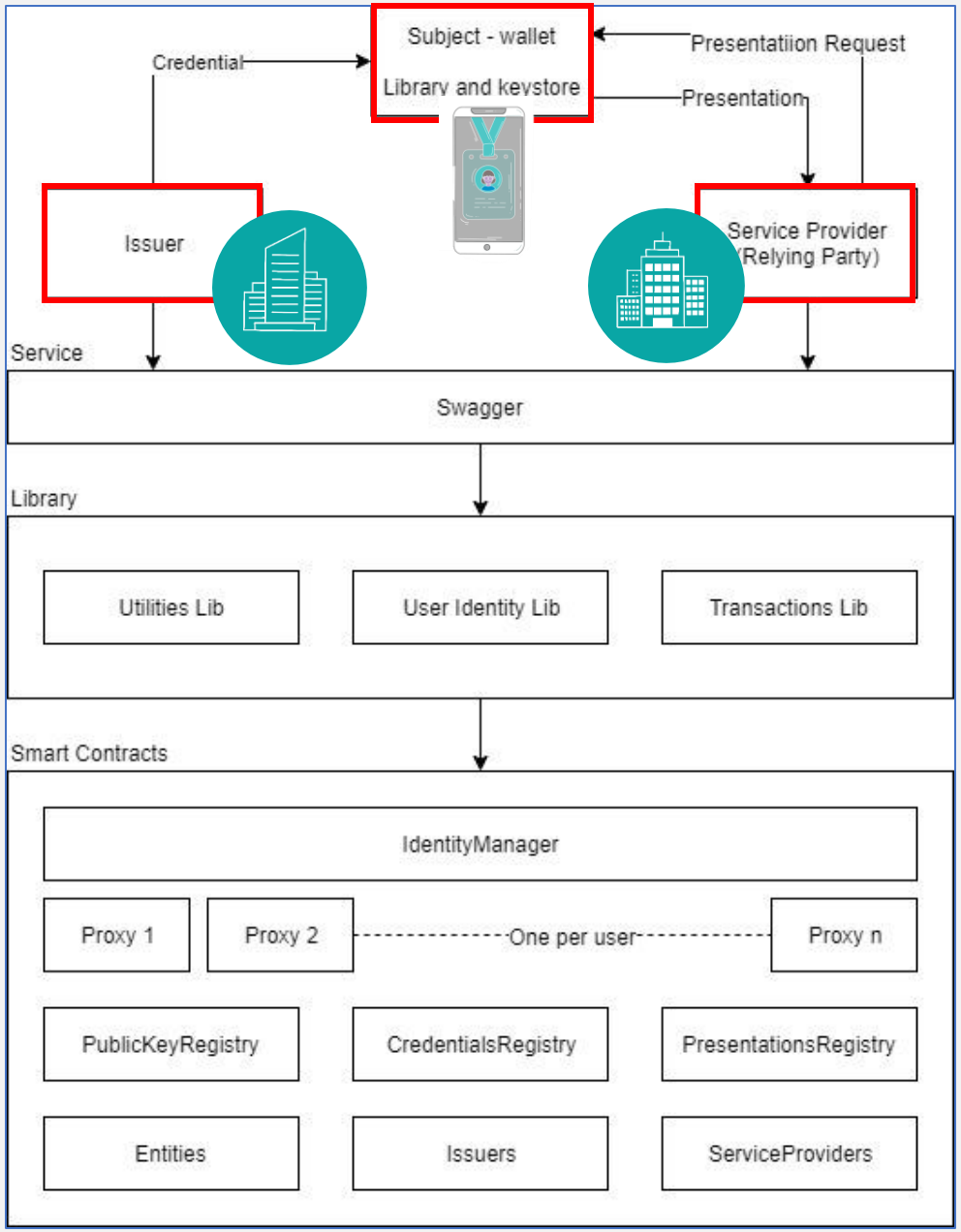
Service API

Library

Strongly recommended to ensure interoperability

Smart Contracts

Mandatory to ensure interoperability



Docs and Software links @

Documentation description	Link
General doc: Alastria Identity wiki	https://github.com/alastria/alastria-identity/wiki
Alastria ID model presentation	https://portal.r2docuo.com/alastria/document?LDDE906FE0
Credential, Presentation & Presentation Requests detailed Definition	https://github.com/alastria/alastria-identity/wiki/Alastria-DID-Method-Specification-(Quorum-version)
alastria-wallet	https://github.com/alastria/alastria-wallet
Alastria Library: typespcript lib to help using Solidity Smart Contracts plus Utility Functions	Https://github.com/alastria/alastria-identity-lib
Solidity Smart contracts	https://github.com/alastria/alastria-identity
Examples of using Alastria Library	https://github.com/alastria/alastria-identity-example

Demo SW Description	Link
Alastria Wallet Mobile App (apk)	https://www.dropbox.com/s/2dtvy8qvgxkpevh/alastriaDemoPortrait.apk?dl=0
Issuer & Service Provider demo implementation (web page)	https://github.com/alastria/alastria-identity-serviceProvider

Practical Implementation

Benefits for the user

Access to services immediately

Greater control of data usage

Ease of rights exercises (GDPR)

Privacy assured

No data trading

Discounts and bonuses

Benefits for the companies

Improves

Customer satisfaction level

Data quality

Regulatory compliance (GDPR)

Reduces

Churn rates

Information verification costs

Problems of Privacy & Security

Response to a real need

We carried out different user investigations before and after the Covid19 pandemic to analyze the perception of users regarding the privacy of their data.

- Desk research: Review of reports, papers and articles on Covid-19
- Six interviews with personalities with a strategic vision of Covid-19
- Online survey carried out in UserZoom between July 13 and 26, 2020 with Sample size (n) = 1439 and Confidence interval = 95%

Main insights

- ☑ Acceleration of digitization as a means of personal and work relationships
- ☑ The generalized perception of obligation in the transfer of data is reinforced
- ☑ **Fear of the use of personal data without their own knowledge and demand for greater control over them**
- ☑ The Public Administration and the Banking are perceived as safe organizations in the protection of data

ALASTRIA

DALION

“Your digital identity controlled by yourself, to use it wherever you want, backed by your trusted entities”

Santander, REPSOL, CaixaBank, Liberbank, Bankia, linea directa, inetum Positive digital flow, MAPFRE, BancaMarch, GENERALI

with potential to reach 30.000.000 users in Spain

- **Collaborative project** to put Alastria's identity model into practice by integrating it with business applications.
- It aims **to give people control of their personal data** so that each of us truly has a single identity controlled and self-managed by ourselves in a safe and reliable environment
- **MVP launch on Q2`21**

+ Public Administration Observers

Gobierno de España – Ministerio de Economía y Empresa – Secretaría de Estado para el Avance Digital

Universidad Zaragoza

Ayuntamiento de Alcobendas

Gobierno de España – Ministerio de Política Territorial y Función Pública – Secretaría de Estado de Función Pública – Secretaría General de Administración Digital

Gobierno del Principado de Asturias

Gobierno de Aragón

ALASTRIA

digitalis®

CEPSA REPSOL

ferrovial Sabadell

GRUPO RED ELÉCTRICA MAPFRE

- Use the Alastria identity model
- Focus on supplier management
- Unique identity for companies acting as suppliers or buyers
- Suppliers manage their own identity, facilitating the sharing of certifications, reducing costs and increasing security
- The subject figure in this case is a legal, non-physical person
- The wallet is therefore on a server, not a mobile

Alastria Id

Other Related Projects

u·port

- Interest on a Alastria Id compatible wallet

KAYTRUST by everis

- Complete Suite for Identity Ecosystem
- Alastria Id compatible wallet
- Several projects

Validated ID
Always be yourself

- Onboarding, KYC & AML focus
- Collaborating with Alastria, Sovrin and DIF

VOTTUN

- Voting solutions
- Focus on Industry specific credentials
- Blockchain agnostic

EBSI - ESSIF

EBSI: European Blockchain Services Infrastructure

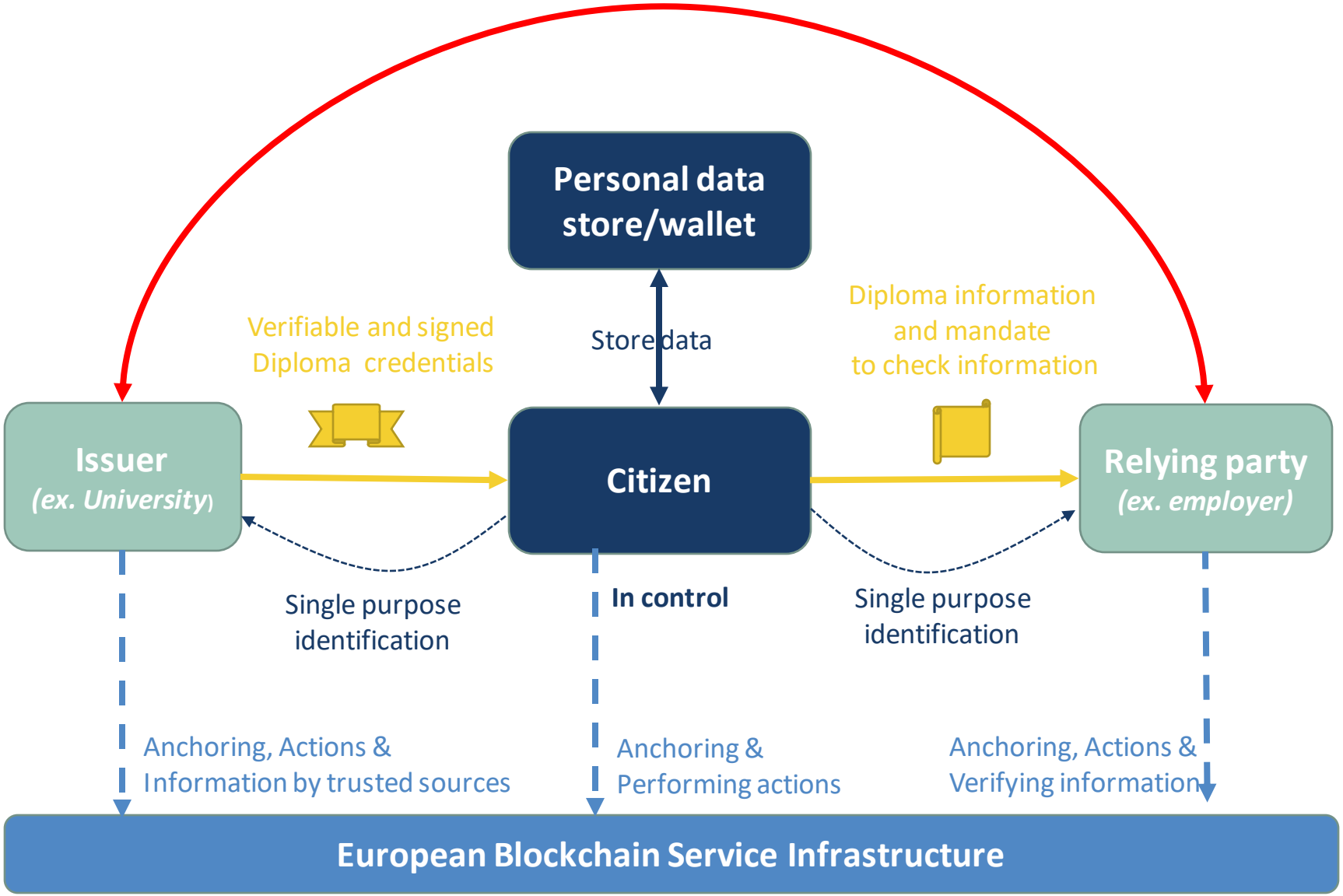
ESSIF: European Self-Sovereign Identity Framework

EBSI v2
May 2021

New Use Cases

European Self Sovereign Identity Framework

Added value in a decentralized identity context



ESSIF

Added value

- Involvement of Government services and information.
- Linking of decentralized identity with eIDAS and GDPR.
- Providing (multiple) government base identity.
- Single purpose identification.
- Secure trust anchor for issuers and credentials.
- Simplification of public services and access to public information cross border and cross sector.
- Standardisation of digital interactions for citizen in public and private sector.

Next Steps

AlastriaID

- Open Source
- Open to Collaboration

Interoperability

- ESSIF
- Hyperledger

Invitation to Hyperledger Identity WG

- Webinar for Alastria Identity Commission

SSI Implementation

Practical Experience From Alastria