A Word on Policy-based Credential Disclosure in SSI

5th Distributed Ledger Technology Workshop (DLT 2023)

Stefano Bistarelli, Chiara Luchini and Francesco Santini

Dipartimento di Matematica e Informatica
Università degli Studi di Perugia

May 25-26, 2023
IAM models

Self Sovereign Identity

**Self Sovereign Identity (SSI)** is a sovereign, enduring and portable identity for any person, organization, or body, that allows its owner to access all relevant **digital services** by using **verifiable credentials** linked to the identity in a privacy-preserving manner.

Unlike previous identity management systems where the service provider was at the center of the model, SSI is user-centric.
Self-sovereign identity

SSI ecosystem

SSI ecosystem is composed by:

- **Issuer**: creates and issues credentials to a holder;
- **Holder**: receives credentials from an issuer, retains it and when it is required, it shares credentials with a verifier.
- **Verifier**: receives and verifies credentials presented by a holder.
SSI issues

PROBLEMS
Collusion
Inference

SOLUTIONS
Usage constraints
Negotiation protocol

User
owns VC
has

Verifier
owns
has

Privacy

Disclosure policy

Security

Access policy
SSI system with AC model

- **DAC model** where the *holder* creates the access policy;
- **ORCON model** where the *issuer (originator)* creates the access policy.
SSI DAC model

Key Legend

- Optional
- Mandatory
- Stored in

Diagram:
- Issuer creates VCs
- Issuer issues VCs
- Holder requests VCs
- Holder creates and deploys
- Private storage controls
- Holder requests Holder's VCs and sends Verifier's VCs
- Verifier sends Holder's VCs
- Holder asks verification results
- Blockchain
- Smart Policy Holder checks Verifier's VCs
Future Works

- Define and detail **DAC/ORCON schema**;
- **Implementation** of these models;
- Possibility of using **ZKP** while exchanging credentials between user/verifier.
Thank You!

chiara.luchini@studenti.unipg.it