Insights on Digital Financial Services (DFS) During COVID-19 Webinar Series

FIGI FINANCIAL INCLUSION GLOBAL INITIATIVE

Episode #3
Benefits of Digital ID to enable governments and private sector response to the pandemic – Part 2

COVID-19 Impact on e-KYC

Abbie Barbir, PhD, CISSP
FIGI SIT WG – Authentication Workstream Chair

Security, Infrastructure, Trust WG

- Security, Infrastructure, Trust Working Group
  - To enhance confidence in using Digital Financial Services (DFS)
  - To address DFS security issues and mass digital fraud in developing countries
  - To assess new technology impact on security & consumer protection
- Authentication Workstream
  - To provide use cases, requirements, definitions and examples of strong authentication solutions
  - To offer guidance for regulators, authentication providers and Digital Financial Services (DFS) providers

Authentication WG Scope and Focus

- Strong interoperable authentication to support DFS
- Use cases (Web/Mobile)
- Means of evaluating authentication assurance (ITU-T X.1254)
- Digital Lab setup
  - APIs for authentication (FIDO Standards (ITU-T X.1277 / ITU-T X.1278))
    - End point validation, subscription and registration
      - Device Registration enabling service provider to register an Authenticator with user account and policy.
      - Device authentication.
      - Deregistration: Relying party can trigger the deletion of the account-related authentication key material

WG Output

- Contributions from working group members
- From industry consortia and standards development bodies
- Report Implementation of Secure Authentication Technologies for DFS
  - (see https://www.itu.int/en/ITU-T/extcoop/figisymposium/Documents/ITU_SIT_WG_Implementation%20of%20Secure%20Authentication%20Technologies%20for%20DFS.pdf)
- Contributed to FATF Digital Identity Report
  - (see https://www.fatf-gafi.org/media/fatf/documents/recommendations/pdfs/Guidance-on-Digital-Identity.pdf)
- Produced a report on e-KYC uses cases

Authentication Systems

- Used in two ways:
  - Establish that the person is who they claim to be when enrolling for an account
  - Verify that a returning customer is the same one that previously opened an account
- For Account Creation
  - Ask for and verify identification information
    - For DFS – ‘Know Your Customer’ (KYC) procedures
    - Obtain from previously-established accounts based on regulatory obligations

On-Line Identity Vetting

Pain points

- E-KYC is hard to do online
  - Harder with no Universal Global ID
- COVID-19 proved that a flexible approach is needed to bootstrap digital identity online
  - Need a trusted digital identity echo system for every citizen

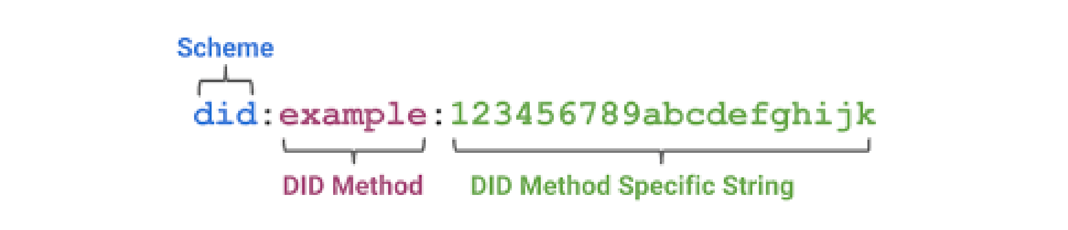
Technical Specifications

Core Standard work is already available to enable digital identity

- FIDO Alliance specifications
  - ITU-T Recommendations x.1277, x.1278
- ITU-T Distributed ledger recommendations
- OpenID Connect + Mobile Connect

W3C Decentralized Identifiers

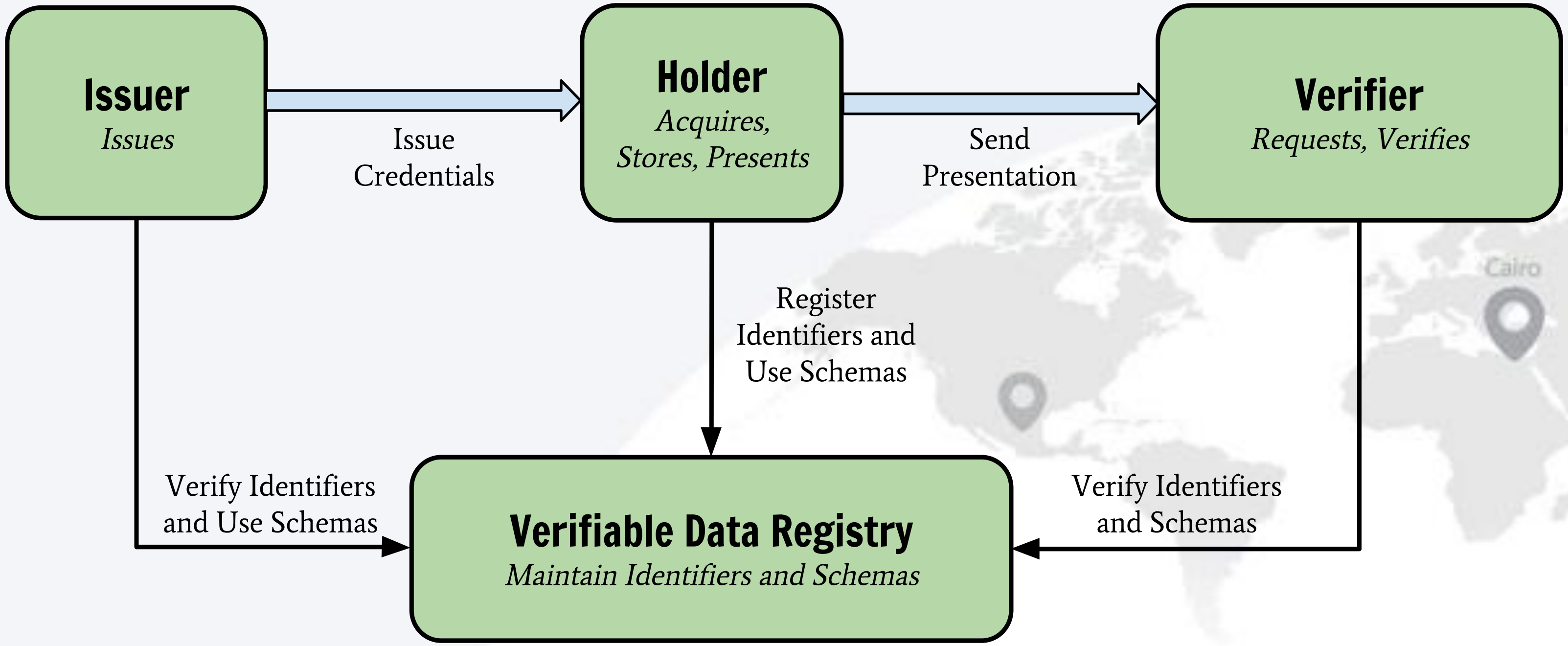
- New type of identifier for verifiable, "self-sovereign" digital identity
- Under the control of the DID subject, enabling independence from any specific:
  - centralized registry
  - identity provider
  - certificate authority



- URL enabling trustable interactions with DID subject
- DIDs resolve to DID Documents:
  - Verification methods
  - Service endpoints for interacting with the DID subject
- Examples:
  - Authentication
  - Requesting a digital signature on a document

W3C Verifiable Credentials

- W3C Verifiable Credentials WG
- The format for interoperable, cryptographically-verifiable digital credentials



Issuer
Issues

Issue Credentials

Holder
Acquires, Stores, Presents

Send Presentation

Verifier
Requests, Verifies

Register Identifiers and Use Schemas

Verify Identifiers and Use Schemas

Verifiable Data Registry
Maintain Identifiers and Schemas

Verify Identifiers and Schemas

DID Alliance

- **See** http://didalliance.org/
- The DID Alliance is an open industry association created to drive the development of a standardized, interoperable framework for decentralized identity services to ensure the authenticity of and establish trust in digital identities.
- The group will contribute to the creation of a global ecosystem, the formation and operation of a collaborative network, the diffusion of standardized technologies and the development of the decentralized identity industry.

Bootstrapping Digital Identity

- Trust sourcing
- Cross-ledger transaction support
- Inclusiveness
- Interoperability