IAMX Allegra Whitepaper

Tim Brückmann, Jochen Leinberger, Tim Heidfeld, Dennis Mittmann

Date: 18.09.2021

Type: Simplified Version

IAMX AG
Dammstrasse 16
6300 Zug
Switzerland

***Abstract*— This document describes the implementation of an Identity and Authentication System based on Decentralized Identifiers, verifiable Credentials in a GDPR/DSGVO conform way.**

Keywords: Decentralized Identifiers, verifiable Credentials, Self Sovereign Identity.

I. MODEL FOR CONVERSION

A. From attributes to true-false credentials, or hash encrypted credentials.
B. Embedded scheme,
C. Unchangeable meta-info
D. Certificate of issuer and certificate of authentication agent
E. Unique identifier for the source, so credentials are holder connected.

Info: Credential onboarding by automate is only possible, when credentials, derived from attributes in combination with biometrics are fully matching with biometric Data.
Explanation: This means that Vitalik can not take over those Credentials from Charles, if he would be in possession of his physical plastic ID.

II. SIMPLIFIED EXPLANATION

1) Selective disclosure exact age

a) Attribute, e.g. birth date 02.08.1993
b) Apply any scheme, e.g. “Over 18?. Possible answers: true-false.”
c) Meta
d) - certificate of issuer: e.g. state USA
e) - source-document: ID
f) - DID of source-document: did:iamx:xxxxyyyyzzz1

g) - certificate authentication agent: e.g. state-level-accepted Global Entry / EasyPASS
h) - scheme: Over 18?. Possible answers: true-false.
i) DID did:iamx:xxxxyyyyzzz1

2) **Selective disclosure exact birthdate**
   a) Attribute, e.g. birthdate 02.08.1993
   b) Apply any scheme, e.g. “Is birthdate hash correct?. Possible answers: true-false.”
      i) verifier/seller can check with public key
   c) Meta
      i) certificate of issuer: e.g. state USA
      ii) source-document: ID
      iii) DID of source-document: did:iamx:xxxxyyyyzzz2
      iv) certificate authentication agent: e.g. state-level-accepted Global Entry / EasyPASS
      v) scheme: Over 18?. Possible answers: true-false.
   d) DID did:iamx:xxxxyyyyzzz2

III. Will this work? Let's do the check. Example:

1. ***Telco-Carrier offers “Unlimited Data and Talk” for 80 USD per month.***
2. Telco-Carrier may contract under condition that applicant has legal age
3. Legal Age concerning this mobile plan means 18 years old
4. Holder Charles discloses credentials over 18 = true
5. Telco-Carrier needs to evaluate if they can contract if legal age is
   a. proven by issuer: state,
   b. certified by authorization agent state approved level

References

[1] Alex Preukschat and Drummond Reed, *Self-Souvereign Identity Decentralized digital identity and verifiable credentials, Manning Publications Co., NY 11964, 2021.*