Namirial

Electronic Attestation of Attributes Extended Validation Services

Luigi Castaldo
BU Wallet Ecosystem & Certified Communication Director

February 3, 2025 - TDI 2025 - Bologna

1

Agenda

- Regulatory context
- Scope
- Proposal
- Credential Refreshing
- VC Cyphered Presentation
- Central Rulebook for Attributes

Regulatory Context

A key aspect covered in the referenced standard drafts (TS 119 471 + TS 119 472-1) is:

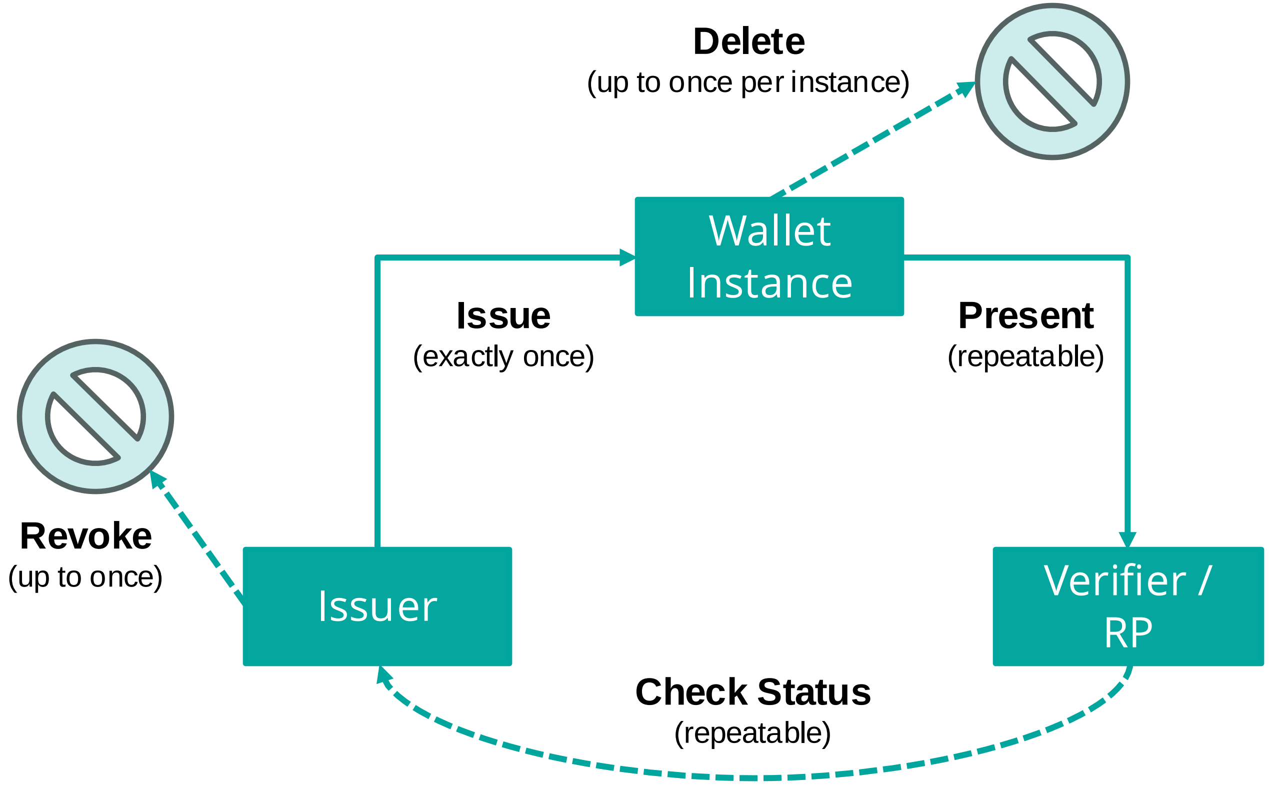
“issuance and validation of EAAs: protocols for the secure issuance and validation of electronic attestations, including the use of privacy-preserving techniques to protect user data”.

- **Unlinkability of transactions**: Issuers cannot know if or when their data is being used in a transaction with others. *(- **REQ-QEAASP-4. 3.-06**: The QEAASP shall have no information regarding the usage of the (Q)EAAs issued when a validity status check is performed.)*

- **User Privacy**: Preserving holders’ privacy limiting the verifier’s ability to access sensitive information. *(- **REQ-EAASP-7.13.-02**: The QEAASP shall enable privacy-preserving techniques. - **REQ-EAASP-4. 3.-05**: The revocation status information shall be publicly and internationally available.)*

Scope

Without an adequate mechanism of compensation for the services it is hard to foresee an optimistic future and wide distribution of the EUDIW Framework.



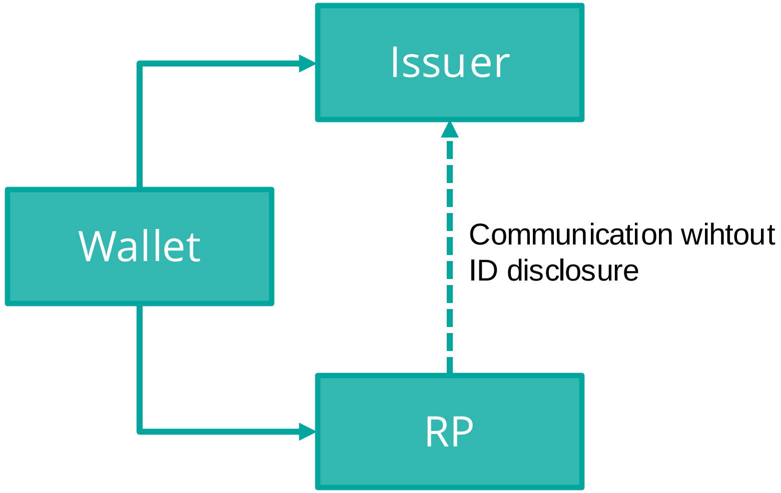
Does Not preserve privacy
Does Not guarantee unlinkability

Focus: Ensure direct communication between Relying Parties (RPs)/Verifiers and Issuers to independently manage payments for the verification transactions, still preserving unlinkability and users' privacy.

Why: We strongly believe that, for many use cases, relying parties (RPs) are the entities that benefit most from the digitized flow of attribute verification. Therefore, they should be willing to share some of these savings with the issuers who provide the attributes and enable their ongoing verification, creating new business model for (Q)EAA, contributing on the flywheel/network effect to incentives on creating (Q)EAA.

Extended Validation Service

The protocol splits the **Verifiable Credential Presentation** in two steps:



1. **Refreshing** the Verifiable Credential before every presentation.

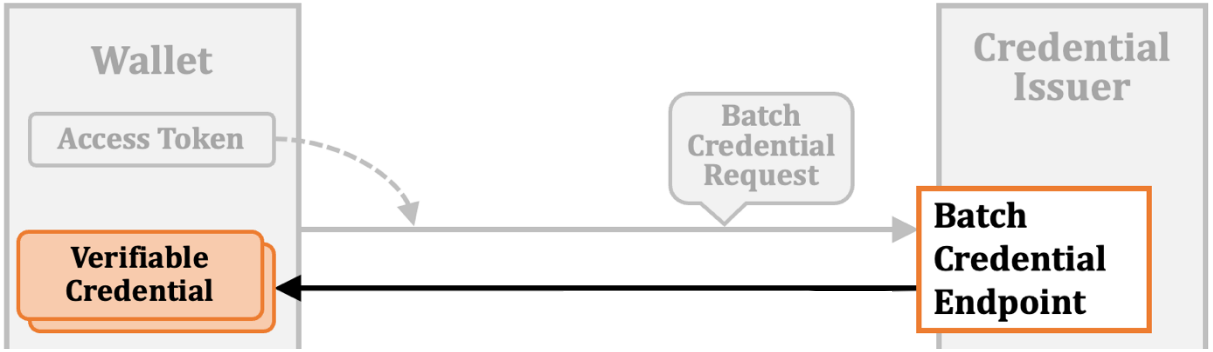
2. **Cyphered VC**: the VC are encrypted by the holder's wallet using a key shared between the **Issuer** and the **Wallet instance**, before sharing them with a **Verifier / RP**.

TR 119 479-2: EAA Extended Validation Services Framework and Application

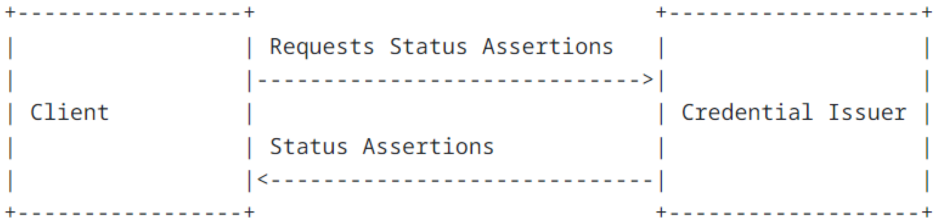
Credential Refreshing

The VC could be regenerated with a new start date [1] or use a linked credential, like the *Oauth Status Assertion* [2].

- **VC Re-Issuance**



- **Linked Credentials**



```
+-----------------+                              +------------------+
|                 | Requests Status Assertions   |                  |
|                 |----------------------------->|                  |
| Client          |                              | Credential Issuer|
|                 | Status Assertions            |                  |
|                 |<-----------------------------|                  |
+-----------------+                              +------------------+
```

Advantages

- There is no requirement for the RP/Verifier to carry out validation processes.
- Tailored policies can be established according to the degree of trust required by the RP (e.g., updates made within the last 8 hours).

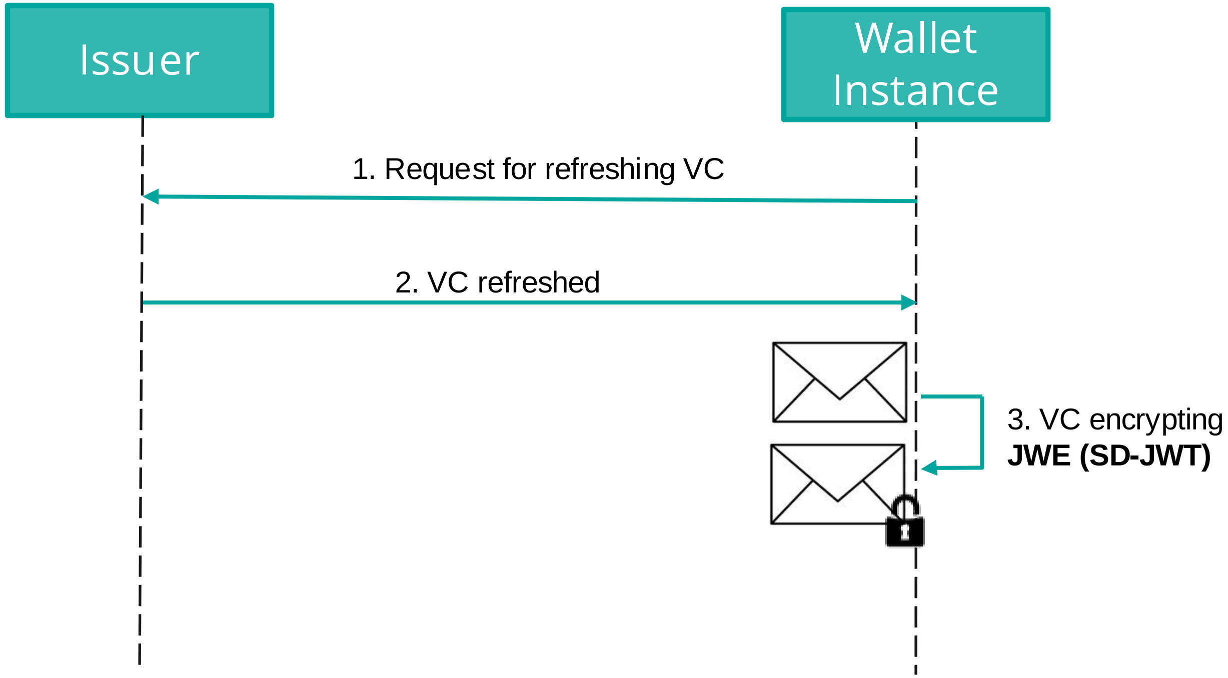
[1] https://openid.net/specs/openid-4-verifiable-credential-issuance-1_0.html

[2] https://datatracker.ietf.org/doc/draft-demarco-oauth-status-assertions/

VC Cyphered Presentation (1/2)

The protocol **doesn’t imply any change to the current Credential Issuance scheme**.

The **Issuer** creates and signs the Verifiable Credential (VC), embedding relevant identity or attribute information for the **Holder** (e.g., identity, access rights, etc.).



Hierarchical Deterministic (HD) Key Derivation

$$\boldsymbol{JWE} = P_k(d) * SD\text{-}JWT$$

- $P_k(d) = MP + T_{id}$
- $T_{id} = SHA_{256}(X) * G$

Where:

MP = Issuer’s public key

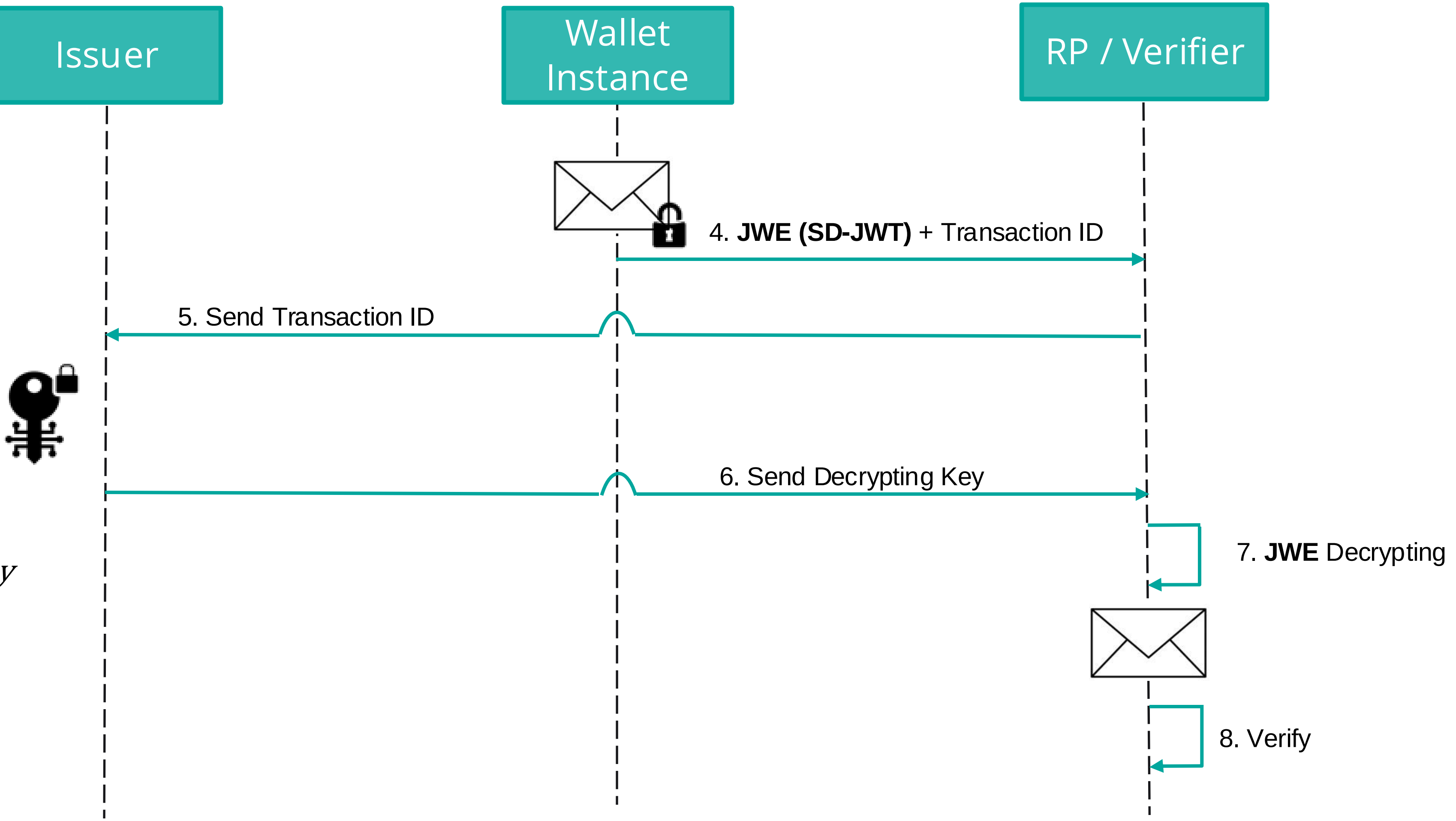
$P_k(d)$ = **derived** public key

X = combination “**nonce**” and a timestamp

G= base point of the elliptic curve

VC Cyphered Presentation (2/2)

The **Transaction ID** is distinct for every transaction and does not connect to the VC or Wallet Instance, nor is it associated with the process of issuance.



$$\boldsymbol{P_r(d)} = P + T_{id}$$

Where:

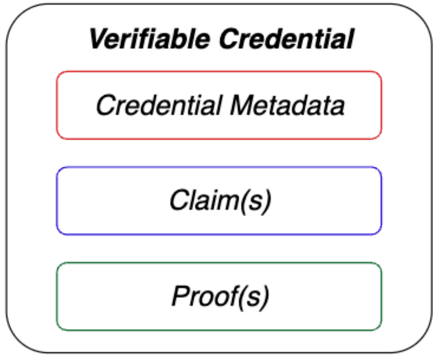
$P = \textit{Issuer private key}$

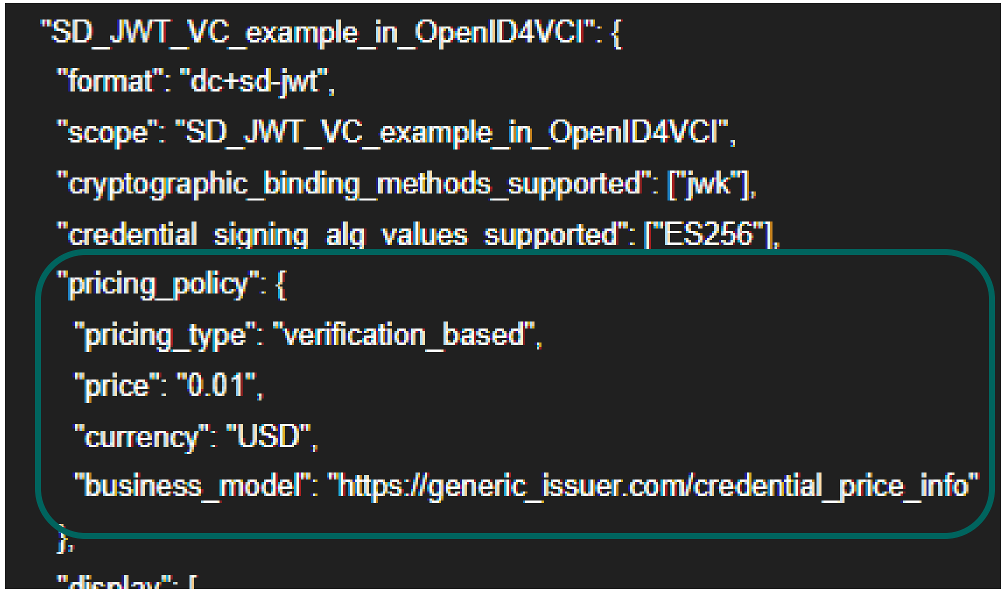
$P_r = \textbf{\textit{derived}}\ \textit{private key}$

Central Rulebook for Attributes - Art. 45e (section 2)

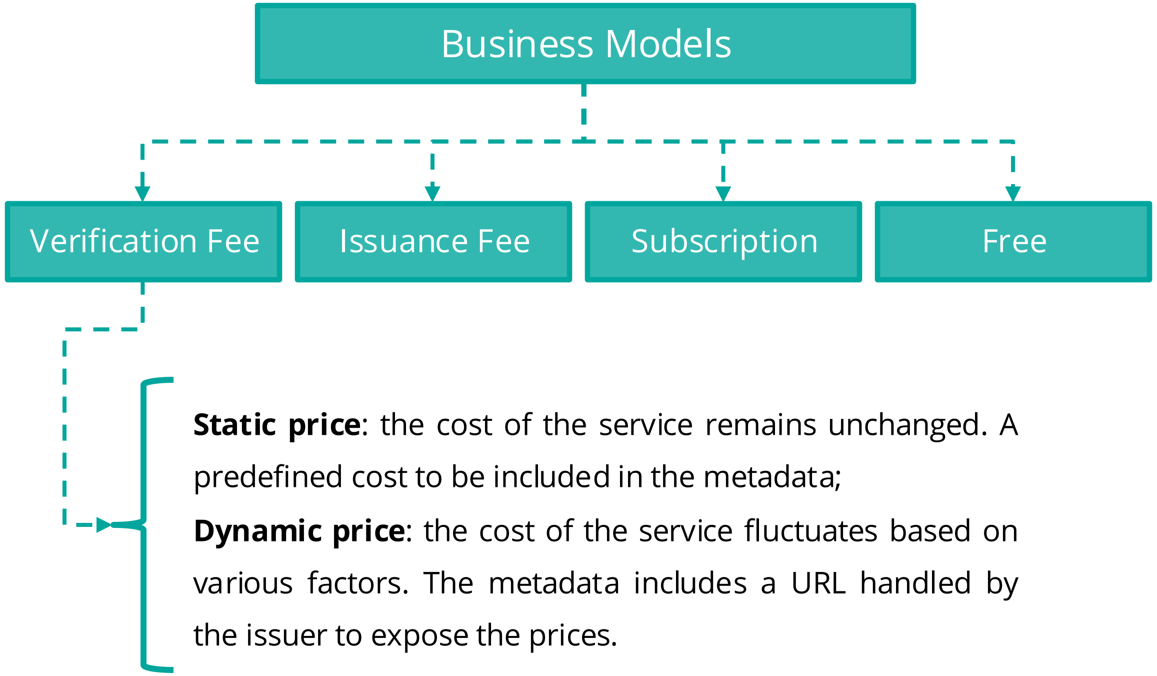
The registry would serve as a comprehensive repository of credential related information, including Credential Metadata:

- **Issuer Information**: Details about the issuer (e.g., name, public keys)
- **Business Model**: Pricing models and costs
- **Attributes** : Description of the attributes (e.g., "Qualification", “email”, …)





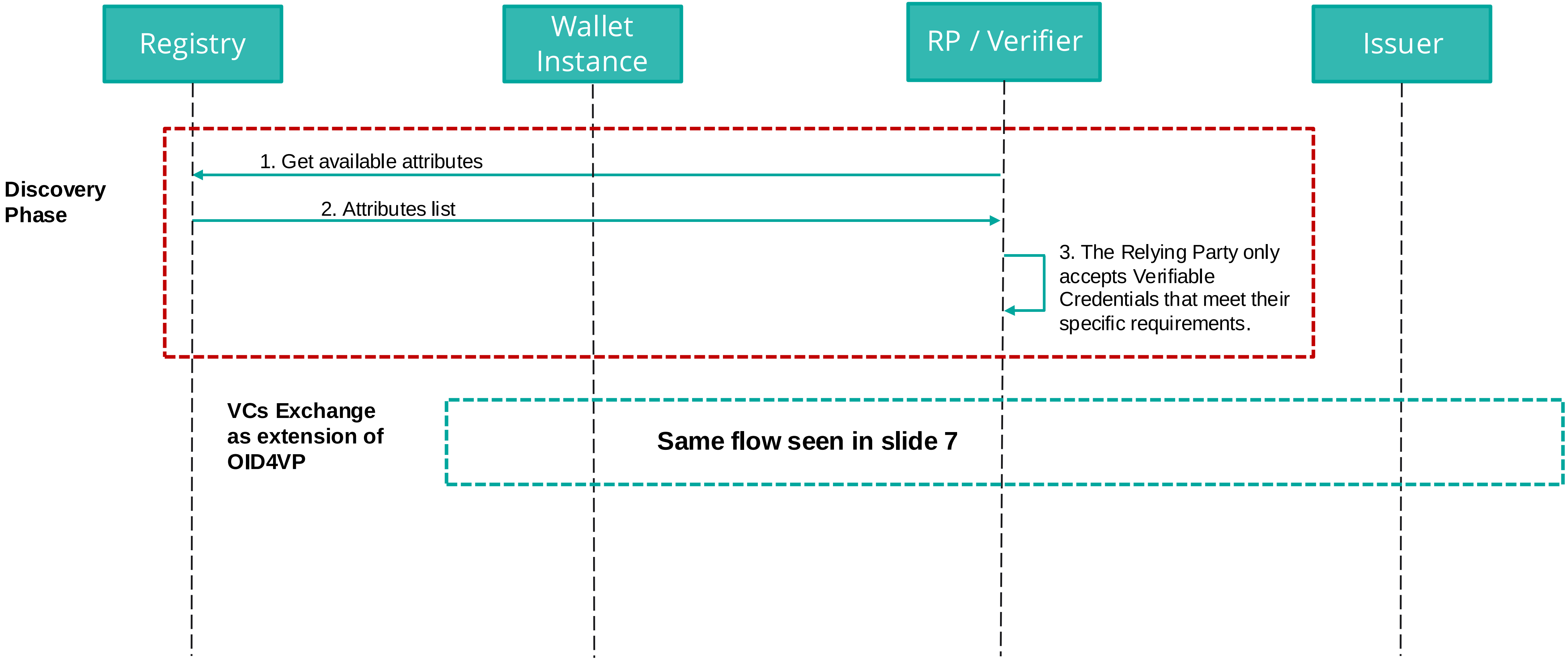
```
"SD_JWT_VC_example_in_OpenID4VCI": {
 "format": "dc+sd-jwt",
 "scope": "SD_JWT_VC_example_in_OpenID4VCI",
 "cryptographic_binding_methods_supported": ["jwk"],
 "credential_signing_alg_values_supported": ["ES256"],
 "pricing_policy": {
  "pricing_type": "verification_based",
  "price": "0.01",
  "currency": "USD",
  "business_model": "https://generic_issuer.com/credential_price_info"
 },
 "display": [
```



Static price: the cost of the service remains unchanged. A predefined cost to be included in the metadata;

Dynamic price: the cost of the service fluctuates based on various factors. The metadata includes a URL handled by the issuer to expose the prices.

Extending OID4VP to support the interaction


Registry
Wallet Instance
RP / Verifier
Issuer
Discovery Phase
1. Get available attributes
2. Attributes list
3. The Relying Party only accepts Verifiable Credentials that meet their specific requirements.
VCs Exchange as extension of OID4VP
Same flow seen in slide 7

Get in contact!

Luigi Castaldo
BU Wallet Ecosystem & Certified
Communication Director

l.castaldo@namirial.com