EUROFILING CONFERENCE 17-18-19 JUNE 2019

USING SELF-SOVEREIGN IDENTITIES ALIGNED WITH EIDAS EU REGULATION: CASES OF MONEY LAUNDERING OR TERRORIST FINANCING

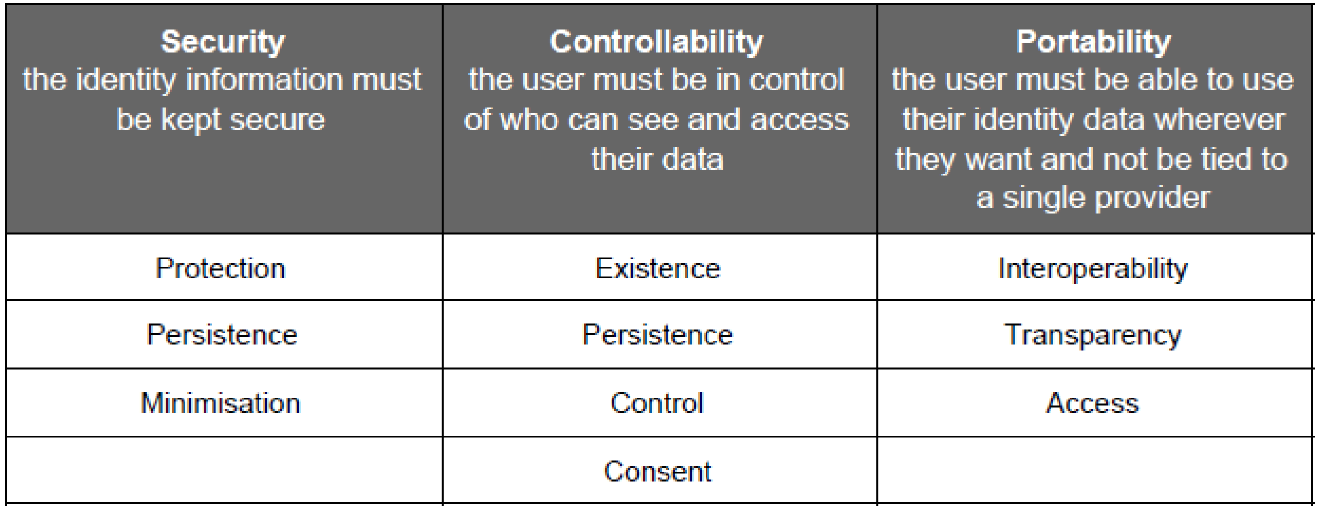
DR. IGNACIO ALAMILLO, CISO
LOGALTY

Frankfurt, 19/06/2019

WHOAMI *@NACHOALAMILLO*

- Dr. Ignacio Alamillo-Domingo, expert in electronic identity management and trust services.
- Lawyer, Certified Information Systems Auditor, Certified Information Security Manager.
- Phd thesis regarding legal aspects of the electronic identification and trust services (eIDAS Regulation).
- +20 years of experience in public and private sector.
- Member of ETSI Electronic Signature Infrastructure group.
- Member of UNE SC 307/ISO TC 307 Blockchain.
- Co-leader of ISO TC 307 “Trust Anchors for Decentralized Identity Management”.

SELF-SOVEREIGN IDENTITIES (SSI)

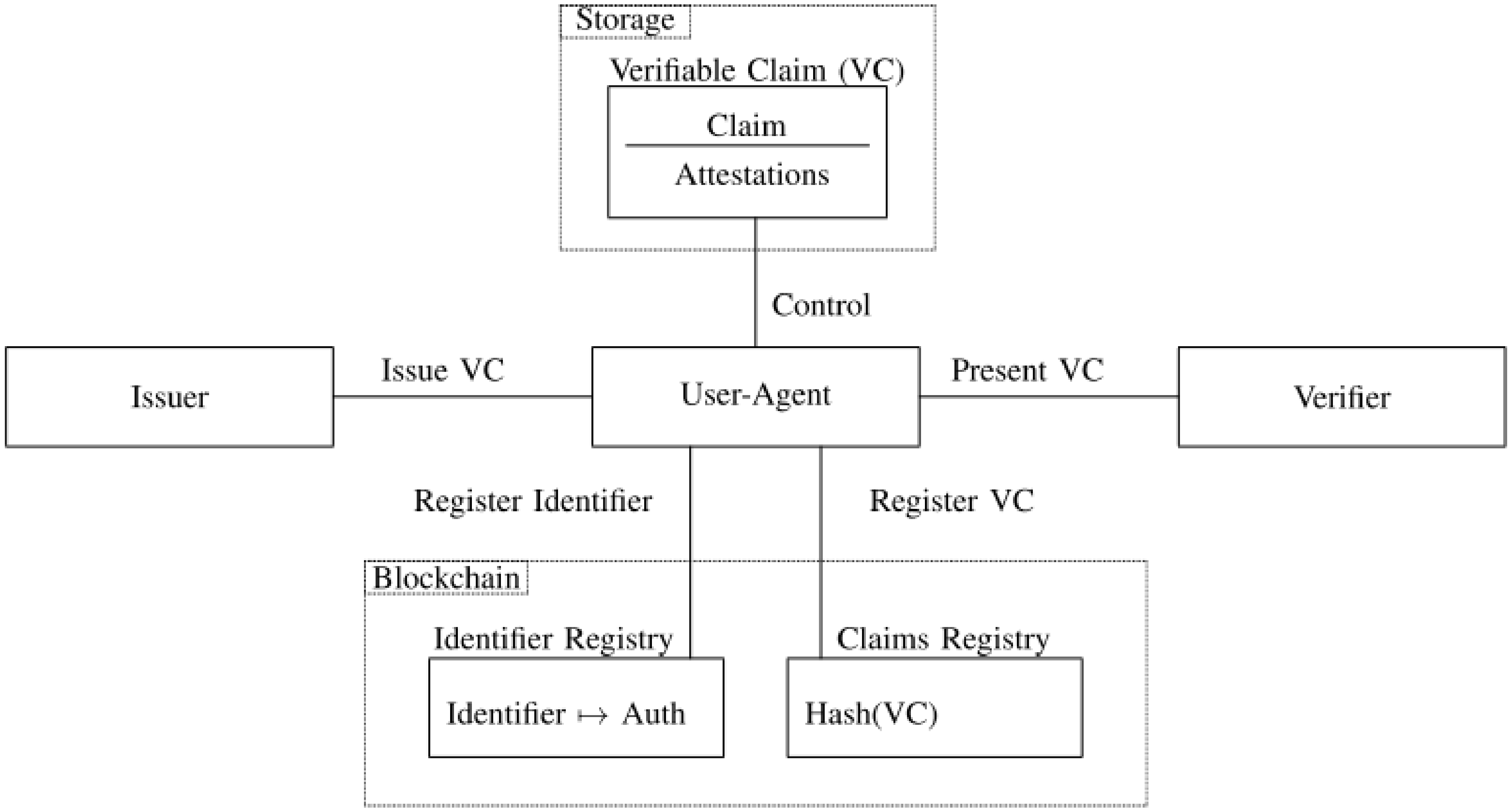


Security the identity information must be kept secure	**Controllability** the user must be in control of who can see and access their data	**Portability** the user must be able to use their identity data wherever they want and not be tied to a single provider
Protection	Existence	Interoperability
Persistence	Persistence	Transparency
Minimisation	Control	Access
	Consent	

C. Allen / The Path to Self-Sovereign Identity (2016)

“Self-sovereign identity is the next step beyond user-centric identity and that means it begins at the same place: **the user must be central to the administration of identity**. That requires not just the interoperability of a user’s identity across multiple locations, with the user’s consent, but also **true user control of that digital identity**, creating user autonomy. To accomplish this, **a self-sovereign identity must be transportable**; it can’t be locked down to one site or locale”.

AN SSI ARCHITECTURE (ILLUSTRATIVE)



A. Mühle et al. / Computer Science Review 30 (2018) 80–86

SSI BENEFITS

- Compared to previous identity management systems (centralized, based in PKI, federated and user-centric), SSI introduces key benefits.

- As identity information, and specially credentials, are not stored by a central Identity Provider, SSI **reduces the risk of massive identity theft**.

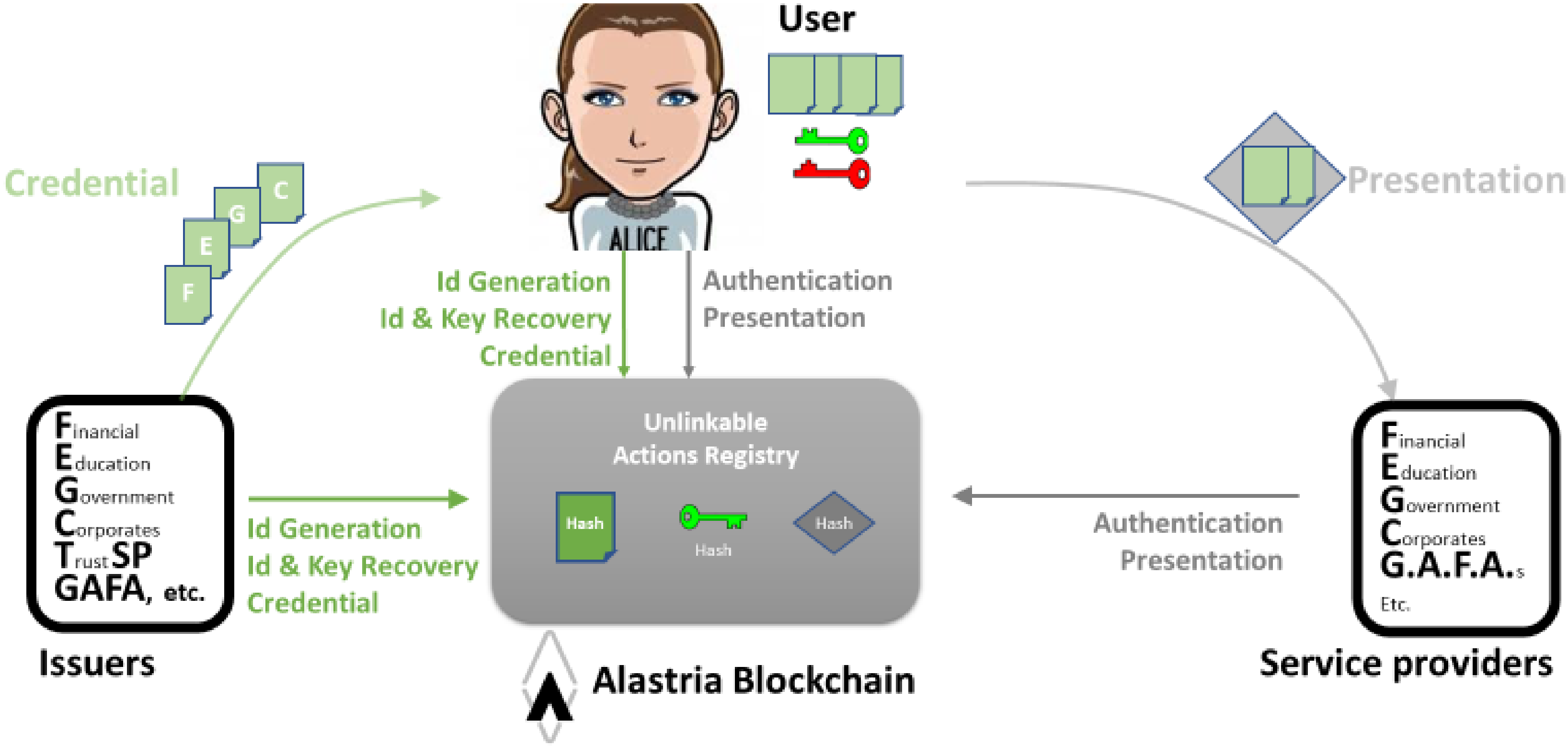
- The SSI “Identity Provider” (the claim/credential issuer) does not intervene in the authentication process, and therefore has not information about the online user activity, **reducing** the “big brother” risk and **GDPR compliance costs**.

- SSI allows the user to decide **which identity data to share**, with whom, and with which limits and constraints for third parties, even using zero knowledge proofs.

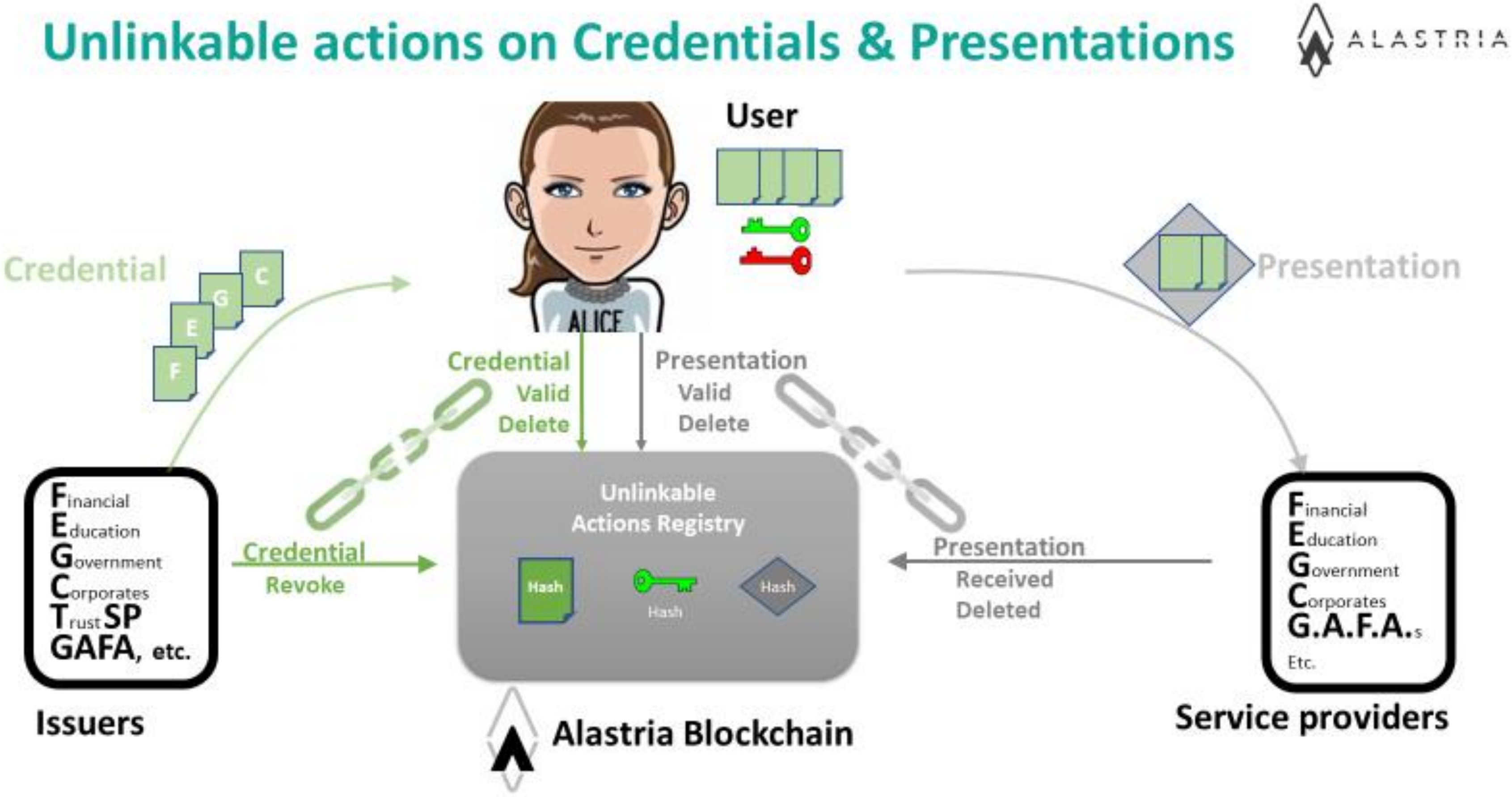
- Even if SSI allows revocation of credentials, the base identity (the Decentralised ID or ID) can not be suspended nor revoked except by the user, **ending with “digital feudalism” business models**, aligning identity management with GDPR principles.

AN SSI IMPLEMENTATION EXAMPLE – 1

Privacy by design: unlinkable actions

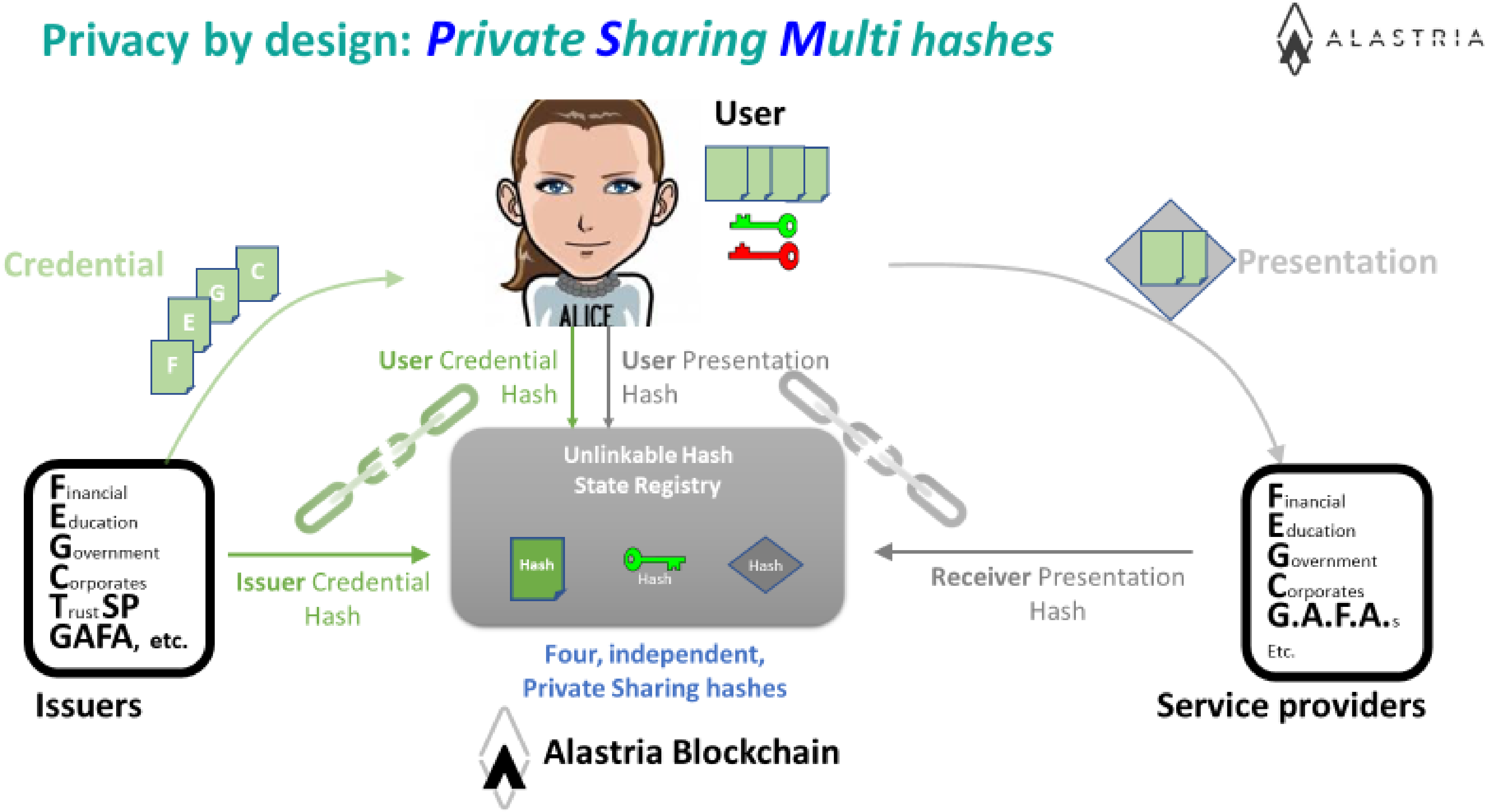


AN SSI IMPLEMENTATION EXAMPLE – 2



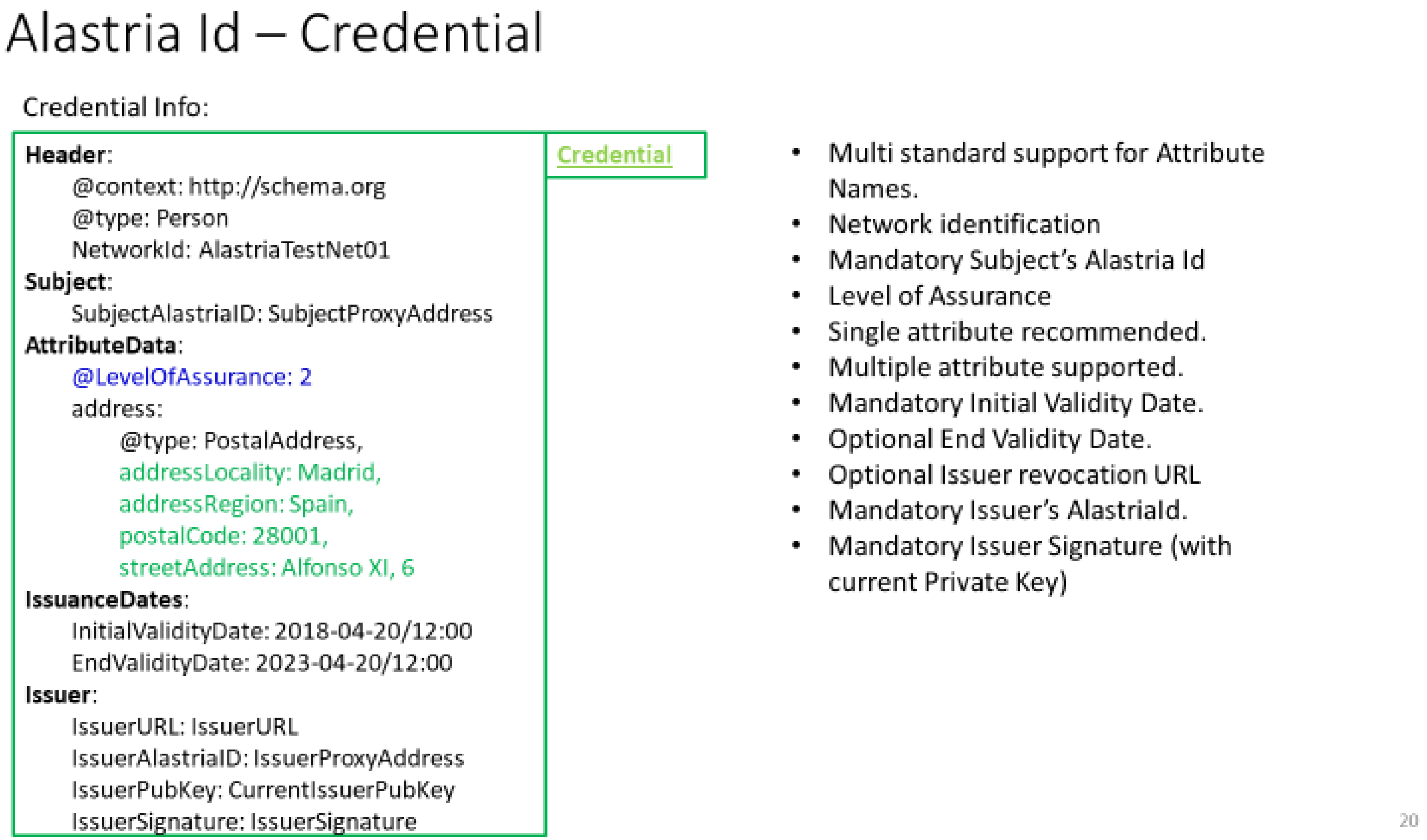
AN SSI IMPLEMENTATION EXAMPLE – 3

Privacy by design: *Private Sharing Multi hashes*



ALASTRIA
User
ALICE
Credential
C
G
E
F
Presentation
User Credential Hash
User Presentation Hash
Unlinkable Hash State Registry
Hash
Hash
Hash
Financial Education Government Corporates Trust SP GAFA, etc.
Issuers
Issuer Credential Hash
Receiver Presentation Hash
Financial Education Government Corporates G.A.F.A.s Etc.
Service providers
Four, independent, Private Sharing hashes
Alastria Blockchain

AN SSI IMPLEMENTATION EXAMPLE – 4



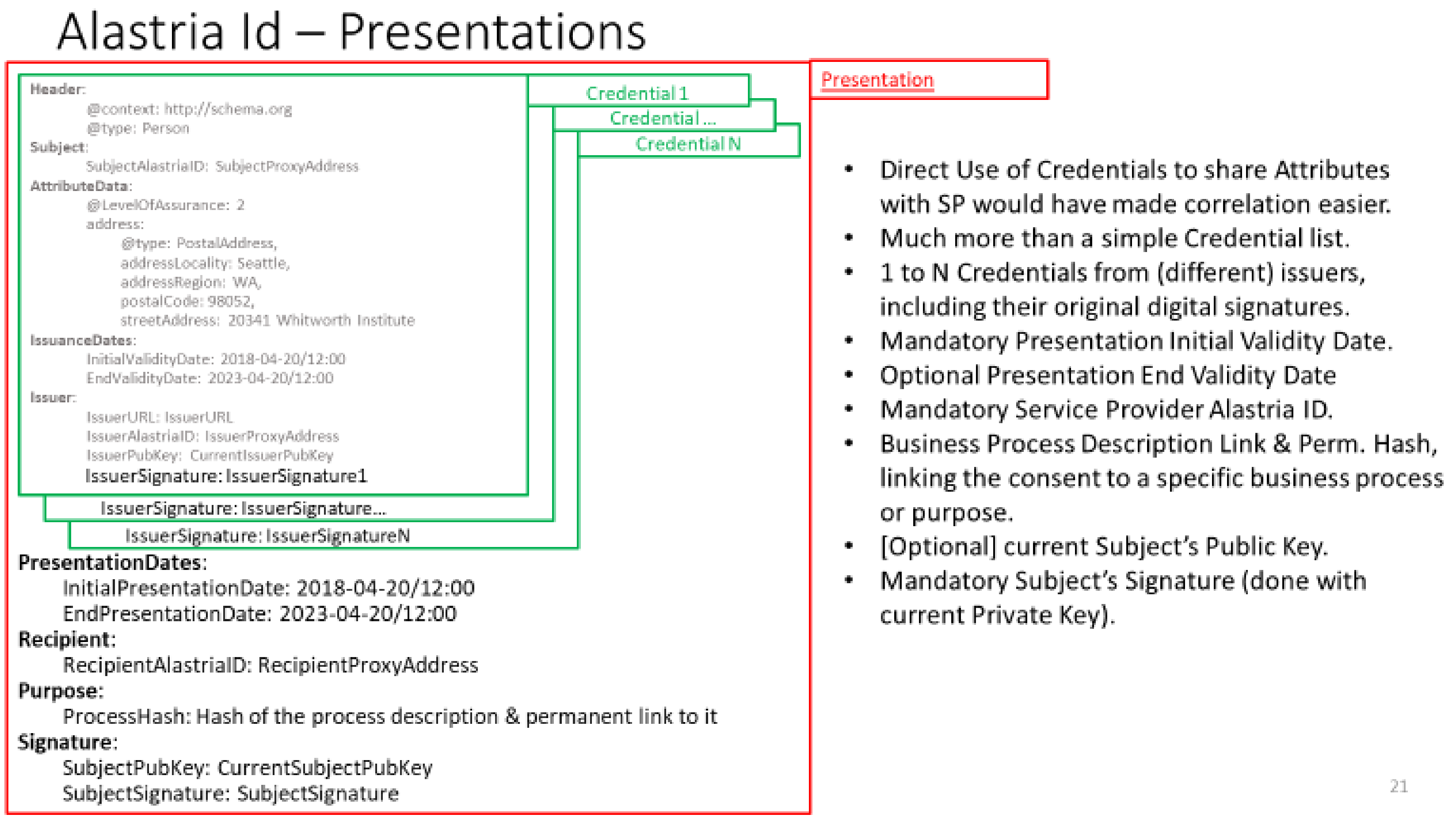
Alastria Id – Credential

Credential Info:

```
Header:
        @context: http://schema.org
        @type: Person
        NetworkId: AlastriaTestNet01
Subject:
        SubjectAlastriaID: SubjectProxyAddress
AttributeData:
        @LevelOfAssurance: 2
        address:
                @type: PostalAddress,
                addressLocality: Madrid,
                addressRegion: Spain,
                postalCode: 28001,
                streetAddress: Alfonso XI, 6
IssuanceDates:
        InitialValidityDate: 2018-04-20/12:00
        EndValidityDate: 2023-04-20/12:00
Issuer:
        IssuerURL: IssuerURL
        IssuerAlastriaID: IssuerProxyAddress
        IssuerPubKey: CurrentIssuerPubKey
        IssuerSignature: IssuerSignature
```

- Multi standard support for Attribute Names.
- Network identification
- Mandatory Subject's Alastria Id
- Level of Assurance
- Single attribute recommended.
- Multiple attribute supported.
- Mandatory Initial Validity Date.
- Optional End Validity Date.
- Optional Issuer revocation URL
- Mandatory Issuer's AlastriaId.
- Mandatory Issuer Signature (with current Private Key)

AN SSI IMPLEMENTATION EXAMPLE – 5



Alastria Id – Presentations

Credential 1

Credential …

Credential N

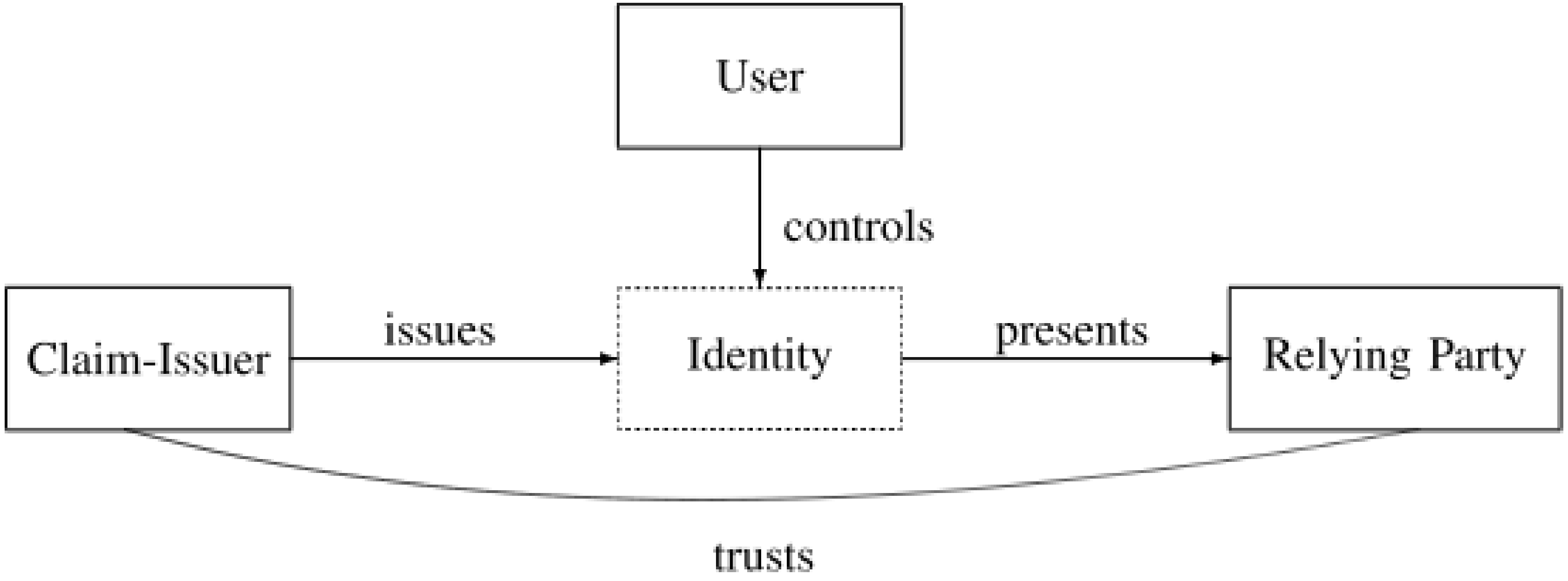
Presentation

```
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: IssuerSignature1
          IssuerSignature: IssuerSignature…
            IssuerSignature: IssuerSignatureN
PresentationDates:
      InitialPresentationDate: 2018-04-20/12:00
      EndPresentationDate: 2023-04-20/12:00
Recipient:
      RecipientAlastriaID: RecipientProxyAddress
Purpose:
      ProcessHash: Hash of the process description & permanent link to it
Signature:
      SubjectPubKey: CurrentSubjectPubKey
      SubjectSignature: SubjectSignature
```

- Direct Use of Credentials to share Attributes with SP would have made correlation easier.
- Much more than a simple Credential list.
- 1 to N Credentials from (different) issuers, including their original digital signatures.
- Mandatory Presentation Initial Validity Date.
- Optional Presentation End Validity Date
- Mandatory Service Provider Alastria ID.
- Business Process Description Link & Perm. Hash, linking the consent to a specific business process or purpose.
- [Optional] current Subject's Public Key.
- Mandatory Subject's Signature (done with current Private Key).

21

SSI TRUST RELATIONS DO NOT ESSENTIALLY CHANGE...

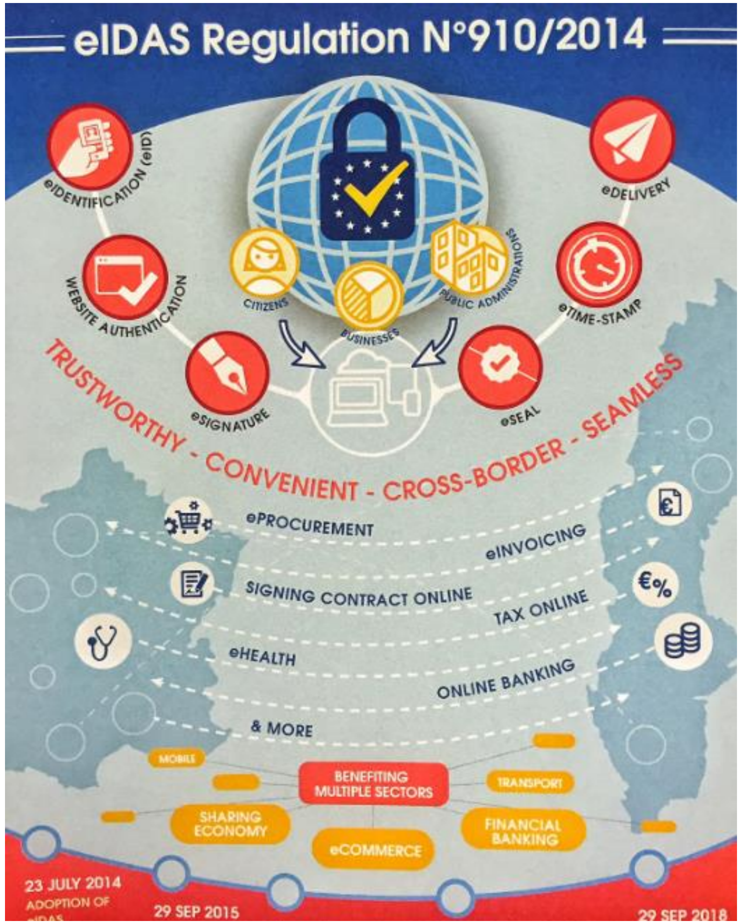


A. Mühle et al. / Computer Science Review 30 (2018) 80–86

SSI CHALLENGES. THE NEED FOR TRUST ANCHORS

- We still need to identity the “real identity” of a DID subject, in a trustworthy manner, both to issue credentials and to consume them.
- We need to define governance frameworks for the **usage of SSI in legally binding transactions**, where social trust frameworks may not be acceptable in terms of liability or regulatory compliance (e.g. in KYC/AML environments).
  - Verifiable credentials level.
  - DID level.
  - Key management level.
  - DLT (Blockchain) level.
- **Trust anchors**, well defined in identity trust frameworks, may be really helpful. Especially when based in a well defined and tech-neutral Law…

EIDAS: THE DSM TRUST FOUNDATION



- “Electronic identification (eID) and electronic Trust Services (eTS) are **key enablers** for secure cross-border electronic transactions and central building blocks of the Digital Single Market […] a **milestone** to provide a predictable regulatory environment to **enable secure and seamless** electronic interactions between businesses, citizens and public authorities” (Comisión Europea, 2015).

EIDAS: THE DSM TRUST FOUNDATION

- “By providing the building blocks for ensuring trust, convenience, and security in the online environment, the eIDAS regulation represents a **major contribution to the European Digital Single Market** […] opens the door for end-to-end electronic transactions and processes that **replace the traditional activities and manual processes**, while keeping the **same legal value** […] opportunities for organizations implementing eIDAS trust services are **evident**: increase the efficiency of the business processes, reduce their operational costs, grow their business, and build a competitive advantage” (Deloitte, 2016).

- “The GDPR and eIDAS are seen as providing the **right foundation** for a true DSM […] eIDAS is often presented as an excellent initiative with **impact beyond European borders** […] an example of an **EU success**. Its regulation and specifications have managed to set a **common framework in a fragmented market** for using digital services across Europe” […] digital identity and e-services are **crucial for EU nationals**, and can also help with European challenges such as the current migration crisis” (PwC, 2018).

WHY EIDAS REGULATION?

- eIDAS Regulation constitutes the main **electronic identification trust framework** in the European Economic Area.

- eID is a **building block of the Digital Single Market**, allowing the establishment of cross-border distance electronic relations in the e-Government field.

- eIDAS may be extended to include the recognition of **eIDs for private sector uses**, such as AML/CFT.

- Its **technology-neutral approach** could easily allow the usage of SSI systems, constituting a real opportunity for their adoption.

- eIDAS Regulation has a **strong influence in the international regulatory space**, thanks to UNCITRAL recent works.

WHY EIDAS REGULATION?

- Directive (EU) 2015/849 of the European Parliament and of the Council of 20 May 2015 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, modified by Directive (EU) 2018/843 of the European Parliament and of the Council of 30 May 2018.

- Article 13. 1. Customer due diligence measures shall comprise:
  - (a) identifying the customer and verifying the customer’s identity on the basis of documents, data or information obtained from a reliable and independent source, **including, where available, electronic identification means, relevant trust services as set out in Regulation (EU) No 910/2014 of the European Parliament and of the Council** or any other secure, remote or electronic identification process regulated, recognised, approved or accepted by the relevant national authorities;

SSI/EIDAS USE CASES – 1

- Using eIDAS identification means and qualified certificates to create verifiable claims
  - The first use case considers the utilization of an electronic identification system for the validation of the identity attributes that are to be included in any assertion contained in the DID document. This would be a scenario in which a means of identification recognized in accordance with the eIDAS Regulation is used to verify the information that will be included in a DID document (i.e., using a special kind of oracle that verifies the eIDAS eID to pass the information to the DID creator).
  - eIDAS Interoperability regulation defines minimum data sets for natural persons and for legal persons, while Annexes I and III of eIDAS Regulation define the same data set in the case of qualified certificates. The main advantage of using this approach is that the DID inherits the level of assurance of the eIDAS electronic identification means, allowing a person with this kind of eID, which is centralized, to get DIDs and leveraging their use in the space of decentralized transactions, gaining real privacy.

SSI/EIDAS USE CASES – 2

- Using SSI VC as an eIDAS identification means
  - Although electronic identification under eIDAS Regulation is today clearly aligned with SAML-based infrastructures (see Opinion No. 2/2016 of the Cooperation Network on version 1.1 of the eIDAS Technical specifications, and eIDAS eID Profile, nothing in the eIDAS or its implementing acts should prevent the usage of a SSI system as an electronic identification means.
  - Thus, the second use case considers a DID as an eIDAS compliant electronic identification means, enabling - at least - transactions with Public Sector authorities and Public Administrations and, if so decided by the DID creator, also with private sector entities, for AML/CFT and other uses.

FINAL THOUGHTS

- SSI is a new paradigm for identity management, more privacy respecting, more secure and flexible, which will allow user's to share, under total controls, their identity data.
- It might foster the rise of new business models, shifting from data feudalism to data self control, according to and beyond GDPR.
- It will help the development of decentralised processes based in Blockchain, in support of currency, electronic payments, titles, transfers, and other financial use cases.
- But we need to be able to trust SSI data to comply with regulation. Although is not the only solution, we can re-use the trust anchors set forth under eIDAS.

THANKS!

MORE INFORMATION: IGNACIO.ALAMILLO@LOGALTY.COM

Frankfurt, 19/06/2019