“Q10/17 Work on DLT Authentication”

Abbie Barbir, PhD

Co-Rapporteur Q10/17, ITU-T SG 17

Agenda

- Q10/17 work on DLT authentication
  - ITU-T NWIP X.Tec-idms
  - ITU-T X.1403 Overview
  - ITU-T X.1252Rev
  - ITU-T X.1254Rev
- FIGI Authentication WG
- OASIS Electronic Secure Authentication (ESAT) TC
- Q&A

Identity management and telebiometrics architecture and mechanisms

Motivation

- While Biometrics is gaining acceptance in identity verification and authentication
- Biometric application systems present various challenges related to operational and technical data protection, reliability, and security of biometric data for biosafety and biosecurity applications
- IdM is a critical component in managing network security because it improves assurance for the nomadic, on-demand access to networks and services that end-users expect. Focus on
  - Strong authentication
  - DLT authentication and DIdM
  - Authentication Assurance
  - Passwordless Authentication

Draft Recommendation ITU-T X.Tec-idms

Scope

- This Recommendation develops techniques for the protection of identifiers as related to user data in distributed identity systems. This document focuses on the following:
  - analysis identification of a few relevant currently deployed solutions, supported use cases and risks and possible response methods related to exposing identity and user data,
  - methods and techniques for identifier un-linkability and de-anonymization inference attacks,
  - guidelines and best practices to mitigate the identified risks.

Recommendation ITU-T X.1403

Scope

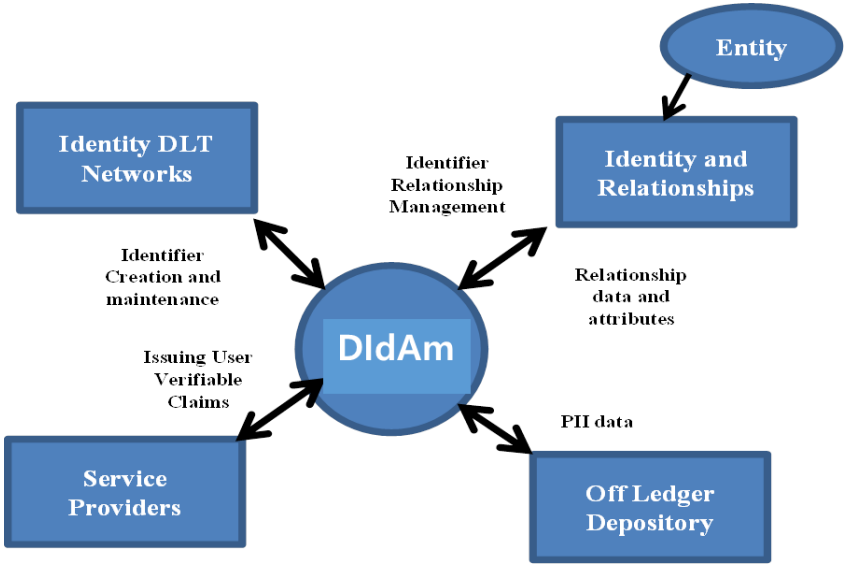
- This Recommendation provides an overview of using DLT for decentralized identity management. The scope of the work includes:
  - a brief overview of using distributed ledgers for the management of identity and identity data, and
  - Discussion on security benefits of decentralized identity, and
  - guidance concerning necessary controls that should be used to mitigate threats to identity data

- DLT provides an opportunity for development of decentralized identity management (DIdAm) solutions
  - means for managing of trust without a centralized authority thus avoiding any single point of failure
    - Centralized identity model
    - Federated identity model
    - Decentralized Identity model

DIdAm framework

Components of a DIdAm are:

- Decentralized identity owner
- Service providers (SP)
- Off ledger identity depository
- Identity systems that are based on DLT can be thought of as separate identity systems with different trust boundaries and cryptography keys.
- Therefore, the DIdAm must facilitate interactions across ledgers on behalf of the user



Threats and vulnerabilities

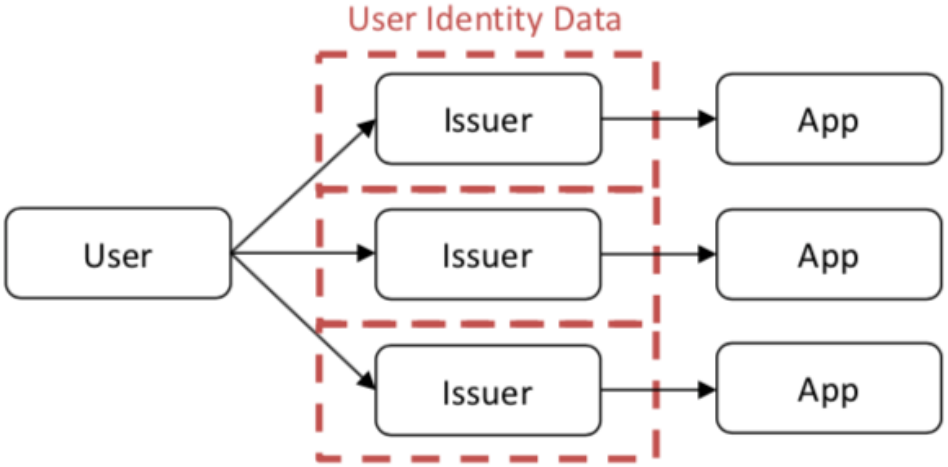
- Identity data management
  - CRUD
- DID key linkability
- DID key protection
- PII preserving techniques
- Vendor lock-in
- Identity-based attacks
- Communication network effects
- Identity data encryption
- Backup
- Smart contracts
- DLT certificate management

DID and VC Emergence

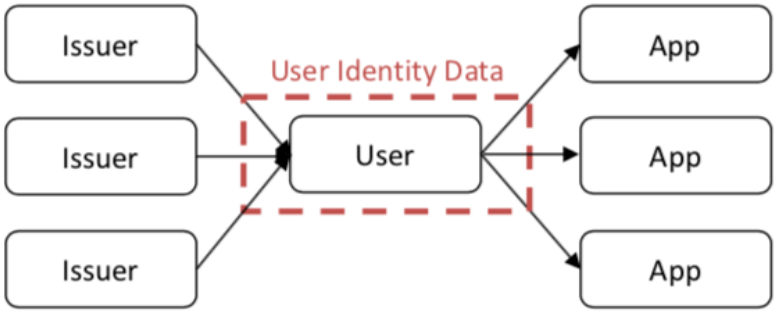
- Rapid development in the standardization of universal identifiers such as W3C DID [https://www.w3.org/TR/did-core/].
- A standard data model and representation format for cryptographically verifiable digital credentials as defined by the W3C DID specification [https://www.w3.org/TR/vc-data-model/].
- **The resolution of W3C DID can be done in a manner that is analogues to the resolution of a URL**
  - **DID resolution does not require the use of a distributed ledger technology (DLT).**
  - Resolution of a DID can be used in hybrid systems that include central and distributed non-DLT and DLT data systems.

PEER DID Status

- NIST Report "A Taxonomic Approach to Understanding Emerging Blockchain Identity Management Systems (https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.01142020.pdf)"
- ISO 2nd WD TR 23249 Blockchain and distributed ledger technologies — Overview of existing DLT systems for identity management "

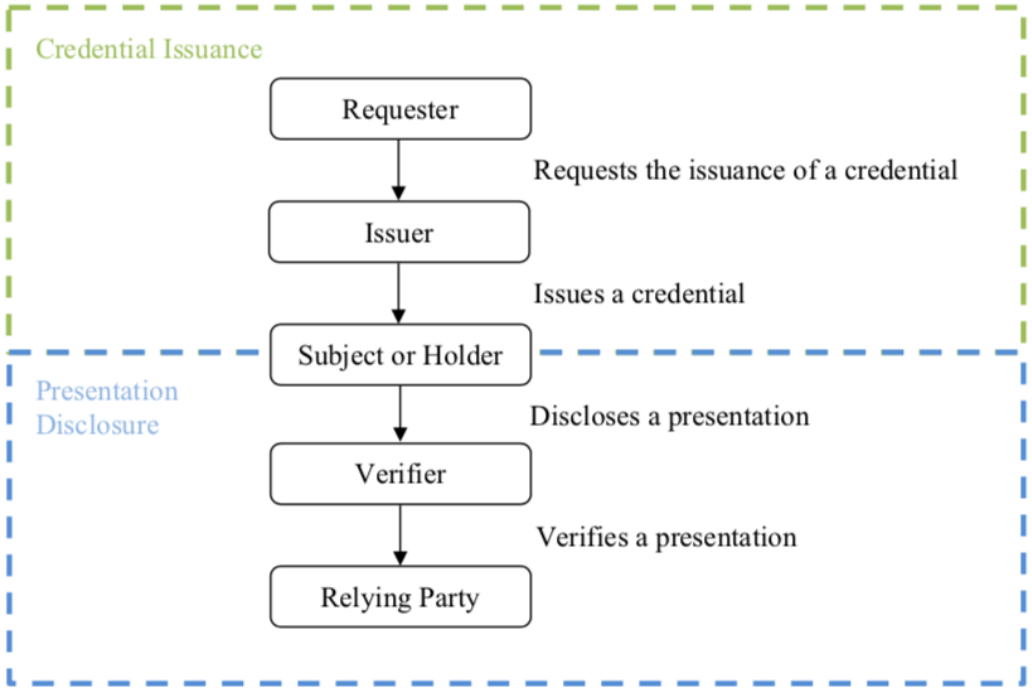


Traditional Identity Management

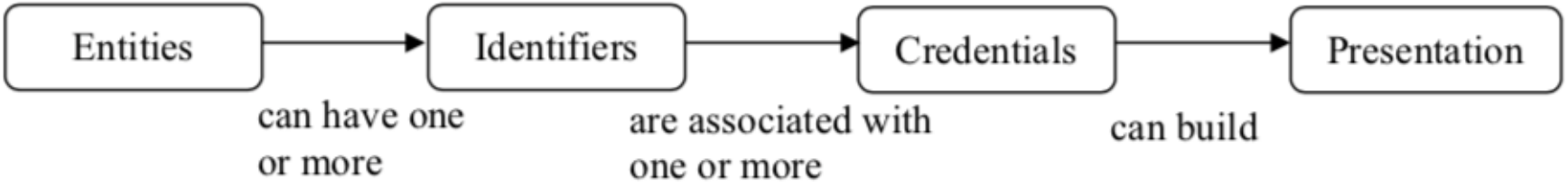


User-Centric Identity Management

Identity Management Roles



- Roles are not exclusive
- a *subject* and an *issuer* can both take the *requester* role;
- a *subject* and a *verifier* can both be a *relying party*
- Depending on the IDMS, the approval of a *subject* may be required to issue a new credential to that *subject*.

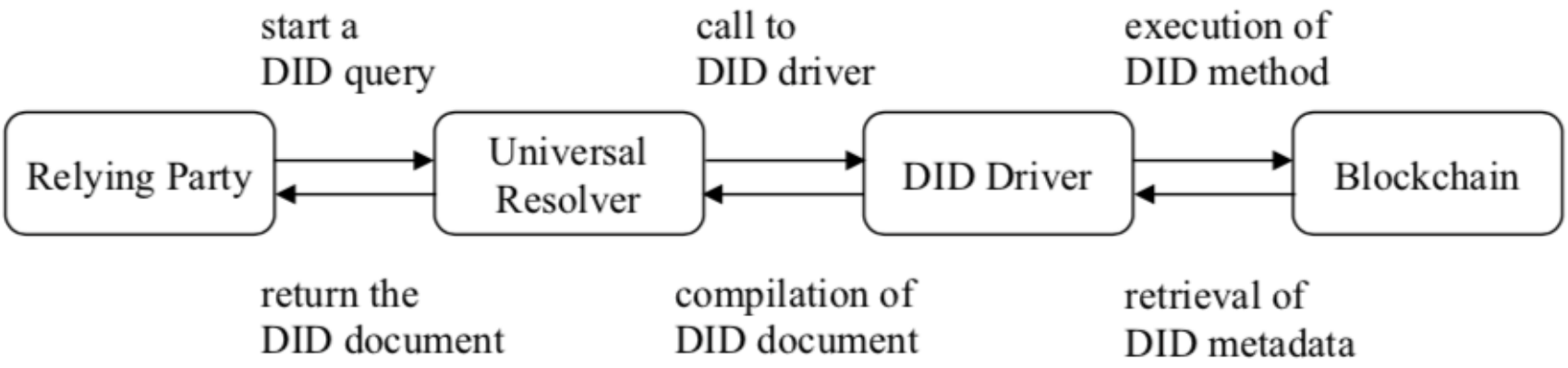


Hierarchy of IDMS Objects

Daniel Hardman (Evernym) has been leading the work on it and presenting it at SSI Meetup meetings.

PEER DID

A DID has the following format:
“did:” + <did-method> + “:” + <method-specific-identifier>



Daniel Hardman (Evernym) has been leading the work on it and presenting it at SSI Meetup meetings.

Additional Recommendations

ITU-T X.1252Rev: **Baseline identity management terms and definitions**

- Added definitions of decentralized identity
- Updated Identity Model to include Decentralized models

ITU-T X.1254Rev: **Entity authentication assurance framework**

- Improvement on Authentication Assurance Framework
- Incorporated FIDO authentication
- True password-less Support

FIGI Security, Infrastructure and Trust Working Group (SIT WG)

- Report on Strong Authentication
- Report of eKYC
- ITU-T End point for FIDO Authentication

OASIS Electronic Secure Authentication (ESAT) TC (see https://www.oasis-open.org/committees/tc_home.php?wg_abbrev=esat)

- **QR Code security**

Q&A