Unlinkability in distributed identity management

Davide Frey (WIDE, davide.frey@inria.fr),
Guillaume Piolle (CIDRE, guillaume.piolle@centralesupelec.fr)

January 9, 2020

Identity management, as a traditional pre-requisite to authentication and authorization, is a core feature in the domain of information security. As systems, assets and applications have evolved to a greater decentralization (at least in their means of access), the models for identity management have developped accordingly. From a completely centralized starting point, the notion of federated identities have emerged and taken precedence, in particular for web-based environments. Even decentralized models have then arised, allowing users to choose between various identity providers or to set up their own.

The current trend of Self-Sovereign Identity [2, 4] marks an orientation towards truly distributed architectures, from which a maximum of single points of failure or trusted entities have been removed. Available frameworks include Namecoin, Emercoin, Ethereum Nameservice, uPort, Blockstack or the overlying W4C Decentralized Identifiers.

However, this evolution is not complete and current identity management systems still rely, for some features (like name and identifier attribution, or sources of authority for attestation and certification), on partially or completely centralized references. Technologies such as distributed hash tables (DHT) or blockchain-based distributed ledgers have allowed for a completely decentralized storage, access and publication of identities, claims, commitment information and the like, but the need for a common source of authority or unicity remains, to some extent at least. Attestation and certification of users' claims on their identities and attributes, in particular, seems hard to design in a completely peer-to-peer fashion. A novel issue in this domain is the pertinence of a local or contextual consensus on the notion of identity and identity verification, as opposed to the "universal truth" borne by a blockchain ledger or a centralized certification authority.

Furthermore, current frameworks do not integrate any kind of unlinkability, a privacy-related evaluation criterion allowing a user to perform two actions in a system without an observer being able to link them to a same actor. Unlinkability is actually a family of properties already studied in the context of centralized authentication and authorization, for instance in the U-Prove [3] and Idemix [1] frameworks. There is a need to examine, in the context of decentralized and distributed identity management, the viability and limitations of unlinkability guarantees: unlinkability between identity attestation and identity verification (issue-show unlinkability), between two identity verifications (multi-show unlinkability), between several personae of a same user or between several verifications of the same persona, unlinkability towards verifiers or towards issuers...

The first objective of this intership is to study the possibilities and variants of a fully distributed identity management framework, without any point of centralization, which may or may not make use of blockchain and distributed ledger technologies.

The second objective is to analyze the ability of candidate models to provide unlinkability properties to user, and to finely characterize those properties, their conditions and limitations.

This intership will take place in the context of a collaboration between the CIDRE and WIDE Inria/IRISA research groups, and the intern will be primarily attached to either one of them.

References

[1] IBM RESEARCH. Specification of the identity mixer cryptographic library, version 2.3.0, 2010. https://domino.research.ibm.com/library/cyberdig.nsf/papers/EEB54FF3B91C1D648525759B004FBBB1/$File/rz3730_revised.pdf.

[2] MÜHLE, A., GRÜNER, A., GAYVORONSKAYA, T., AND MEINEL, C. A survey on essential components of a self-sovereign identity. *CoRR abs/1807.06346* (2018). https://arxiv.org/pdf/1807.06346.pdf.

[3] PAQUIN, C. U-prove technology overview v1.1, 2013. Microsoft Corporation, https://www.microsoft.com/en-us/research/wp-content/uploads/2016/02/U-Prove20Technology20Overview20V1.120Revision202.pdf.

[4] THE SOVRIN FOUNDATION. Sovrin: A protocol and token for self-sovereign identity and decentralized trust. white paper, January 2018. https://sovrin.org/wp-content/uploads/2018/03/Sovrin-Protocol-and-Token-White-Paper.pdf.