

# The use of Electronic Attestations of Attributes beyond the Wallet

Wim Coulier

eIDAS expert & contributor to ETSI ESI







# EAA as upcoming novelty

## eIDAS definition is **very open**:

- 'electronic attestation of attributes' means an attestation in electronic form that allows **attributes** to be **authenticated**;
- 'attribute' means **a characteristic, quality, right or permission** of a **natural** or **legal person** or of an **object**;
- 'authentication' means an electronic process that enables the confirmation of the electronic identification of a natural or legal person or the **confirmation of the origin and integrity of data** in electronic form

## **New technologies** are being adopted

- New features (e.g. selective disclosure)
- Software & services for issuance, validation, etc.

## **A new trust framework** is created

- Standards and audit framework
- Trust registers



# The valuable characteristics of EAA

- For natural persons, legal persons or objects!
- Verified information
- Self contained cryptographic verifiability
- Structured data => machine readable
- Selective disclosure possibility
- Decentralised portability
- Can be preserved for traceability and auditability

## EAA

Professional Qualities  
Issuer: Atatserp BV  
Subject: Wim Coulier  
Validity: From 02/11/2024 to 02/12/2024  
Value:

- Project Management:
  - PRINCE II certified
  - 06/06/2010
- ETSI ESI contributor
- eIDAS expert @ itsme
- Founder Trust Agency

## EAA presentation

Professional Qualities  
Issuer: Atatserp BV  
Subject: Wim Coulier  
Validity: From 02/11/2024 to 02/12/2024  
Value:

- eIDAS expert @ itsme





# Always in a EUDIW?

- EUDIW is a huge undertaking => At this moment the **focus is on the EUDIW**
- Danger that EAA technologies trust framework will work ONLY for the EUDIW. That could introduce **limitations** to EAA that makes them **unusable** for some **other use cases**.
- Those other use cases might require **other characteristics**, e.g. multiple subjects in one EAA, Hybrid EAA\*, absence of wallet binding, etc.



\*Hybrid EAA = combined human readable (e.g. PDF) and structured (e.g. W3C VC DM) in one file that can be both authenticated



# EAA with existing infrastructure



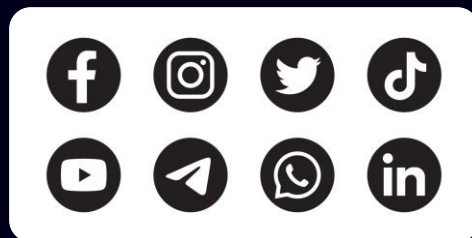
Identity providers

- SAML
- OIDC

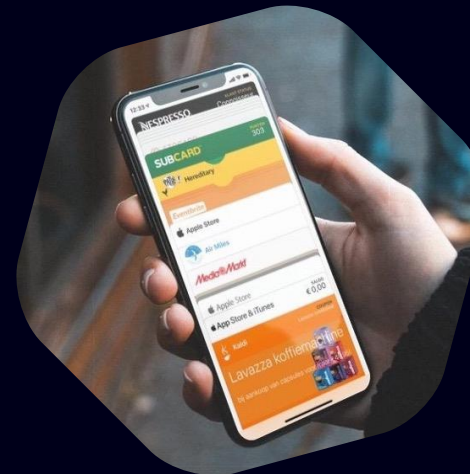


Vaults

- Solid Pods
- Proprietary



Simple Download and send



Private wallets



Interconnected business applications  
Data exchanges between different actors



Use cases beyond the Wallet



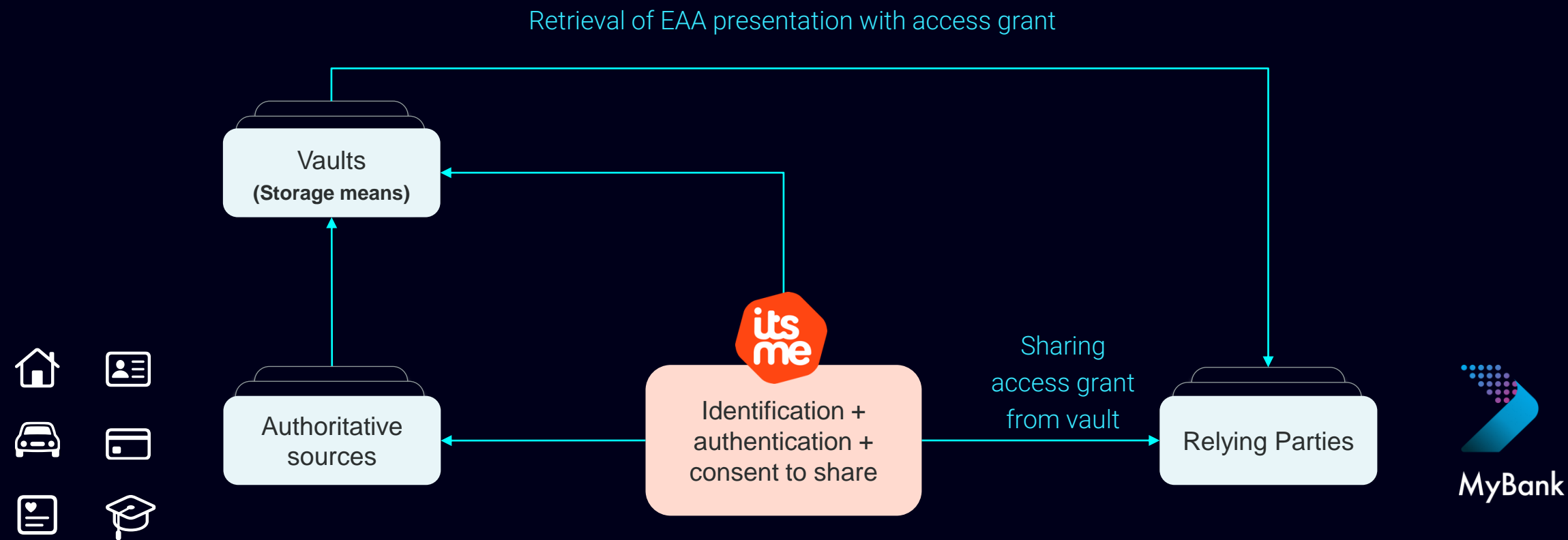




# Selective disclosure on salary slips

Use case

- Users already get salary slips in Vaults (e.g. Doccle) on monthly basis, makes no sense to put them in a EUDIW
- For allowing a mortgage, the bank needs proof of income
- Salary slip in Hybrid EAA format allow for selective disclosure, e.g. income above a certain amount



**itsme is the trust factor connecting the dots.**

Removing friction and building on familiar and solid grounds



# Digital Product Passport

Use case

Digital Product Passports (DPPs) are digital records containing information about a product's components, materials, chemical substances, and information related to repairability, spare parts, and proper disposal.

- Characteristics of Objects (attributes)
  - Need to be able to confirm integrity and origin of those characteristics (authentication)
- ⇒ They are attestations in electronic form that allows attributes to be authenticated, i.e. they fit the definition of an EAA
- ⇒ This means that **service Providers that will issue DPP are Trust Service Providers**
- ⇒ A DPP that is certified as QEAA will have a higher trust value

User will not want to overload their EUDIW with DPP of everything they use

The technology and trust framework that we are building for (Q)EAA can serve also the DPP. Let's **not reinvent the wheel** with new standards and trust frameworks, but be efficient and reuse the work on EAA for the DPP and adopt DPP solutions (e.g. Visible Digital Seal) for EAA.





Patients and nurse might not have a lot of tools to deal with EAA and will need a human readable file. Nurse will not put the attestations of her patients in her own EUDIW.

When sending the EAA to large organizations (e.g. hospitals, medical insurance,...) they will want to be able to treat it in automated fashion.

Hybrid attestations that can be stored in a vault of the patient or nurse could lead to faster adoption





# Car documents

Use case

A driver needs at all time to be able to show several document about the vehicle:

- Vehicle registration certificate
- Vehicle certificate of conformity
- Vehicle insurance
- Technical inspection certificate

These documents are linked to the car, not to the driver. They could be stored online, accessible via a QR code in the car that gives authentication to access the documents online.

- Not possible anymore to steal these document and use them with another car
- Not possible to create fake documents anymore
- No need anymore to move documents between multiple drivers that use the car (in families, car rentals, company pool cars, etc.)

**NOTE:** The Visible Digital Seal technology of the DPP could be reused here





4	Context
4.1	Source of attributes
4.2	EAA distribution
4.3	Multiple subjects
4.4	Wallet binding
4.5	EAA Policy and EAA Service Policy
4.6	Vaults

5	EAA trust service overview
5.1	Electronic Attestations of Attributes in eIDAS
5.2	EAA Service actors
5.2.1	EAA Service Provider
5.2.2	Subscriber
5.2.3	Attribute subject(s)
5.2.4	Authentic source
5.2.5	Authoritative source
5.2.6	Wallet holder
5.2.7	Vault Holder
5.2.8	EAA Recipient
5.2.9	Authorised Party
5.2.10	RP Intermediary
5.2.11	Relying party
5.3	EAA Service Provider components
5.4	EAA Policy
5.4.1	Context
5.4.2	EAA policy governance model
5.4.3	Establishing EAA Policies
5.5	Business processes
5.5.1	EAA registration
5.5.2	Identity proofing
5.5.3	Collection from or verification against Authoritative source
5.5.4	EAA Issuance
5.5.5	Wallet/key binding
5.5.6	Handover
5.5.7	Revocation request
5.5.8	EAA Status information

6	EAA trust ecosystem
6.1	General provision on policies and practices
6.2	EAA Policy trust
6.3	Registration of EAA request
6.4	Attributes aggregation
6.5	Identity proofing & authorization
6.6	EAA Issuance
6.7	EAA Dissemination
6.8	EAA Lifecycle management
6.9	Embedded disclosure policy

Annex A: Example use cases	40
A.1 Digital Product Passport (DPP)	40
A.1.1 Description of the use case	40
A.1.2 Trust Service Actors	40
A.1.3 Business processes	40
A.1.4 Technical implications	40
A.2 Mandate of natural person on European Business Wallet (EUBW)	40
A.2.1 Description of the use case	40
A.2.2 Trust Service Actors	40
A.2.3 Business processes	40
A.2.4 Technical implications	41

Annex B: Impact on standardisation	42
------------------------------------	----

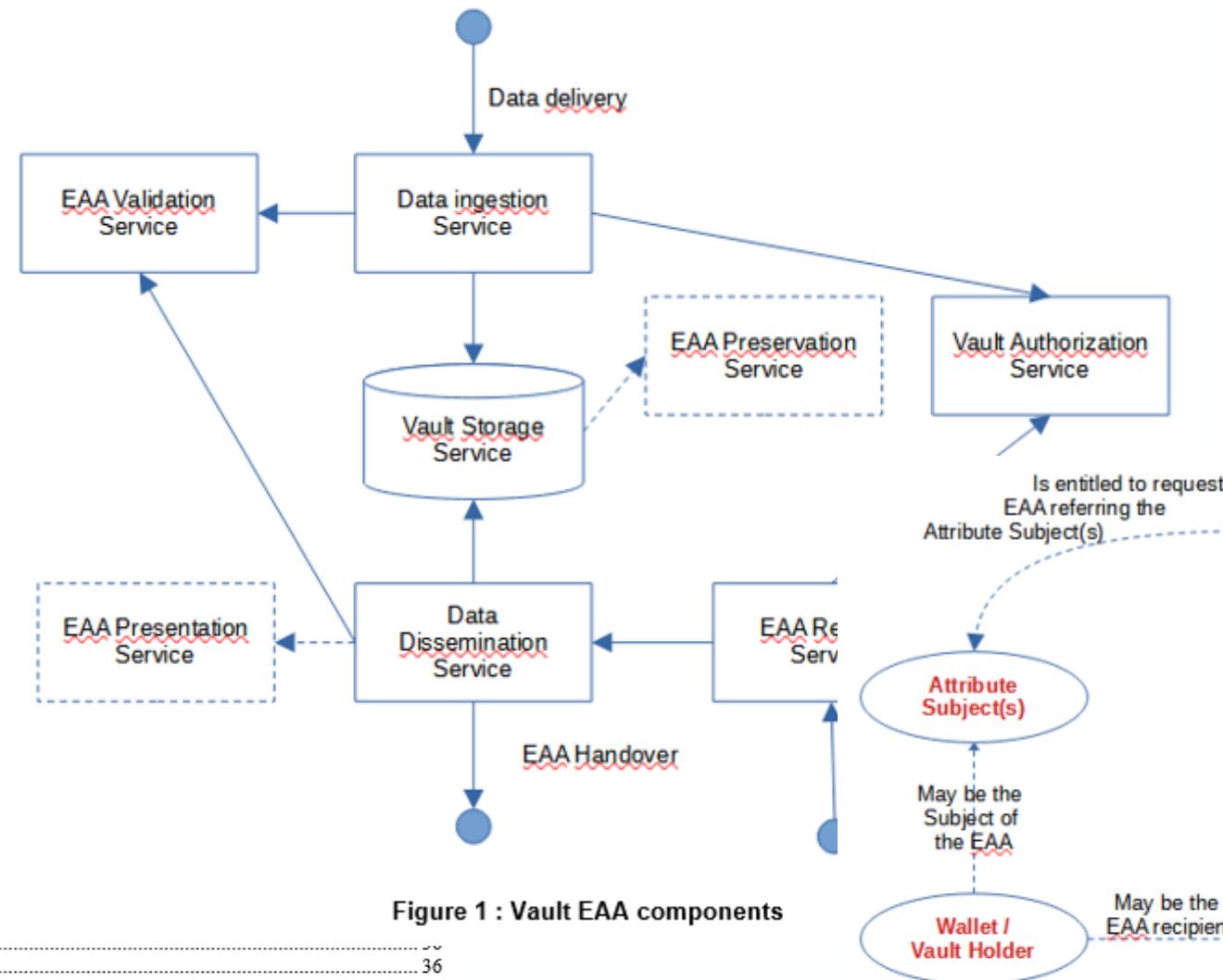


Figure 1 : Vault EAA components

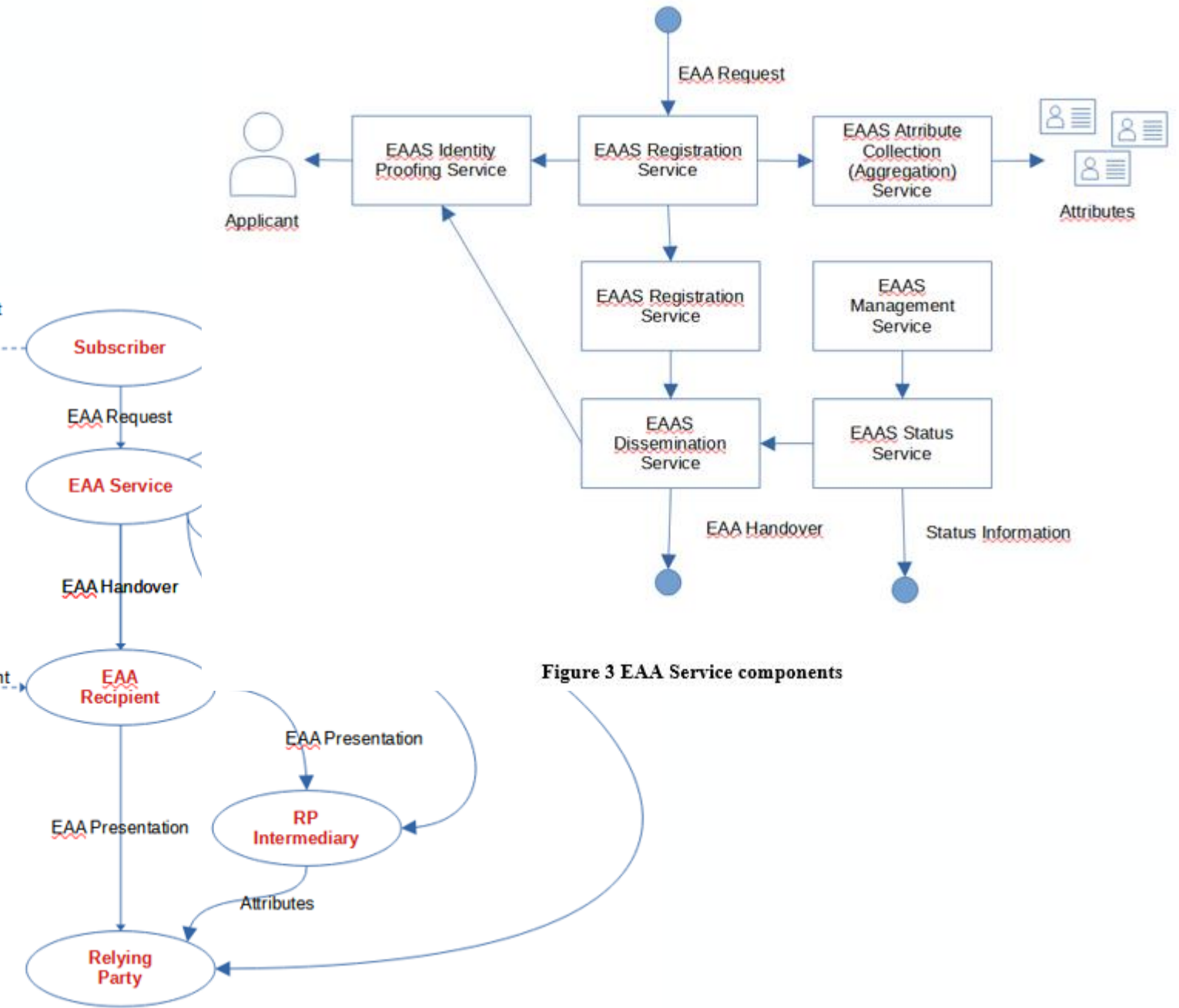


Figure 3 EAA Service components

Figure 2 : EAA Service actors





# Thanks

Wim Coulier

eIDA expert & contributor to Etsi ESI

[wim.coulier@itsme-id.com](mailto:wim.coulier@itsme-id.com)