IAM in Hazardous Goods environnment
Eidas Regulation and SSSI brief

SSI Eidas Legal Report Executive summary

Source : https://joinup.ec.europa.eu/sites/default/files/document/2020-04/SSI_eIDAS_legal_report_final_0.pdf

www.aerosurete.com

Our Business 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 potentialy 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

What is our business risk Matrix position ?

		Impact of damages				
	Likelihood	Very High	High	Medium	Low	Negligible
Risk i	Almost certain	(1)	(1)	Level 4	Level 3	Level 3
	Likely	(1)	Level 4	Level 3	Level 3	Level 2
	Moderate	Level 4	Level 3	Level 3	Level 2	Level 2
	Unlikely	Level 3	Level 3	Level 2	Level 2	Level 1
	Rare	Level 3	Level 2	Level 2	Level 1	Level 1
(1): Not applicable to remote authentication over open networks.						

Figure 10. Risk matrix considered in IDABC

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

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”.

Article 13 (1) (a) of the Directive (EU) 2015/849

- customer due diligence measures shall comprise: [...] 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"19

Qualified Trust services : Prior Supervision and 2 year Conformity assessement

- Article 17 (3) (a) (4) (g) stipulates that the national body will carry out prior supervision and the award of the qualification, and that the service cannot be started until such qualification has been obtained (Article 21 (3)), and it has been publicly disseminated through the mechanism provided for in Article 22 of the eIDAS Regulation (the Trusted List). Although with a somewhat obscure terminology, this is an administrative authorisation, which must be granted under the relevant administrative procedure, within the national legislationnframework
- Conformity assessment every 2 years (Article 20 (1) of the Regulation)

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 !

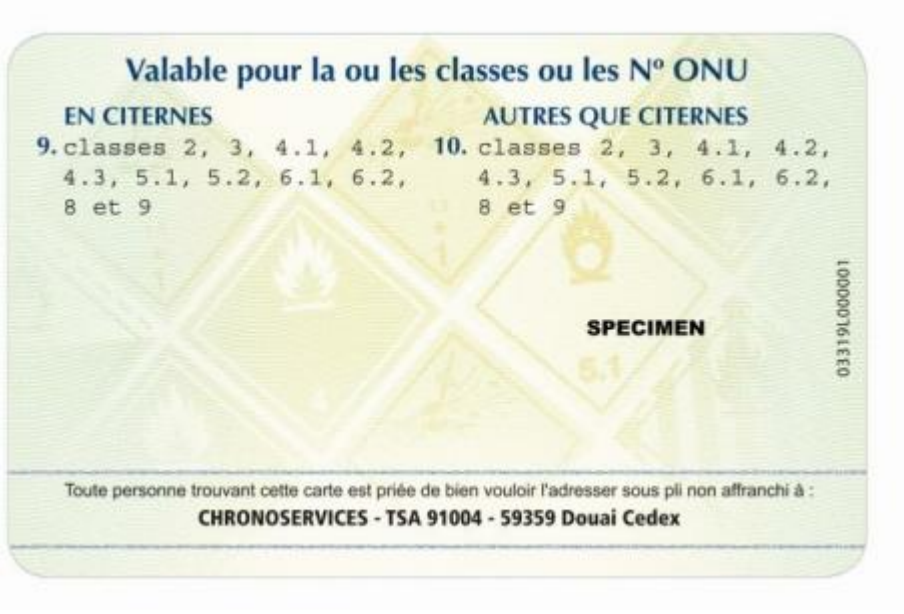
- Where procedures used previously by a public or private entity in the issuer's Member State for a purpose other than the issuance of electronic identification means provide for an equivalent assurance level, confirmed by a conformity assessment body, and steps are taken to demonstrate that the results 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

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 Criptography 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 Responsability Tranfert at load and Unload
- Internal Threat Focus



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

+

HYPERLEDGER INDY

HYPERLEDGER ARIES

Current members of consortium Safe Chain

PELAGOS AVIATION

- Roland FAURE
- CEO
- www.aerosurete.com
- +33 6 24 97 62 88