UNIVERSITÀ DEGLI STUDI FIRENZE

A.D. 1308 unipg
DIPARTIMENTO DI MATEMATICA E INFORMATICA

Workshop su Modellazione e Verifica Formale di Sistemi di Dialogo, Argumentation per Cybercrime e Civil Security Applications | 5 Feb 2026, Rimini

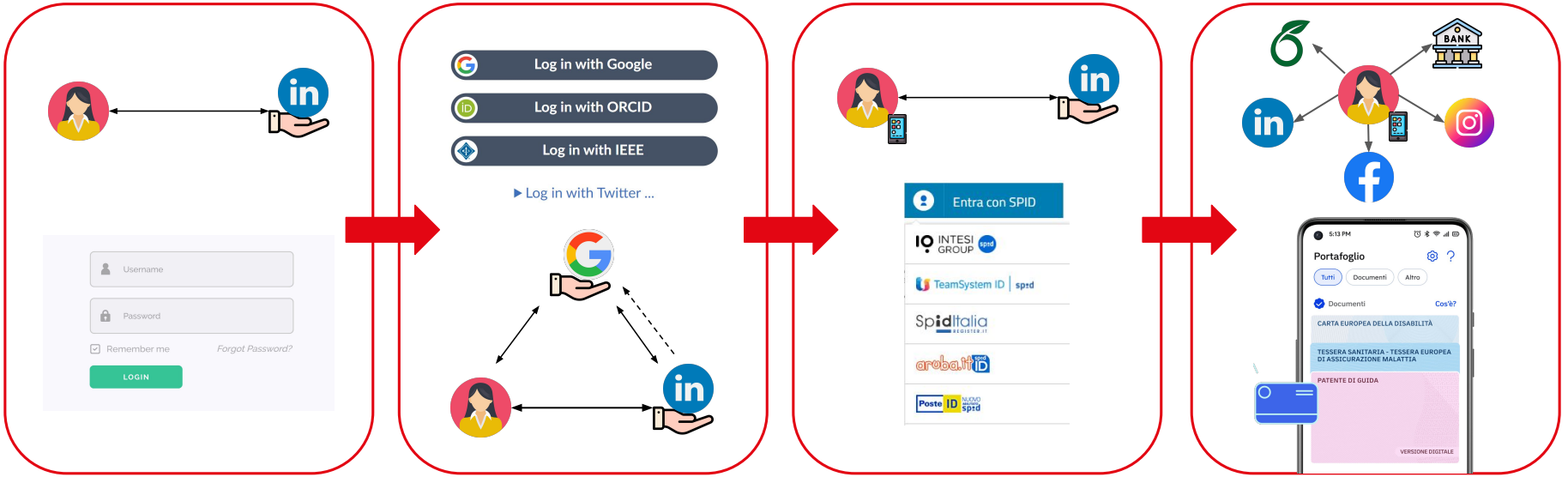
Unauthorized Disclosure Prevention and Reasoning on VC Claims in SSI

PhD Student
Chiara Luchini[1,2]

Supervisors
Prof. Stefano Bistarelli[2]
Prof. Francesco Santini[2]

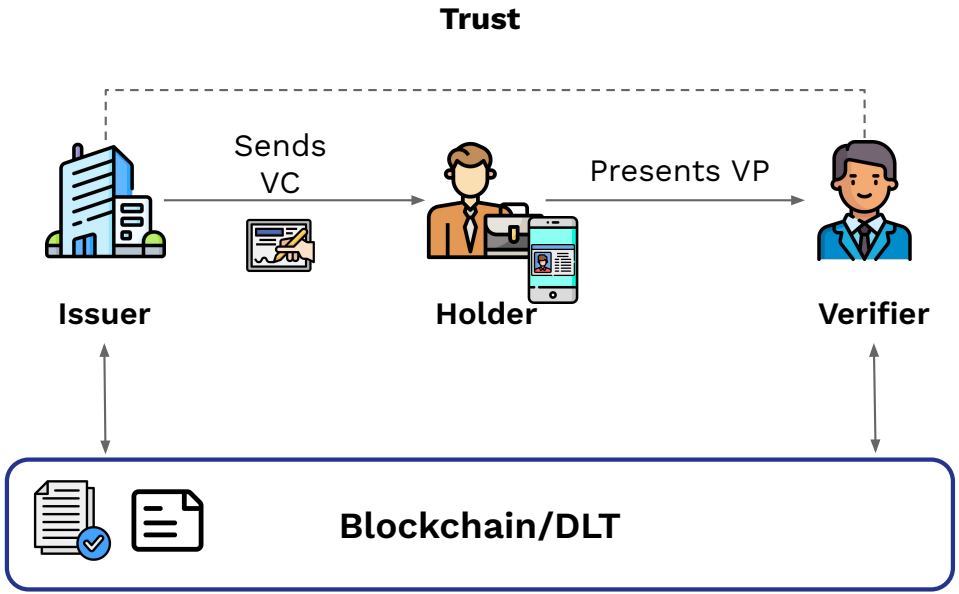
[1]*Dipartimento di Matematica e Informatica "Ulisse Dini", Università degli Studi di Firenze*
[2]*Dipartimento di Matematica e Informatica, Università degli Studi di Perugia*

Identity and Access Management Evolution



Schardong F, Custódio R. *Self-Sovereign Identity: A Systematic Review, Mapping and Taxonomy*. Sensors. 2022; 22(15):5641.
Dipartimento per la trasformazione digitale, *IT-Wallet: tre documenti digitali su app IO per i primi 50.000 cittadini*. 2024.

Self Sovereign Identity

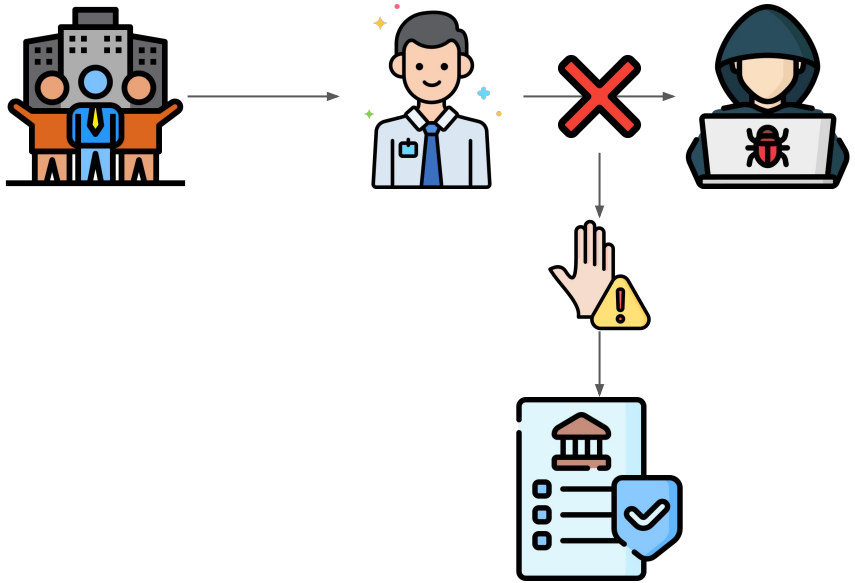


Self Sovereign Identity (SSI) *is a* ***sovereign, durable and portable identity*** *for any person, organization or entity that allows its owner to access all digital services using* ***verifiable credentials*** *in a privacy-preserving manner.*

Motivation: Unauthorized Disclosure

Industries handling sensitive data are vulnerable to **unauthorized disclosure** of sensitive information.

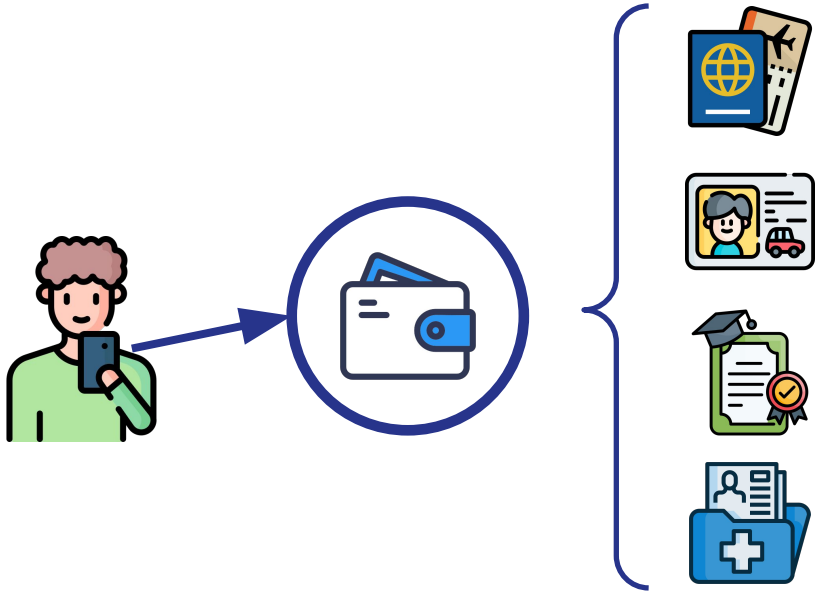
Self-Sovereign Identity (SSI) systems provide enhanced security and privacy, but **improper policy enforcement** may still lead to data leaks.



S. Bistarelli, **C. Luchini**, and F. Santini. *"Policy-based Credential Disclosure in SSI by Using ORCON-based Access Control."* 6th Distributed Ledger Technologies Workshop (DLT2024), 14-15 May 2024, Torino (TO), Italy.

Terms Of Use

Terms of use may be used by the **issuer** or **holder** to specify the conditions under which a verifiable credential or verifiable presentation has been issued.



If the recipient (a holder or verifier) is **not willing to adhere** to the specified terms of use, then they do so on their **own responsibility** and might incur **legal liability** if they violate the stated terms of use.

Terms of Use

“termsOfUse is insufficiently specified”[1]

Verifiable Credentials Data Model v1.1

```
"termsOfUse": [{
    "type": "HolderPolicy",
    "id": "http://example.com/policies/credential/6",
    "profile": "http://example.com/profiles/credential",
    "prohibition": [{
      "assigner": "did:example:ebf...c21",
      "target": "http://example.edu/credentials/3732",
      "action": ["3rdPartyCorrelation"]
    }]
  }]
```

Verifiable Credentials Data Model v2.0

```
"termsOfUse": {
     "type": "TrustFrameworkPolicy",
     "trustFramework": "Employment&Life",
     "policyId": "https://policy.example/policies/125",
     "legalBasis": "professional qualifications directive"
   }
```

[1]World Wide Web Consortium (W3C), termsofuse is insufficiently specified, https://github.com/w3c/vc-data-model/issues/1010, 2023.

D. Longley M. Sporny and D. Chadwick. *"Verifiable credentials data model v1.0"*. Technical report, W3C, 2022.
D. Longley M. Sporny and D. Chadwick. *"Verifiable credentials data model v2.0"*. Technical report, W3C, 2023.

Terms Of Use in Organizations

- Organizations can use terms of use to define the **conditions for using verifiable credentials**, including whether the credential can be transferred.
- These terms act as **contracts** with potential legal implications.

Credential Terms of Use (IV-CT01) requirement[1]: systems should enable organizations to specify terms of use for each credential they issue, and these terms should ideally be **technically and legally enforceable** to prevent misuse.

[1]R. Bochnia, D. Richter and J. Anke, "Self-Sovereign Identity for Organizations: Requirements for Enterprise Software," in IEEE Access, vol. 12, pp. 7637-7660, 2024, doi: 10.1109/ACCESS.2023.3349095.

Overview of Current ToU Implementation

The digital identity landscape is shifting from centralized architectures to user-centric, decentralized models like **Self-Sovereign Identity** (**SSI**).

❗ Despite this progress, most existing SSI wallet implementations focus on **individual users** and lack important features for organizational use.

✅ We conducted a systematic secondary review of the current industrial digital wallet landscape assessing how these wallets implement the **Terms of Use (ToU)** field.

🎯 The goal is to inform the development of digital wallets tailored for enterprises and governments in SSI ecosystems.

S. Bistarelli, **C. Luchini**, and F. Santini. "*Analyzing terms of use adoption in ssi digital wallets: A review of current implementations*". In Proceedings of the 7th Distributed Ledger Technologies Workshop (DLT2025), Pizzo (VV), Calabria, Italy, 2025.
S. Bistarelli, **C. Luchini**, and F. Santini. "Analysing the Adoption of the Terms-of-Use Field in EBSI Digital Wallets". In Proceedings 9th International Workshop on Cryptocurrencies and Blockchain Technology (CBT 2025), Toulouse, France, 2025.

Final results

Wallet	Vendor	ToU	License
Connect.Me	Evernym	No	Apache 2.0
Trinsic	Trinsic Technologies Inc	No	MIT
Jolocom SmartWallet/ Jolocom SDK	Jolocom	No	AA2-SDK of Governikus GmbH/Apache 2.0
SelfKey Identity Wallet	SelfKey	No	Apache 2.0
PingOne Neo SDK (Shocard)	PingOne Identity	No	Apache 2.0
Veramo (uPort)	DIF/Veramo User Group	No	Apache 2.0
Talao Wallet	Talao	No	Apache 2.0
Yivi (IRMA)	Privacy by Design Foundation	No	GPLv3
KayTrust SDK	NTT DATA	No	Apache 2.0
walt.id	walt.id	**Yes**	Apache 2.0

EBSI Conformant Wallets

Wallet	Vendor	ToU	License
Talao Wallet	Talao	No	Apache 2.0
walt.id	walt.id	**Yes**	Apache 2.0
IN2 Wallet	IN2	No	Apache 2.0
SimpleIdServer	SimpleIdServer	No	Apache 2.0
Identfy	Izertis	**Yes**	AGPL-3.0/ commercial/ MIT
Masca	Blockchain Lab:UM	No	Apache 2.0/MIT
Triveria SDK	Triveria	**Yes**	Commercial License
wwWallet	GUNet	No	BSD 2-Clause
Altme	Talao	No	Apache 2.0

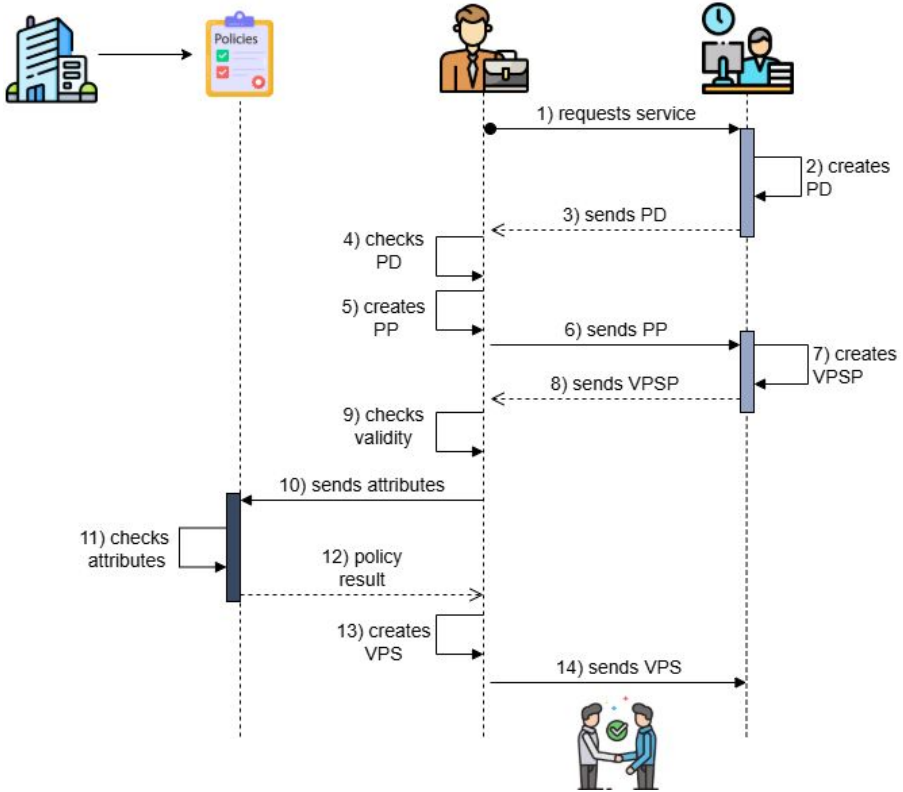
ToU for Unauthorized Disclosure

Using ToU for Unauthorized Disclosure

- Definition of an SSI model for specific scenarios whereby the **disclosure of holder credentials must be controlled**, i.e. company sector.
- Usage of **Terms of Use (ToU)** field in Verifiable Credential (VC) to describe how the the information can be disclosed:
  - **to whom** it may be disclosed
  - **what actions** they can perform
- Definition of an **“Agreement VC”** by the verifier to attest the acceptance of the ToU
- Illustration of the model with a concrete example.

S. Bistarelli, **C. Luchini**, and F. Santini. 2025. “*Controlling VC disclosure with Terms of Use and ABAC in SSI*”. In Proceedings of the 40th ACM/SIGAPP Symposium on Applied Computing (SAC '25). Association for Computing Machinery, New York, NY, USA, 389–390.
S. Bistarelli, **C. Luchini** and F. Santini, "*SSI Policies Implementing Terms of Use to Control VC Disclosure*," in 2025 IEEE International Conference on Pervasive Computing and Communications Workshops and other Affiliated Events (PerCom Workshops), Washington DC, DC, USA, 2025, pp. 25-30

Example Use Case Scenario

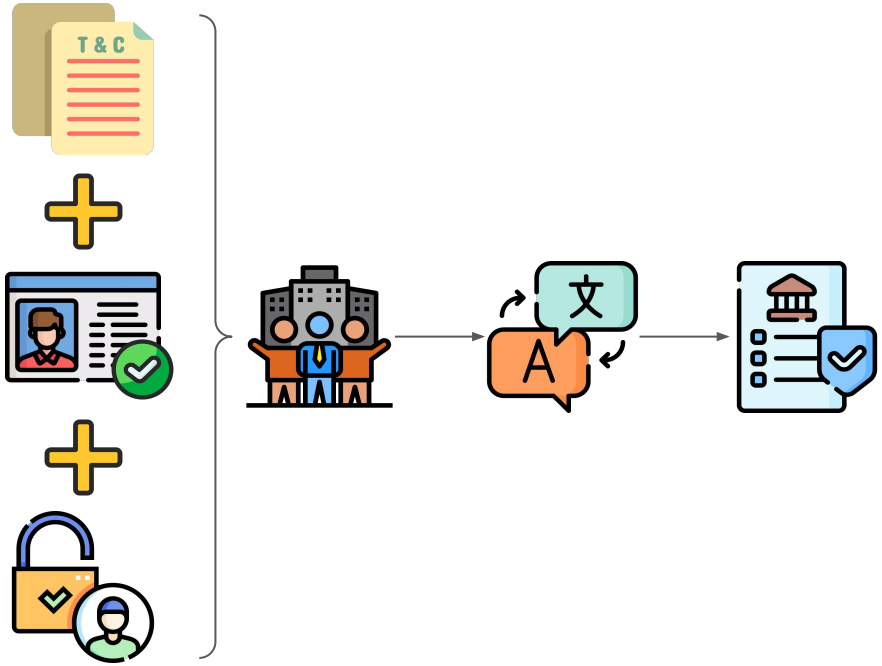


- Company → Employee → Business Partner
  - Company Badge as a VC:
    - Employee's ID, role, and access permissions.
- Policy Example:
  - *"Partners from Company X can access employee info during working hours only."*
- How it works :
  1. Issuer embeds ToU into VC.
  2. DIF Presentation Exchange
     - Presentation Definition
     - Presentation Submission
  3. Verifier must agree to ToU before accessing data (**Verifiable Presentation Submission Policy**):
     - verifier's VCs
     - Agreement VC
  4. Disclosure Policy model checks attributes before granting access.

ToU and Smart Policies

ToU and Smart Policies

- 💡 **Idea:** combining ToU, VC and AC.
- ❌ **Research Gap:** Manual translation of ODRL policies to smart contracts can be error-prone and inefficient.
- ✔ **Solution:** Define a translator from ODRL-ABAC policies to (Solidity) smart contract.



S. Bistarelli, **C. Luchini** and F. Santini, "*A Preliminary Approach for Translating ODRL to Smart Policies*" 2025 IEEE International Conference on Pervasive Computing and Communications Workshops and other Affiliated Events (PerCom Workshops), Washington DC, DC, USA, 2025, pp. 44-49.

Open Digital Rights Language (ODRL)

- A policy expression language standardized by the W3C that defines policies to manage:
  - **Permissions:** ability to exercise an Action over an Asset.
  - **Prohibitions:** inability to exercise an Action over an Asset.
  - **Duties:** obligation to exercise an agreed Action.
- Used in digital rights management, cloud access control.

```
{     “@context”:
"http://www.w3.org/ns/odrl.jsonld",
      “@type”: “Offer”,
      “uid”: “Policy:84112”,
      “permission”: [{
            “uid”: “P1”,
            “target”:
      “http://example.com/asset:9898.movie”,
            “assigner”:
      “http://example.com/party:org:abc”,
            “action”: “play”,
      }]}
```

ODRL-ABAC policy

ODRL

Constraints/ LogicalContraints

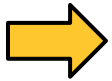
A **boolean/logical expression** that refines an Action and Party/Asset collection or the conditions applicable to a Rule.

+

ABAC

Attributes

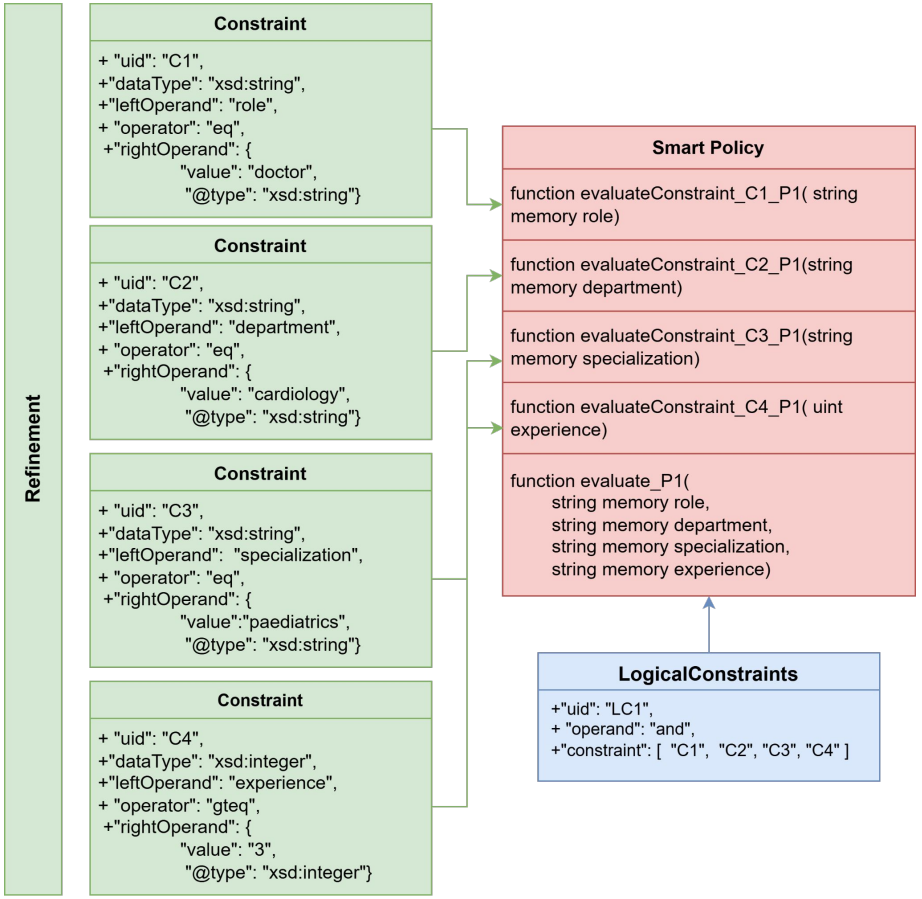
Characteristics of the **subject, object**, or **environment conditions.**



```
{"@context": "http://www.w3.org/ns/odrl.jsonld",
        "@type": "Offer",
        "uid": "Policy:84112",
        "permission": [{
                "uid": "P1",
                "target":
        "http://vc.com/document:8541",
                "assigner":
        "http://issuer.com/org:616",
                "action": "read",
                "constraint": [{
                        "uid": "C1",
                        "leftOperand": "dateTime",
                        "operator": "gteq",
                        "rightOperand": {
                                "value": "09:00:00",
                                "@type": "xsd:time"}},
                        {"uid": "C2",
                        "leftOperand": "dateTime",
                        "operator": "lteq",
                        "rightOperand": {
                                "value": "17:00:00",
                                "@type": "xsd:time"
                        }}]}]}
```

ODRL Policy Translation

- A hospital issues a VC containing a patient's medical history.
- Access is restricted to:
  - *Certified medical practitioners with >3 years of experience, from cardiology dept and with a specialization in pediatric.*
- Implementation:
  - ODRL defines who can access patient records and under what conditions.
  - Translated into a Smart Contract, enforcing rules on-chain.



Tested Smart Policies

- **Set Example:**
  - Verifies if a user is part of a predefined role set (e.g., "Project Manager").
- **Listing 1 Example:**
  - Requires meeting two constraints (time-based access control).
- **zkABAC Example:**
  - Defines multiple conditions for students to access a scholarship prize (five constraints):
    - Must be a bachelor student.
    - Must have an average grade > 27.
    - Must be enrolled for less than 3 years.
  - For the zkABAC, the deployment costs with 10 and 20 constraints increased by 41% and 130%.
- **Listing 2 Example:**
  - Example of the previous slide.

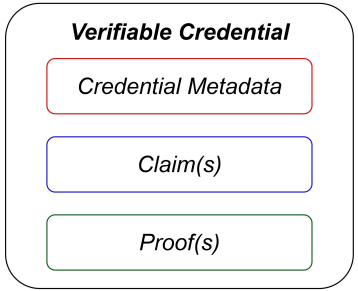
Example	*Deployment*	*Satisfied*	*Not Satisfied*
Set	1769328	5012	5012
Listing 1	537876	3335	2990
zkABAC	1136850	6237	6215
Listing 2	1287194	8471	8449

Gas cost of Smart Policies.

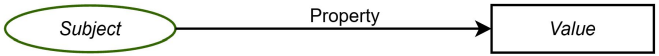
Reasoning on Credentials

What is a Verifiable Credential?

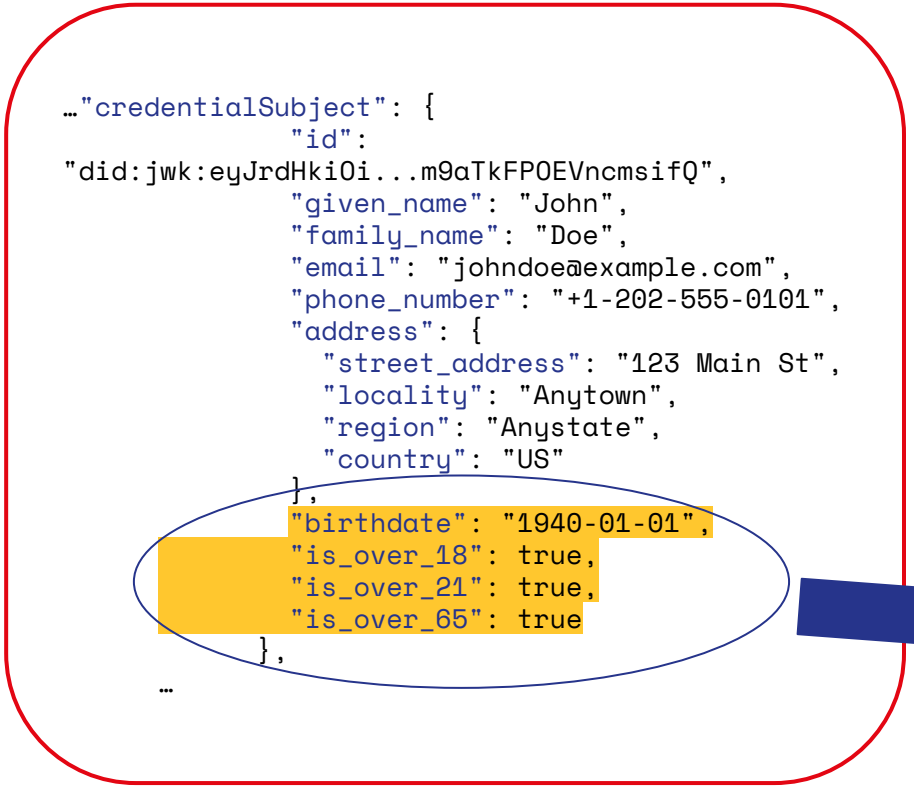
*A **verifiable credential** is a set of **tamper-evident claims** and **metadata** that cryptographically prove who issued it.*



*A **claim** is a statement about a **subject**.*
*A **subject** is a thing about which claims can be made. Claims are expressed using **subject-property-value** relationships.*



How is written a claim?

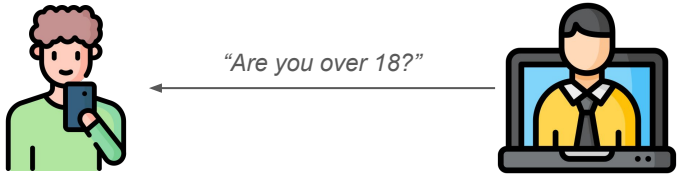


Claims can be of various **types** depending on the type of Credentials.
For instance an **Identity Credential** containing:

- given_name;
- family_name;
- email;
- phone_number;
- birthdate;
- address…

Same claim, written in different version to **minimize information disclosure**

Minimizing information disclosure




```
"birthdate": "1940-01-01",
"is_over_18": true,
"is_over_21": true,
"is_over_65": true
```

Also with **non-numerical values**

Real Age: exact match calculated as *current_year - birth_year = age (e.g 86)*

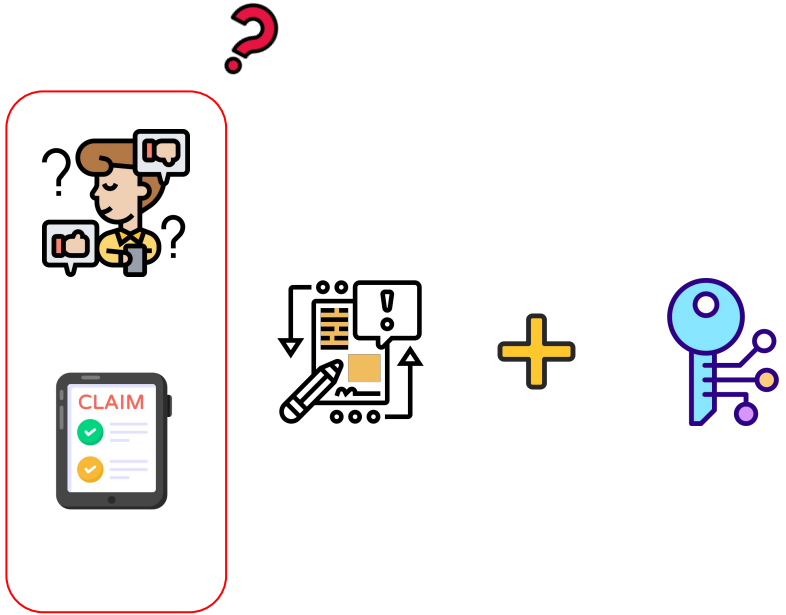
Loose Bind Strategy: **less tight bound** about the actual value of the attributes and thus provides a **higher uncertainty** about the actual values.

Tight Bind Strategy: the claim that **logically implies** the term in the disclosure policy and that is **closer** to the actual value assumed by the birth date.

F. Paci, D. Bauer, E. Bertino, D. M. Blough, and A. Squicciarini. 2008. *"Minimal credential disclosure in trust negotiations."* In Proceedings of the 4th ACM workshop on Digital identity management (DIM '08). Association for Computing Machinery, New York, NY, USA, 89–96.

Framework for VC Reasoning

- **Idea:** combining constraint solver with VC claims.
- **Research Gap:** No semantic reasoning on the VC claims.
- **Goal:** Framework for semantic reasoning on VC.



Thank you for your attention!

A.D. 1308
unipg
DIPARTIMENTO
DI MATEMATICA E INFORMATICA