Decentralized Semantic Identity

José G. Faísca
Copelabs – ECATI
Universidade Lusófona
jose.faisca@ulusofona.pt

José Q. Rogado
Copelabs – ECATI
Universidade Lusófona
jose.rogado@ulusofona.pt

ABSTRACT

This paper examines a semantic approach for identity management, namely the W3C WebID, as a representation of personal information, and the WebID-TLS as a decentralized authentication protocol, allowing individuals to manage their own identities and data privacy. The paper identifies a set of important usability, privacy and security issues that needs to be addressed, and proposes an end to end authentication mechanism based on WebID, JSON Web Tokens (JWT) and the blockchain. The WebID includes a personal profile with its certificate, and the social relationship information described as the RDF-based FOAF ontology. The JWT is a standardized container format to encode personal related information in a secure way using "claims". The distributed, irreversible, undeletable, and immutable nature of the blockchain has appropriate attributes for distributed credential storage and decentralized identity management.

The full paper is included in the ACM Proceedings of the 12th International Conference on Semantic Systems, SEMANTICS 2016, ISBN 978-1-4503-4752-5.

DOI http://dx.doi.org/10.1145/2993318.2993348

SEMANTICS 2016: Posters and Demos Track
September 13-14, 2016, Leipzig, Germany