Federation of Attribute Providers for User Self-Sovereign Identity

Pedro Coelho[1], André Zúquete[2], Hélder Gomes[3]

1 — IEETA, University of Aveiro
2 — Department of Electronics, Telecommunication and Informatics & IEETA, University of Aveiro
3 — ESTGA – Águeda School of Technology and Management & IEETA, University of Aveiro

Today, people expect that companies and public institutions will provide many of their services through the Internet. However, this calls for a general-purpose, attribute attestation system, capable of allowing people to collect and remotely provide their digitally certified attributes to service providers on a needed basis.

These attributes belong to the set that represents a person's identity. They can be perpetual, ephemeral or can vary over time. An attribute is some piece of data about a person that often can be attested by some trusted party. Such attestation is essential to allow a person to claim their ownership when interacting with service providers. The concept of self-sovereign identity rose from a citizen-centric identity turned into an interoperable, federated identity. A citizen-centric identity means that citizens must be central to the administration of their identity. This requires not only interoperability of such identity across multiple locations but also true control of identity. This control refers to how, when, for how long and to whom users citizens disclose portions of their identity, i.e. attributes.

We designed a system that provides trusted, personal attributes to service providers and facilitates the organization and distribution of those attributes by their owners, while adhering to the principles of self-sovereign identity [1].

The system recognizes four groups of entities (or roles): Users, Attribute Providers (APs), Regulation Bodies (RBs) and Service Providers (SPs). RBs are responsible to manage and supervise the set of APs that may participate in the system. APs certify and publish Users' attributes upon their request, and may latter revoke them. Users provide trustworthy, certified attributes of their own to SPs on a need-to-know basis. All certificate requests and certified attributes are privately and centrally stored in a permissioned blockchain, maintained by RBs and APs. Privacy is ensured by pseudonyms managed by Users.

For ensuring privacy, each certified attribute is bound to a pseudonym. The set of pseudonyms of each User is managed through their wallet. For confidentiality, certified attributes can be obfuscated.

A User wallet is a fundamental piece for managing the issuing and the exploitation of the user certified attributes. A wallet keeps the references to all the certified attributes belonging to its owner and the elements for revealing obfuscated attributes.

[1] P. Coelho, A. Zúquete, H. Gomes, "Federation of Attribute Providers for User Self-Sovereign Identity", J. of Information Systems Engineering & Management, 3(4), Nov 2018