SEAL Project
StudEnt And citizen identities Linked

SEAL meets Self-Sovereign Identity trajectory path

Presentation at the Project Monitoring Group
03.04.2020 | version 1.0

Petros Kavassalis, UAegean | i4m Lab
Nikos Triantafyllou, UAegean | i4m Lab

GRANT AGREEMENT UNDER THE CONNECTING EUROPE FACILITY (CEF) - TELECOMMUNICATIONS SECTOR AGREEMENT INEA/CEF/ICT/A2018/1633170.
Action No: 2018-EU-IA-0024

Agenda

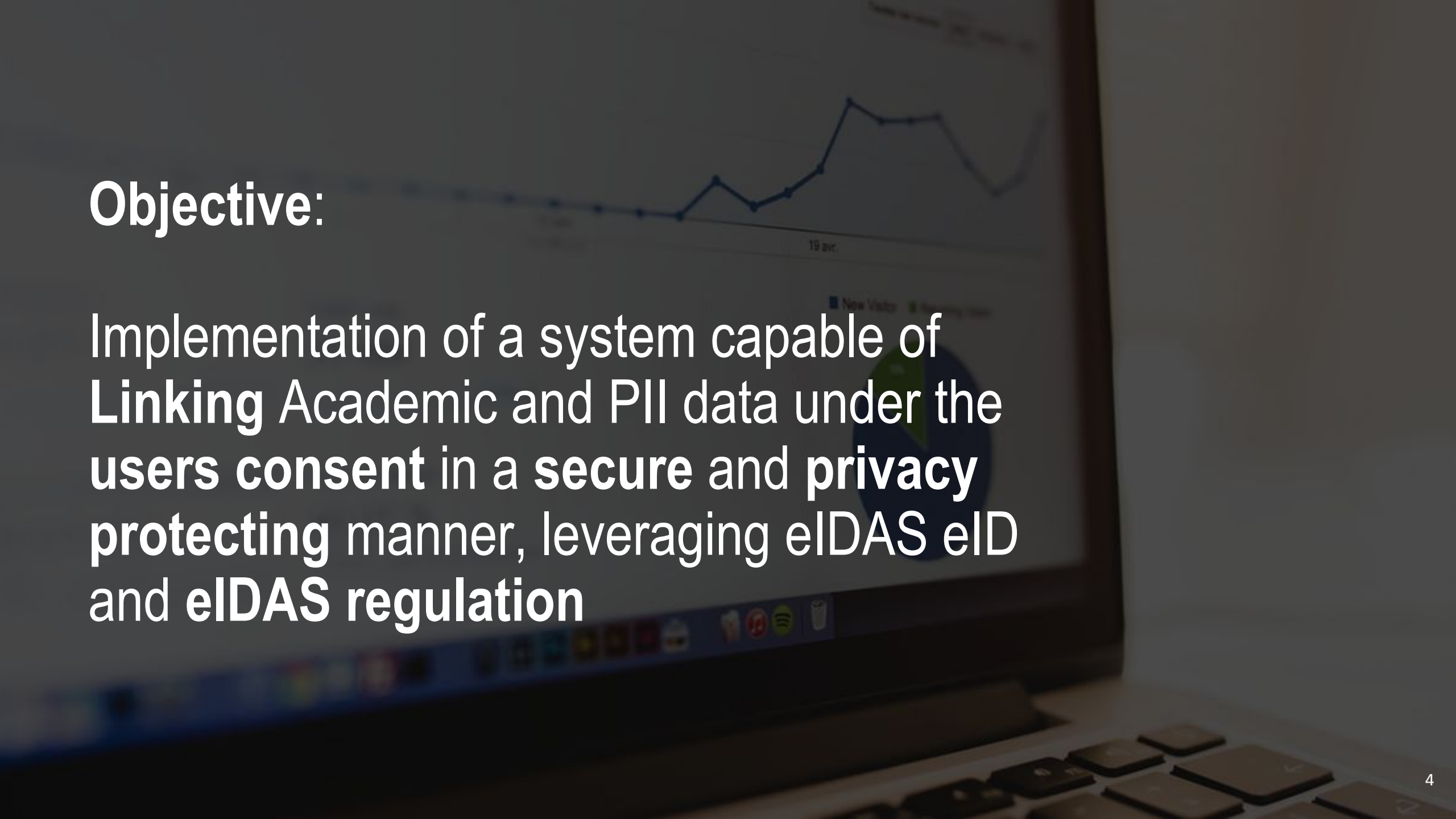
01 SEAL Self Sovereign Identity (SSI) enabled Service

02 SEAL SSI Use Cases

03 SEAL SSI Recap and Demo

1|3

SEAL Self Sovereign Identity (SSI) enabled Service

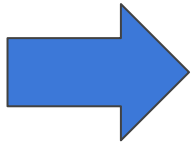


Objective:

Implementation of a system capable of **Linking** Academic and PII data under the **users consent** in a **secure** and **privacy protecting** manner, leveraging eIDAS eID and **eIDAS regulation**

The Problem

- **Identity is fragmented:** sum of attributes that exist about us* in siloed IdPs/APs
- **Integration is limited**: Sources of identity information about us are constantly growing and evolving
- **Academic Sector even more fragmented**! Student and faculty mobility increases the fragmentation of the information about us
- eIDAS Identifiers **meaningless** in most Academic APs



- **Centralised solution** poses huge risks**: Identity theft****
- **Interconnection** of various Academic APs and PII IdPs **costly**
- **Consequent authentication** (serial authentication with many IdP/AP providers) leads to a very bad user experience: **service drop out**

*https://www.eesc.europa.eu/sites/default/files/files/1._panel_-_daniel_du_seuil.pdf

** https://techjury.net/stats-about/identity-theft/

SEAL SSI approach: Verifiable Credentials

- **Verifiable Credentials** (VCs) as a means of **Identity Linking** removes the need for interoperability between data sources
- **VCs** are **tamper-evident credentials** that have authorship and can be cryptographically verified
- VCs under the users control, create no honey pots, protect users privacy
- **VCs** can cover **more than PII** (extended Student Identity)

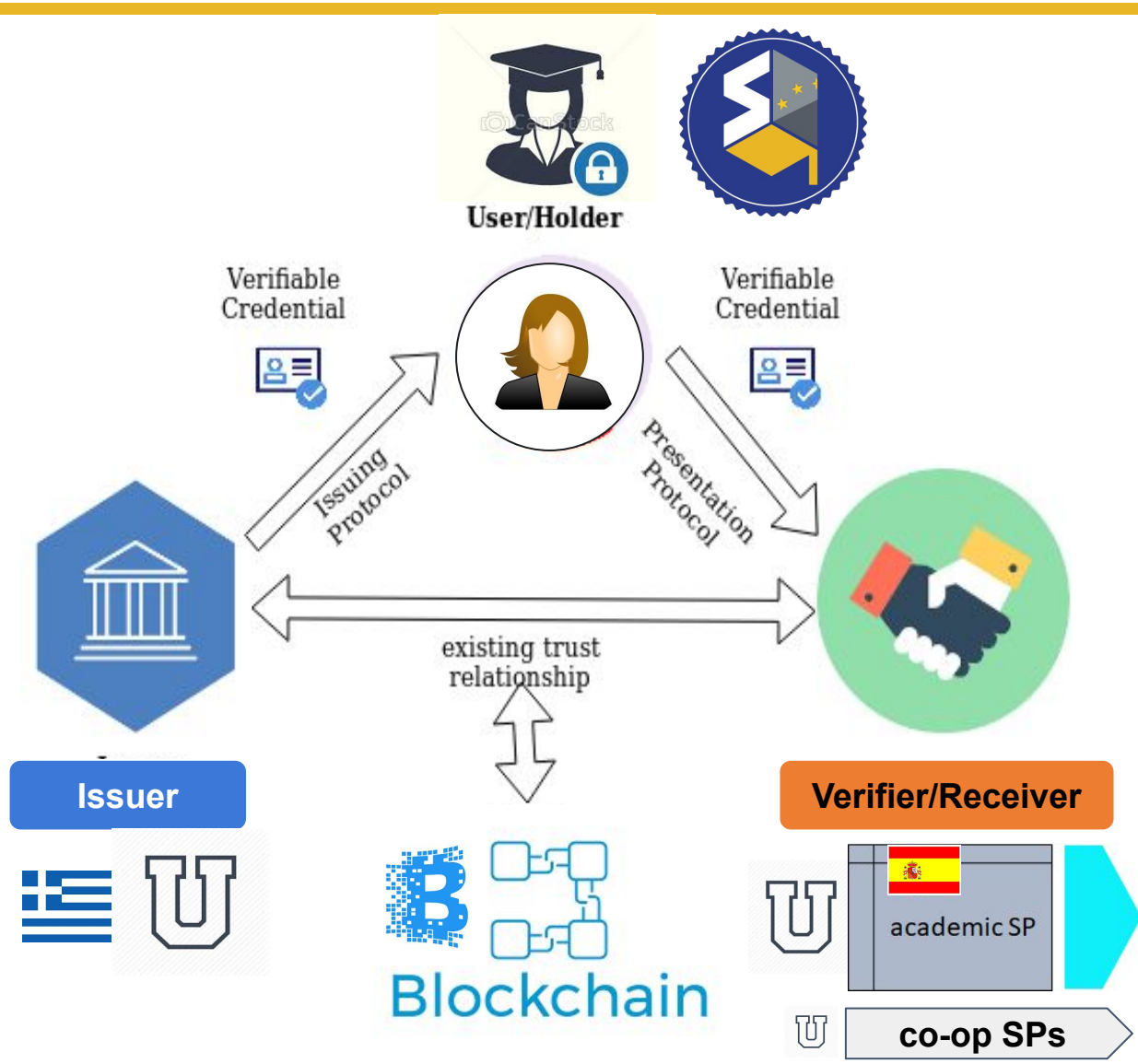
SEAL SSI Service (in brief)

At a high level the flow is as follows:

- **User** access the SEAL SSI Issuer service
- At the **SEAL SSI Issuer** service they **authenticate** to the various connected **IdPs**
- **Issue VCs** based on the retrieved attributes
- SEAL Issuer may perform additional **linking processes** (derivative VCs)
- **Present** such VCs **to SPs**, who verify them, to gain access to their services

Main **Actors** in SSI:

- Issuers
- User/Holders/Subjects
- Verifiers/Receivers



SEAL SSI Service Model (in more details)

1 SEAL SSI Service Provision side

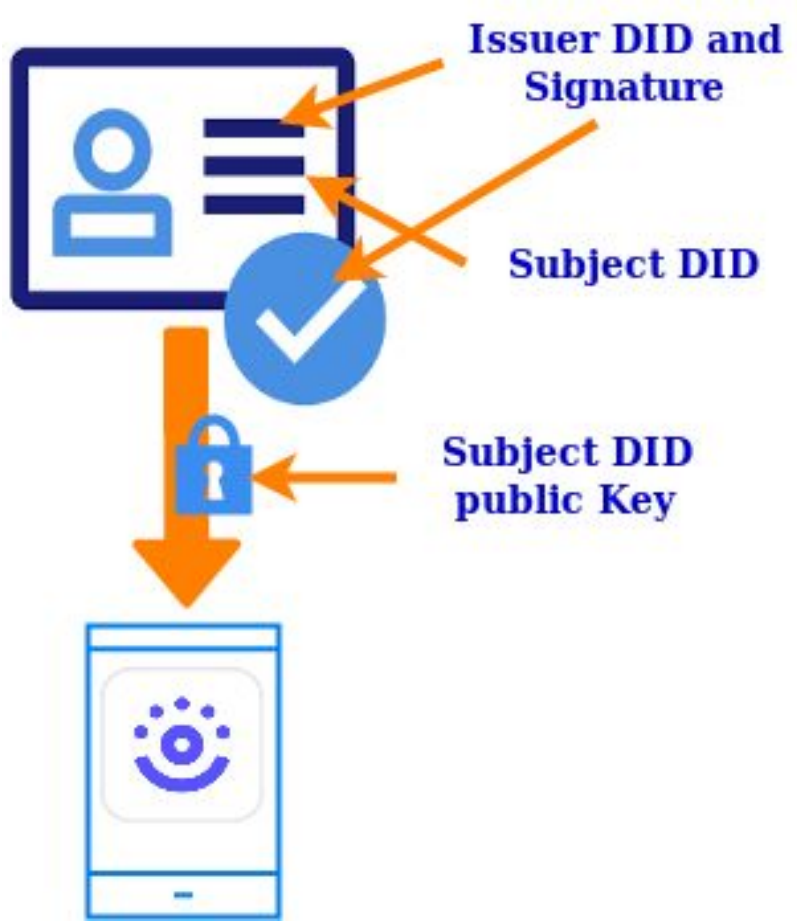
- User accesses the SEAL Service via a web browser
- Authenticates through her **eIDAS eID**
- (using the API Manager) Selects the issuance of Verifiable Credentials
- Access the available data sources connected to Athens ESMO GW (eIDAS eID, eduGain etc.) | https://esmo-gateway.eu/about/
- Selects which of the available data to use for issuing VCs
- VCs are sent to the user's wallet app where the user reviews, accepts and stores them
- VCs link identities (civil, academic etc.) through the built-in Linking Service support

2 SEAL SSI Service Consumption side

- User accesses HEI Services (SP)
- User is asked to authenticate by presenting one of more VC generated by the SEAL Issuer service
- User's wallet prompts the user who authorizes the transfer of the requested VC(s)
- VCs are verified based on: authenticity, ownership, expiration and revocation
- HEI SP grants access to the service accordingly

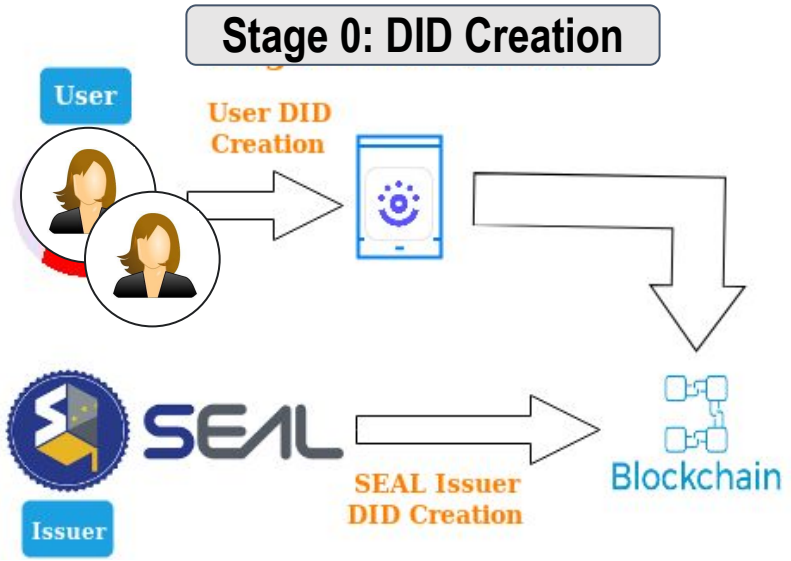
Verifiable Credential (VCs) need Decentralized Identifiers (DIDs)

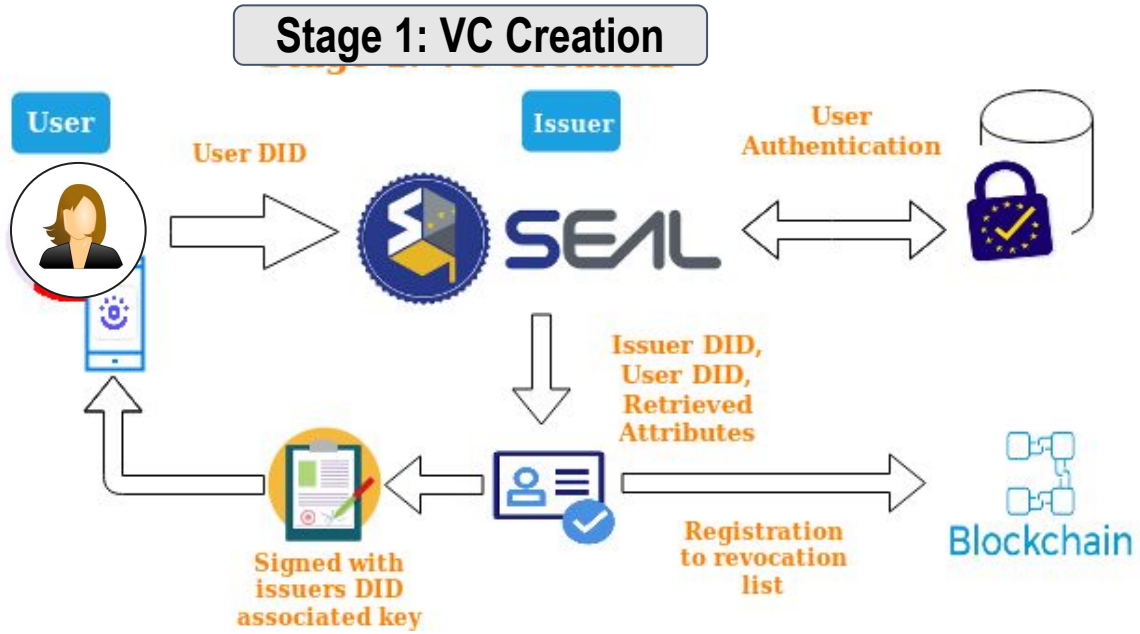
- W3C: A Decentralized Identifier (DID) is a new type of identifier that is globally unique, persistent, resolvable with high availability, cryptographically verifiable and decentralized
- DIDs can be used to anchor the identity of the Issuer of a VC and the subject of it
- The public key associated with the DID of the Issuer is used to sign a VC
- VCs are transferred to the subjects wallet encrypted using their public key

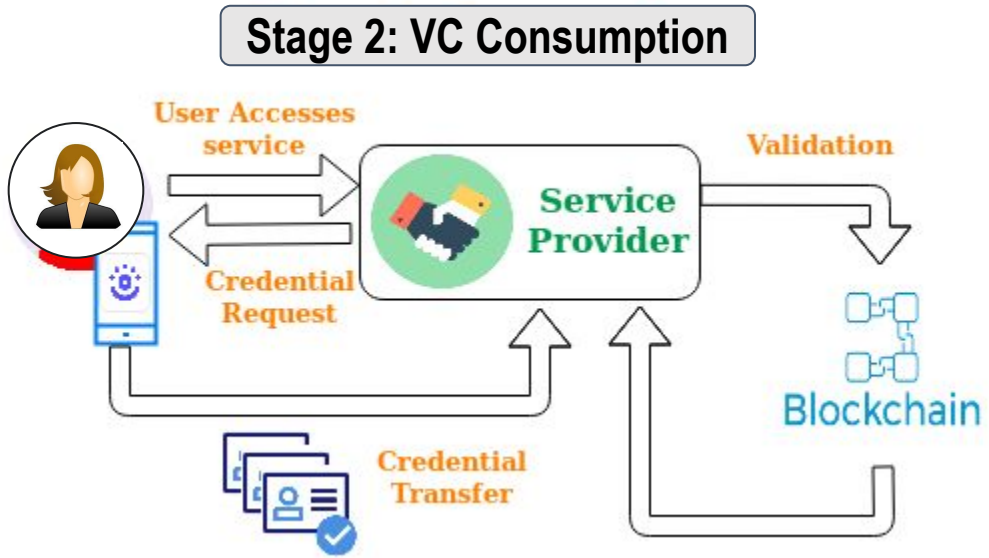


The life-cycle of a Verifiable Credential

From personal attributes retrieval to the VC storage in user's wallet



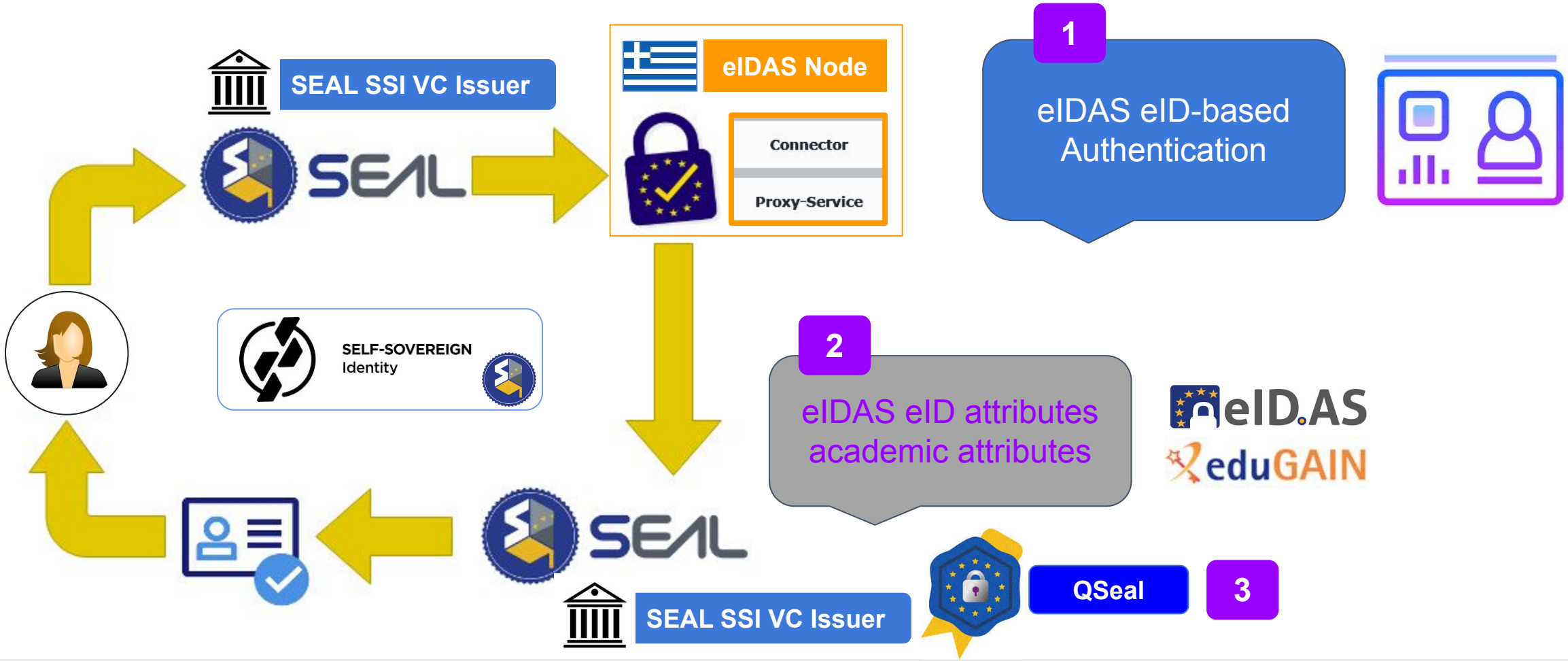




**SPs can delegate VC verification to SEAL using OIDC/SAML protocols, minimizing entry costs

SEAL SSI Service: the specificity of VC creation process

helicopter view



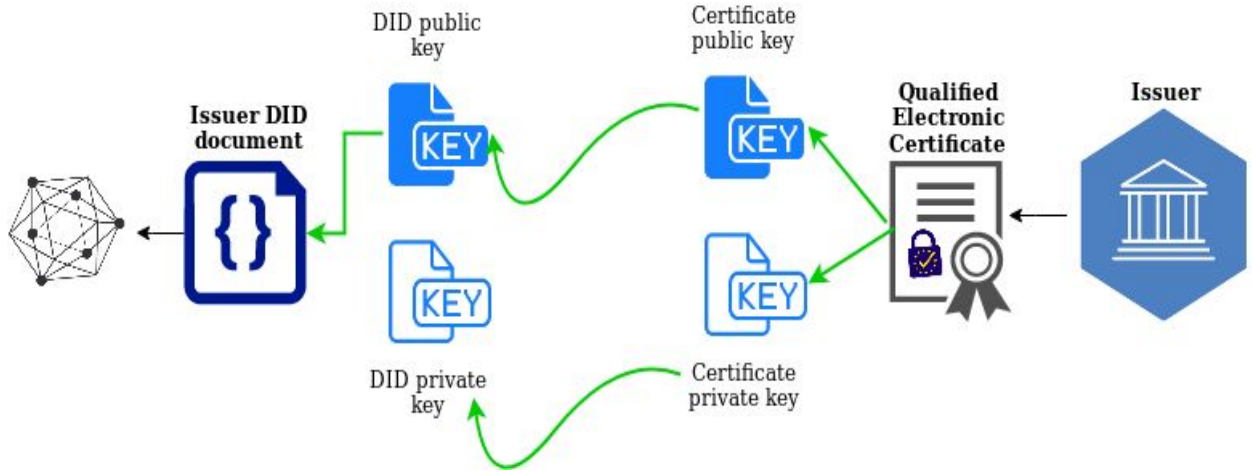
Create Verifiable Credentials (VCs) via a SEAL SSI Issuer

1. eIDAS eID-based Authentication
2. Credentials (VCs) always have eIDAS eID Unique Identifier (UI) as Header
3. Credentials (VCs) are signed with a Qualified eSeal (QSEAL)

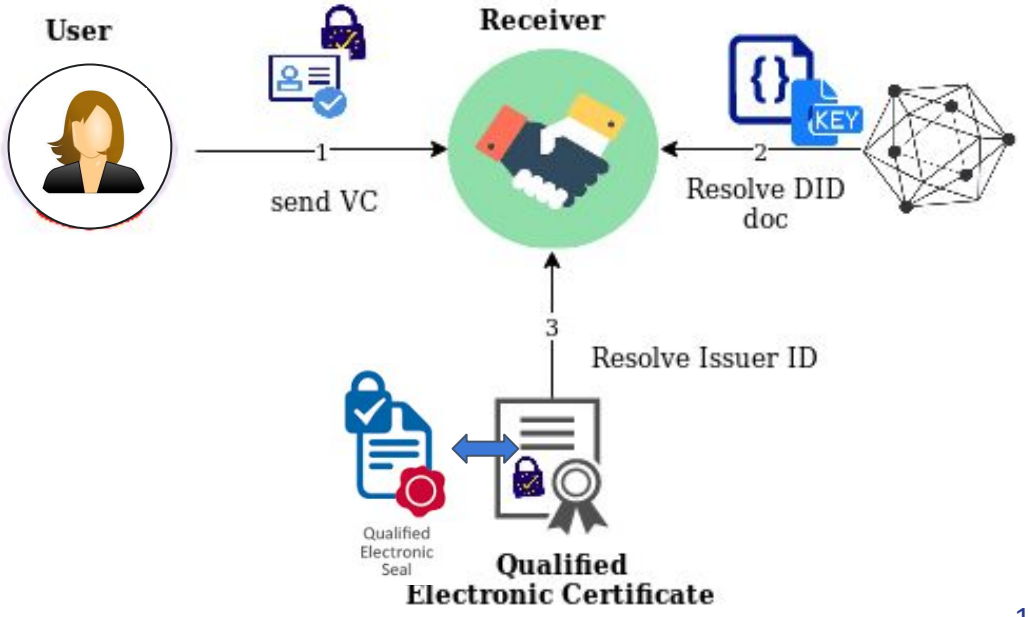
SEAL SSI Service: the specificity of VC creation process

eIDAS standards complied

- **A SSI VC Issuer** establishes an identity using Decentralized Identifiers (DIDs)
  - DIDs are URLs that relate a DID subject to means for trustable interactions with that subject and enable the controller to prove control over them
  - DIDs are publically discoverable

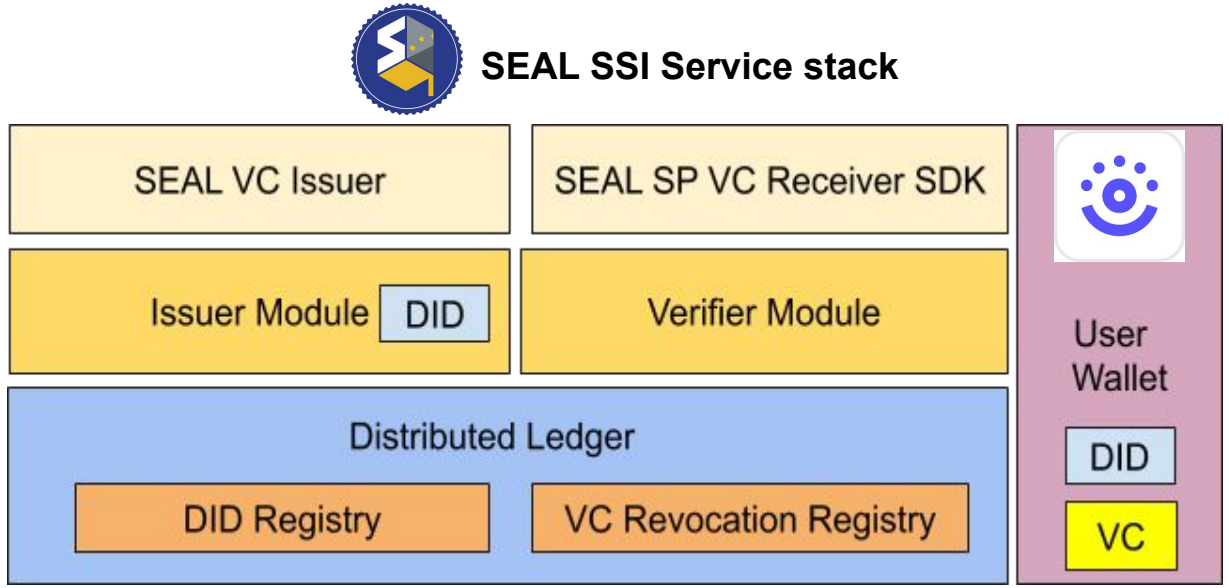


- **A SEAL VC Issuer** builds its DID using a **Qualified eIDAS electronic Seal (QSEAL)** enabling eIDAS supported SSI. This way:
  - The link between the DID and the actual identity can be easily achieved by using the pair of keys corresponding to a qualified certificate
  - The identity of the Issuer is associated to the content signed or sealed
  - The VC signature will have the status of a qualified signature produced with am eIDAS Qualified Certificate according to the eIDAS Regulation.



SEAL SSI Service Architecture

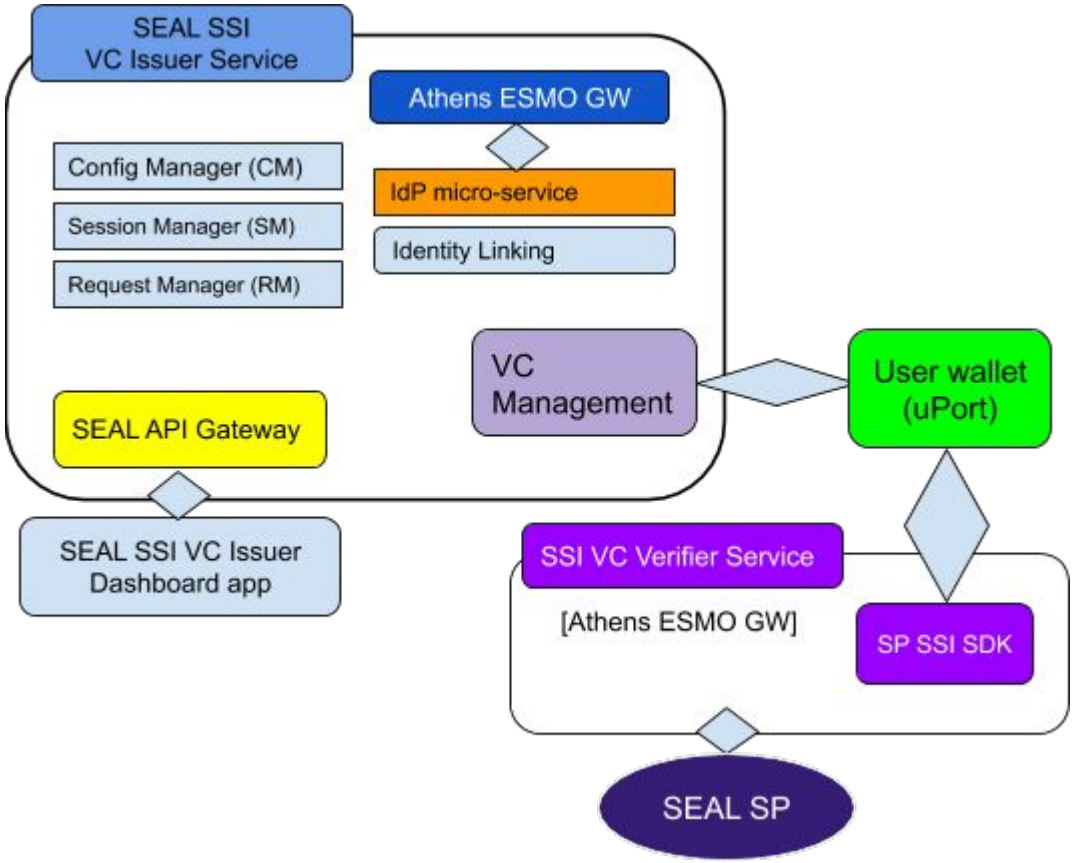
- **DID**: Decentralized Identifier, adhering to the W3C standards
- **DID Registry**: DID Document Resolution Registry
- **VC**: Verifiable Credentials adhering to the W3C standards attesting to a set of identity claims about a subject
- **VC Revocation Registry/List**: Registry to store the validity status of issued Credentials
- **User Wallet**: User controlled application, situated in users mobile device

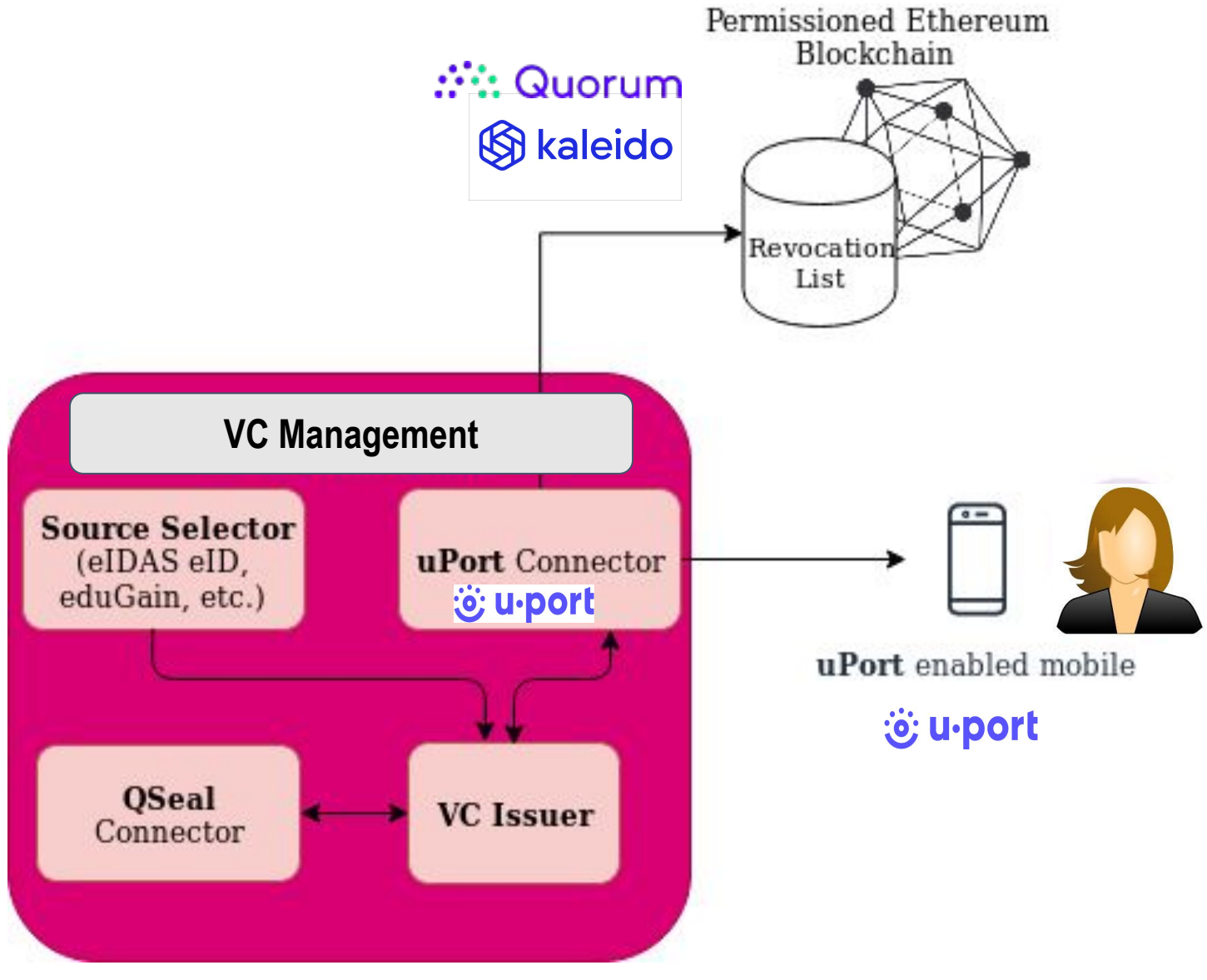


- **SEAL SSI VC Issuer:** SEAL service capable of issuing VCs to user's Wallets based on the retrieved data sets and signing them using Qualified eIDAS Seal
- **Issuer Module:** Module capable of generating VC and signing them with a QSEAL certificate

- **SEAL SSI VC Receiver (SP)**: SDK capable of requesting SEAL issued VCs and verify them
- **Verifier Module**: Module capable of requesting sets of VCs and validating them

SEAL SSI Service Components



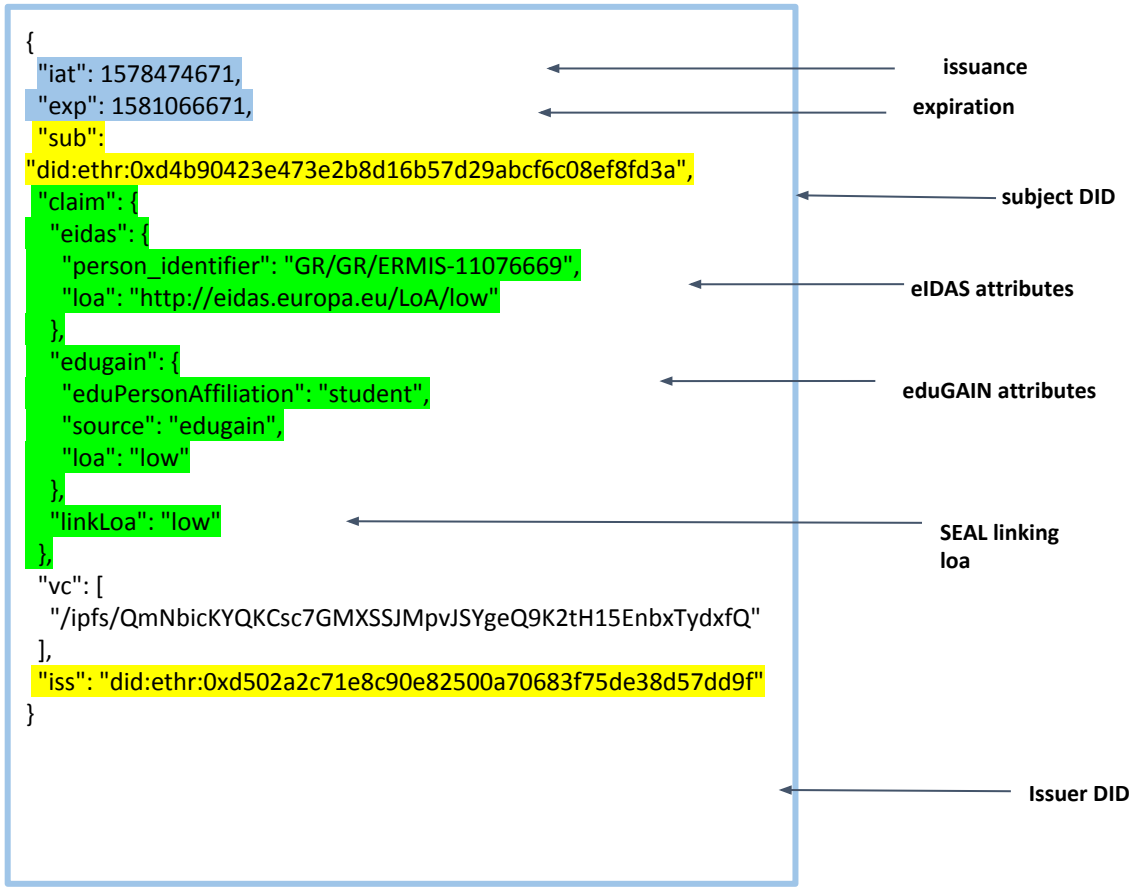


An eIDAS eID Verifiable Credential example
standard offering

- JSON-LD / JWT
- Signed by the VC Issuer
- Bound to the user cryptographically
- User proves ownership of VC
- VCs are individually revocable
- VCs contain a specific Time-To-Live (TLT)

An “isStudent” Verifiable Credential example
minimal

- Links:
  - eIDAS eID
  - eduGAIN
- Linking LoA:
  - Low
  - Matching of name, surname, date of birth



A Verifiable Credential instantly creates a linked identity

The concept of Linking Service

- Verifiable Credentials contain explicitly a **subject** (i.e. the owner) using DIDs
- **Subjects** are the **only** entities that can prove **ownership of a DID**
- DIDs offer an **native** Identity Linking mechanism
  - Different VCs can be used together by the holder to prove a linked identity profile (e.g. eIDAS VC and eduGAIN VC)
  - Minimum linking profile
- **Linking Profiles** are required for sensitive services
  - Minimum linking guarantees same entity identified successfully at the data sources
  - Not that they belong to the same person

2|3

SEAL SSI Use Cases

SEAL SSI Service Use Cases framework

- **Issuer**
  - The entity that can issue **Verifiable Credentials (VC)s** about individuals retrieved from the various Data Sources that is available to it (a Verifiable Credential is a piece of information that is cryptographically trustworthy)
    - **GUnet** GUnet ΑΚΑΔΗΜΑΪΚΟ ΔΙΑΔΙΚΤΥΟ UNIVERSITY OF THE AEGEAN
- **User/Holder/Subject**
  - A student (or any person affiliated with an HEI) who interacts with SEAL Issuers is identified by them (by any means available, even physical) in order to get issued a VC about themselves. VCs are securely stored on her mobile phone under the sole control of the Holder called a "**Wallet**"
    - **uPort** u·port
- **Receivers/Verifiers**
  - Any HEI Online Service that is capable of accepting and validating Verifiable Credentials and grant access accordingly
    - **UAegean Online Services (Smart Class etc). Also:**

UNIVERSITY OF THE AEGEAN

UNIVERSITAT JAUME I

U.PORTO

UNIVERSIDAD DE MÁLAGA

UC1.1: User with SSI Wallet and valid VCs

Assumptions:

- The user is in possession of an SSI wallet compatible with SEAL (uPort, Jolocom*)
- The SP requires a set of VCs to authenticate the user (essentially requesting a SEAL linked identity with a suitable linking level of assurance)
- The user has been issued a set of VCs by the SEAL SSI Issuer service, matching the request of the SP. Finally those VCs are stored on the users wallet

Flow:

- User accesses the SP service and selects SSI authentication
- User is prompted to scan a QR code with their wallet app
- The user's wallet app requests their consent (and does a biometric check to verify the user)
- After consent is given the wallet propagates the VCs to the SP
- The received VCs are verified for authenticity, ownership and validity
- If all checks pass the user is authenticated to the SP service

*Jolocom compatibility will be evaluated at a later stage of the project, but multiple wallet providers will be available

UC1.2: User with SSI Wallet and invalid VCs

Assumptions:

- The user is in possession of an SSI wallet compatible with SEAL (uPort, Jolocom*)
- The SP requires a set of VCs to authenticate the user (essentially requesting a SEAL linked identity with a suitable linking level of assurance)
- The user had been issued a set of VCs by the SEAL SSI Issuer service, matching the request of the SP that are now **expired**

Flow:

- User accesses the SP service and selects SSI authentication
- User is prompted to scan a QR code with their wallet app
- The wallet app informs the user that (some) of the VCs requested by the SP are not available
- The wallet app presents the link (to the SEAL SSI Issuer service) to obtain the requested VCs
- The wallet app opens a browser for the user to navigate to the SEAL SSI issuer service and (after authenticating through the requested data sources) issue the requested type of VC to the user
- The flow now continues as UC 1.1

*Jolocom compatibility will be evaluated at a later stage of the project, but multiple wallet providers will be available

UC2: User with SSI Wallet and no VCs

Assumptions:

- The user is in possession of an SSI wallet compatible with SEAL (uPort, Jolocom*)
- The SP requires a set of VCs to authenticate the user (essentially requesting a SEAL linked identity with a suitable linking level of assurance)
- The user is not in possession of the requested by the SP VCs

Flow:

- User accesses the SP service and selects SSI authentication
- User is prompted to scan a QR code with their wallet app
- The wallet app informs the user that the VCs requested by the SP are not available
- The wallet app presents the link (to the SEAL SSI Issuer service) to obtain the requested VCs
- The wallet app opens a browser for the user to navigate to the SEAL SSI issuer service and (after authenticating through the requested data sources) issue the requested type of VC to the user
- The flow now continues as UC 1.1

*Jolocom compatibility will be evaluated at a later stage of the project, but multiple wallet providers will be available

UC3: User with no SSI Wallet

Assumptions:

- The user is **not** in possession of an SSI wallet compatible with SEAL (uPort, Jolocom*)
- The SP requires a set of VCs to authenticate the user (essentially requesting a SEAL linked identity with a suitable linking level of assurance)

Flow:

- User accesses the SP service and selects SSI authentication
- User is prompted to scan a QR code with their wallet app and is informed from where to download a suitable wallet app
- The user installs the required SSI wallet app
- The user scans the QR code
- The wallet app informs the user that (some) of the VCs requested by the SP are not available
- The wallet app presents the link (to the SEAL SSI Issuer service) to obtain the requested VCs
- The wallet app opens a browser for the user to navigate to the SEAL SSI issuer service and (after authenticating through the requested data sources) issue the requested type of VC to the user
- The flow now continues as UC 1.1

*Jolocom compatibility will be evaluated at a later stage of the project, but multiple wallet providers will be available

3|3

SEAL SSI Recap and Demo

Benefits of SEAL SSI approach

SEAL SSI Service offers:

- Full user control of the sharing of their personal identity data
- Linking of Academic and Citizen Identities over VCs
- Explicit Linking Level of Assurance
- Decentralized solution, no honeypots
- Minimize entry barriers for HEI SPs (using OIDC/SAML)
- Inherent decentralized blockchain benefits of integrity and accountability
- eIDAS regulation alignment

Nikos Triantafyllou

THANK YOU

for your attention

http://project-seal.eu/

UAegean i4m Lab | pkavassalis@aegean.gr

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No. 837854