

# Safe Chain Consortium Project

Identity, Cross Border and  
Blockchain

[www.aerosurete.com](http://www.aerosurete.com)

# Our customers Needs



- To be Allowed To load a high dangerous Goods Truck (Under Security plan such as explosives cat 1.1 for exple) , Both Identity of Truck driver needs to be verified at Guard Post and both his capability to drive the specified dangerous goods = Driver should be trained by an accredited training company and should be in period of validity ;
- Law enforcement Agencies In a context of terror threat, can potentially be requested by transport companies to screen the profile of the driver at any moment ( In France L 114-2 of CSI)
- Business to Employee / Government to Business / Government to Citizen RGPD Compliance Non disclosure

# European IT Spaghetti Model



# Interoperability or Common framework ?

- EIDAS
- EBSI Initiative
- Our vision

# Eidas Concepts

- Eidas objective : Mutual recognition between heterogeneous European electronic Identity, signature, seals, web certificates.
- Currently Eidas real Interoperability between EU Member states is still in progress ( even from a legal point of view)
- EBSI : EU project is aiming a global Pan European Platform for Blockchain Relation Ship between Citizen and Governments
- Source :  
[https://joinup.ec.europa.eu/sites/default/files/document/2020-04/SSI\\_eIDAS\\_legal\\_report\\_final\\_0.pdf](https://joinup.ec.europa.eu/sites/default/files/document/2020-04/SSI_eIDAS_legal_report_final_0.pdf)

## section 4 of Article 13b

- Nonetheless, under section 4 of Article 13b, “where justified by reason of the public interest in preventing identity misuse or alteration, Member States may, for the purposes of verifying an applicant’s identity, take measures which could require the physical presence of that applicant before any authority or person or body mandated under national law to deal with any aspect of the online procedures referred to in this Chapter, including the drawing up of the instrument of constitution of a company”. BUT **Member States shall ensure that the physical presence of an applicant may only be required on a case-by- case basis where there are reasons to suspect identity falsification, and that any other steps of the procedure can be completed online”.**

# Qualified trust provider : A Strict Liability Regime !

- Article 13 (1) “trust service providers shall be liable for damage caused intentionally or negligently to any natural or legal person due to a failure to comply with the obligations under this Regulation”
- “the intention or negligence of a qualified trust service provider **shall be presumed** unless that qualified trust service provider proves that the damage referred to in the first subparagraph occurred without the intention or negligence of that qualified trust service provider”

# Use of notified eIDAS eID means and qualified certificates to issue verifiable credentials

- The requirements for identity proofing are, therefore, detailed in the eIDAS Security Regulation, and they are more or less strict depending on the desired level of assurance
- We will assume that the minimum acceptable level of assurance for a Verifiable ID (or another verifiable credential) is substantial.



# High Trust Level Required !

- Where the person has been verified to be in possession of photo or biometric identification evidence recognised by the Member State in which the application for the electronic identity means is being made and that evidence represents the claimed identity, the evidence is checked to determine that it is valid according to an authoritative source; and the applicant is identified as the claimed identity through comparison of one or more physical characteristic of the person with an authoritative source.

# Exempt of renewing Identity Proofing !

- Where procedures used previously by a public or private entity in the issuer's Member State for a purpose other than the issuance of electronic identification means provide for an equivalent assurance level, confirmed by a conformity assessment body, and steps are taken to demonstrate that the results of the earlier procedures remain valid.
- Identity proofing and verification is based in a valid notified electronic identification means having the assurance level high.
- Identity proofing and verification is based in a valid electronic identification means having the assurance level high, confirmed by a conformity assessment body



# European Self Sovereign Identity Framework

---

12-06-2020

Daniel Du Seuil - ESSIF convenor

[daniel.duseuil@digipolis.be](mailto:daniel.duseuil@digipolis.be)

<https://ec.europa.eu/cefdigital/wiki/display/CEFDIGITAL/EBSI>

---



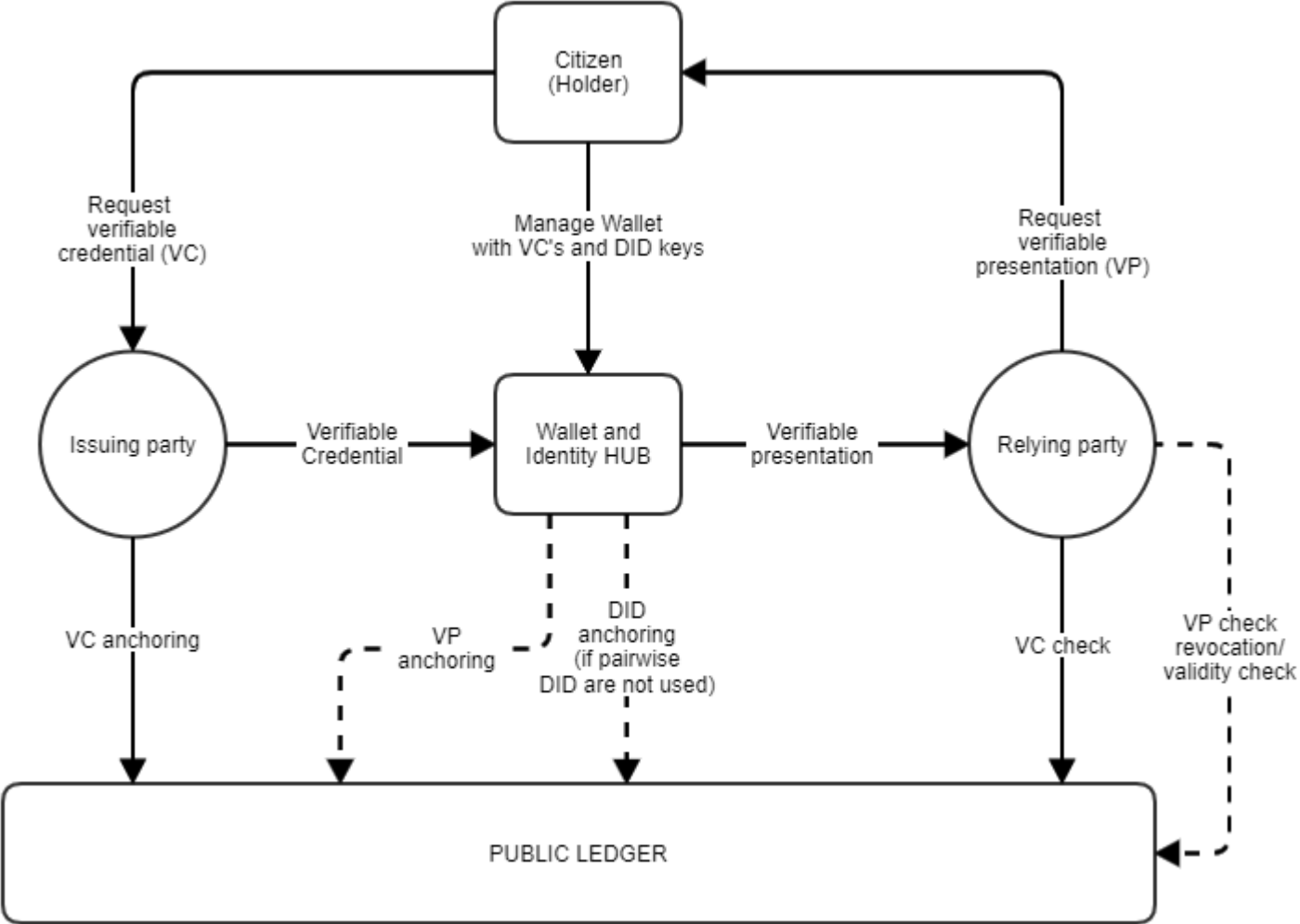
## Start of ESSIF (2018)

- How to collaborate in on the many cross border challenges of Self Sovereign identity in Europe?
- Initiative launched in EBP by Germany/ Nordrhein-Westfalen with help of Netherlands, Belgium and Italy.
- Use case and project in the European Blockchain Service Infrastructure (28 member states involved)
- Use case convenors: Daniel Du Seuil (Belgium) and Carlos Pastor (Spain)

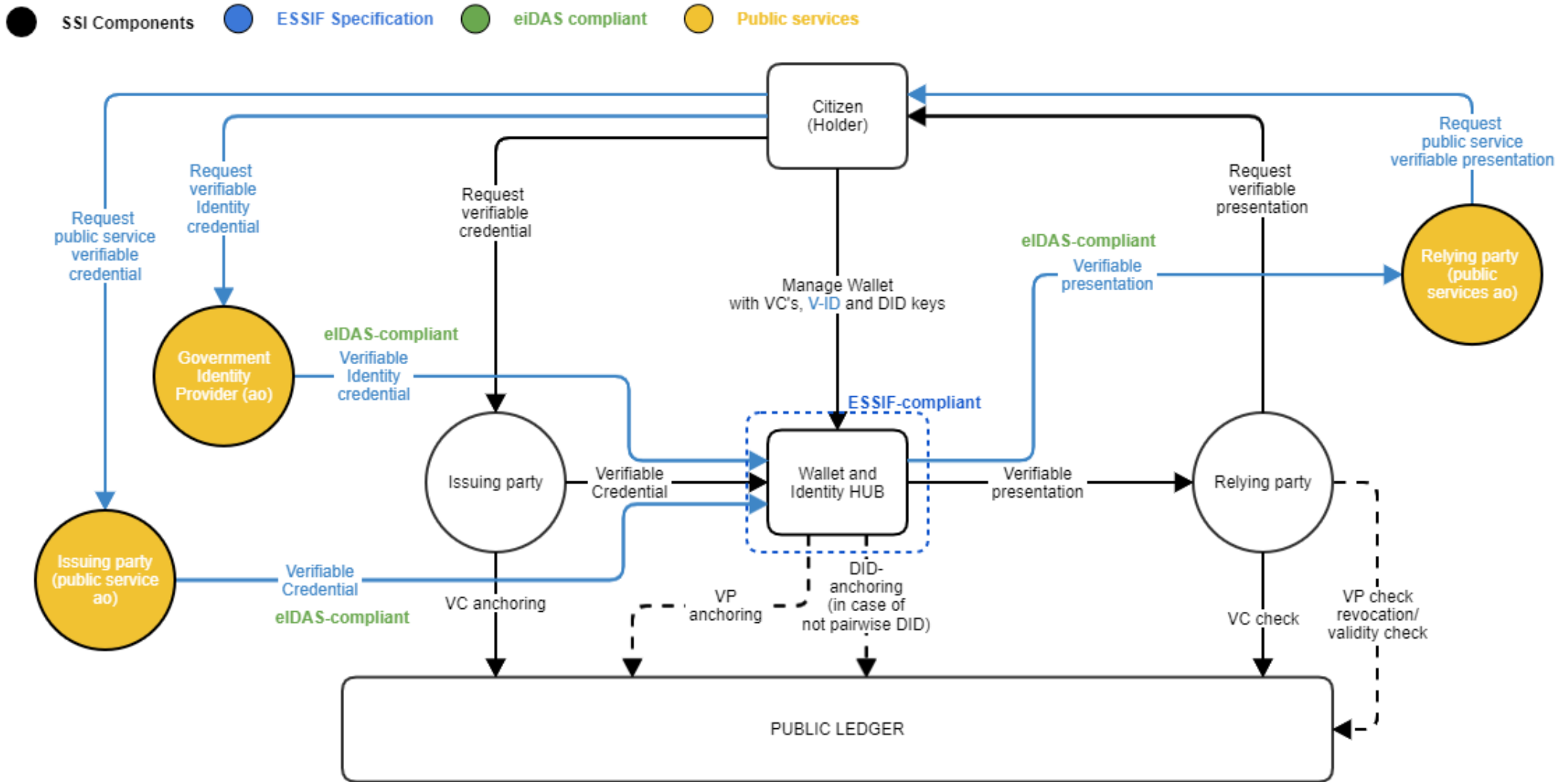
## Scope of ESSIF

- Empower citizen in the management of their data via SSI
- Stimulate the SSI-transformation of public services
- Facilitate cross-border interaction with SSI
- Make/keep national SSI projects interoperable
- Integrate/align existing building blocks such as eIDAS, e-delivery, once-only with SSI
- Conceptualize and build an identity layer in the new European Blockchain Services Infrastructure supporting the current use cases
- Preserve European/democratic values in the implementation of Self Sovereign identity
- Stimulate SSI development and standardization on global level (W3C, DIF, ISO, CEN-CENELEC, etc.)

# SSI ecosystem without ESSIF



# SSI ecosystem with ESSIF specification and public services involvement



# Our business case « Safe Chain for HAZMAT »

- Build from Eidas regulation Point of view a TRUST LEARNING NETWORK for Accredited learning Companies in dangerous goods Area in Europe
- Trust « Dangerous Goods Driver network » based on a Hardware wallet highly secure technology using INDY and ARIES Key management ( Working in progress with Rennes University Cryptography research Center ) in order to adress the different levels of sensitivity and to Comply GDPR
- Employee can allow Wallet Acces on the demand of any Einforcement Authorities (Anti terrorist check in France for Example)
- Avoid Multiple recheck when an Employee change of company
- Allow European interoperability Check (Eidas + EBSI Compliance)
- Build sector Accreditation based on ISO 17065:2012 (Compliance and Liability Criteria)



# Dangerous Goods Driver Wallet experiment

- Storage of DID
- Accredited training Proof ( unique Training Hash) allowing access to Accredited Trainer DLT check including validity date Check
- Instant scan of danger class that can be transported by the driver IN ERP /TMS interface
- Signing and Notarizing in Hyperledger Fabric all Docs related to Responsibility Tranfert at load and Unload
- Internal Threat Focus



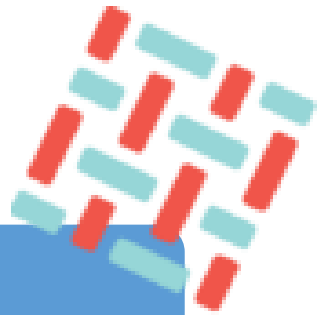
Mix of Crypto asset storage and Biometric USB+ Indy+Aries  
crypto Library= 2 factor auth = Trust Network for dangerous  
goods Driver = our Roadmap to open Hyperledger Fabric DLTS  
for Trust Providers in [EBSI Compliance](#)



+



# Technical Brief of our Proof of concept



**FABRIC**  
**HYPERLEDGER**



## Verifiers User Interface for Verifiable Credentials (VC)

- H accredited personnel managing Drivers's Training / Security Check
- Accredited Security Employee



## Verifiable Credential Management With Indy Sdk

- Creation by Truck driver
- Revocation
- Interoperability with other Wallets , Integration with BIOMETRICS(To be developped)



## Software development

- Libindy using Hyperledger SDK and ARIES Library Modules

# Roadmap to the Next Months

- Use cases :
  - ICAO IATA DGR Goods Declaration as a smart contract between Shipper, Freight Forwarder, Airline ( Hyperledger Fabric private DLT)
  - Customs Border : Private DLT dedicated to Customs Origin Rules ( Preferential vs non Preferential) in a trust chain of providers for complex integration supply chains
- Technology :
  - Hyperledger Cactus in EBSI node compliance objective



# Current members of consortium Safe Chain



**PELAGOS AVIATION**



- Roland FAURE
- CEO
- [www.aerosurete.com](http://www.aerosurete.com)
- +33 6 24 97 62 88