UNIVERSITÀ DEGLI STUDI FIRENZE

A.D. 1308 unipg
DIPARTIMENTO DI MATEMATICA E INFORMATICA

8th Distributed Ledger Technology Workshop (DLT2026)
1-6 June 2026 | Pula, Sardinia, Italy

A Policy-Enforced SSI Framework Integrating ABAC, Terms of Use, and Smart Contracts

PhD Student
Chiara Luchini[1,2]

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

[1]*Department of Mathematics and Computer Science "Ulisse Dini", University of Florence*
[2]*Department of Mathematics and Computer Science, University of Perugia*

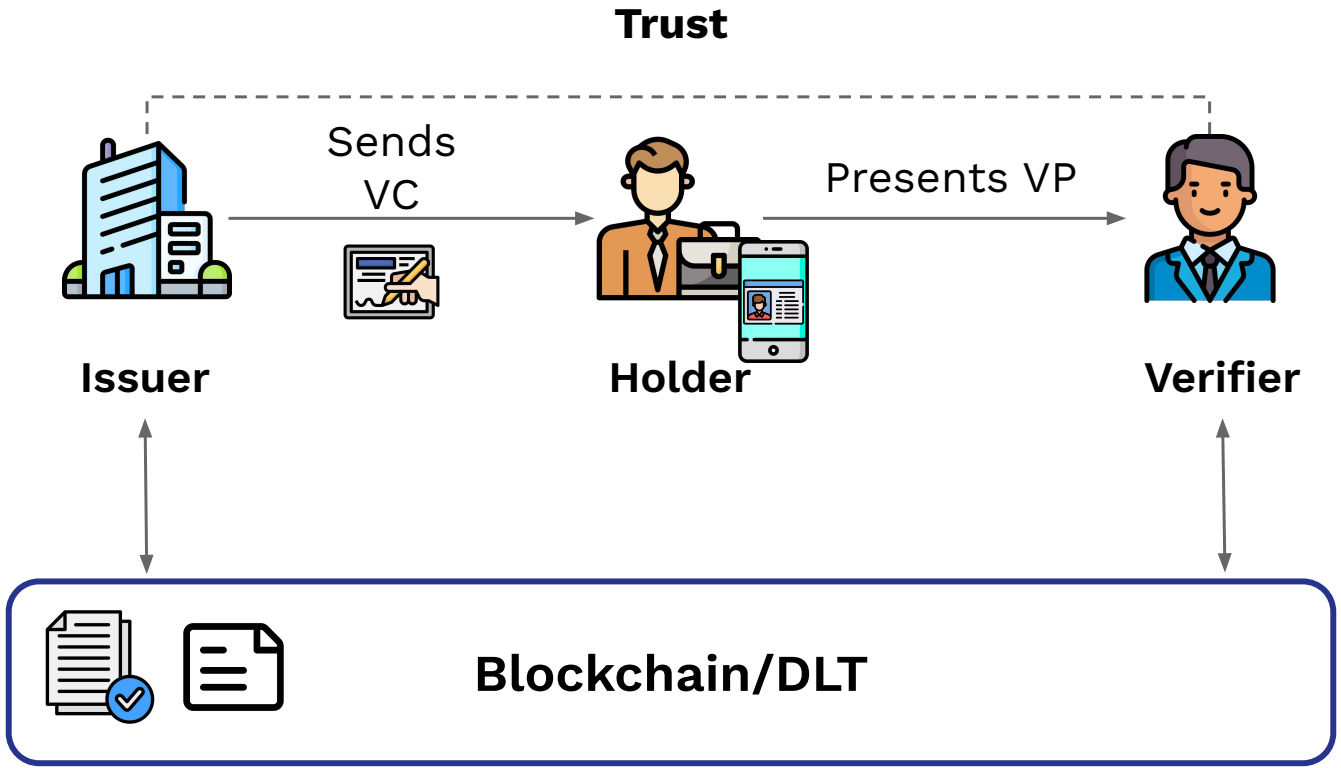
Outline

- What is SSI and motivations
- Overview of Current ToU Implementation
- Using ToU for Unauthorized Disclosure
- ToU and Smart Policies
- Conclusion

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.*

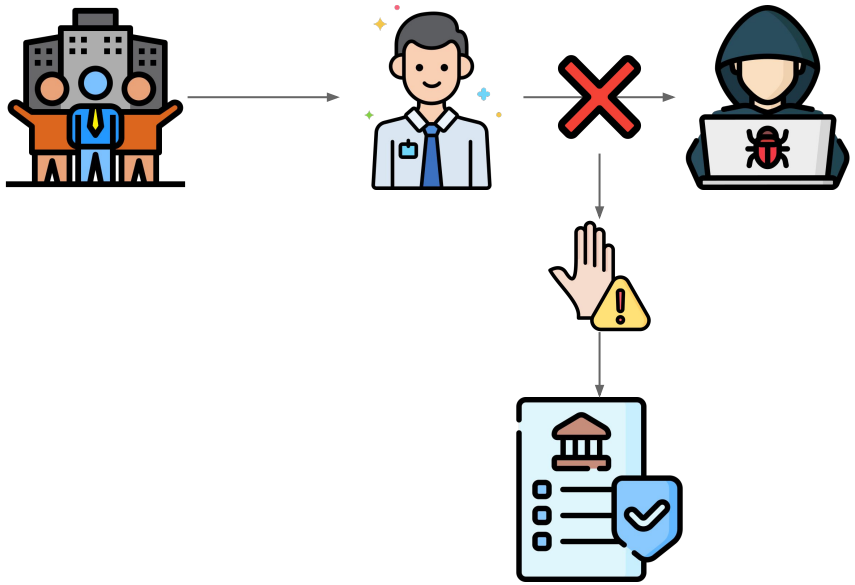
Self-Sovereign Identity workflow



Motivation: Unauthorized Use

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

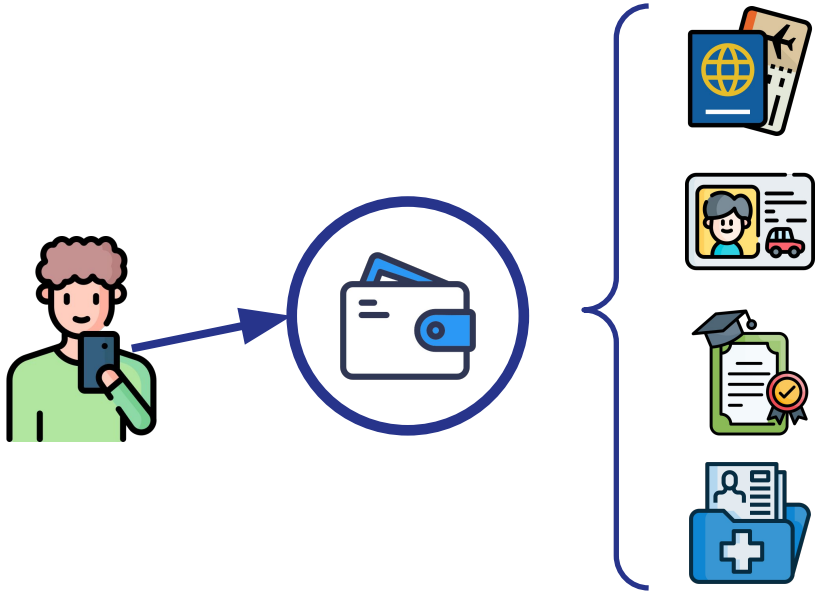
Self-Sovereign Identity (SSI) systems provide enhanced security and privacy, but **improper policy enforcement** may still lead to data leaks.



Stefano Bistarelli, Chiara Luchini, and Francesco 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.
M. Sporny, D. Longley, D. Chadwick, I. Herman, Verifiable Credentials Data Model v2.0 (W3C Recommendation), Technical Report, World Wide Web Consortium (W3C), 2025, url: https://www.w3.org/TR/vc-data-model-2.0/#unauthorized-use.

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, 2025.

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**).

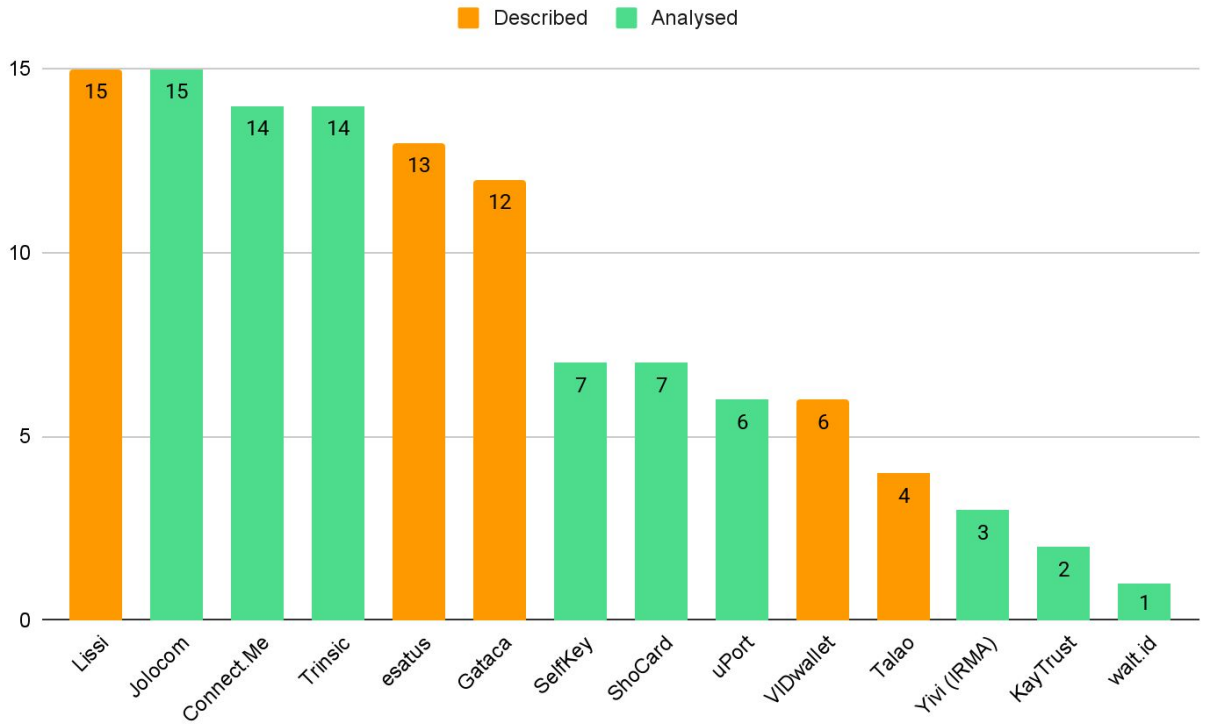
❗ Despite this progress, most existing SSI wallet implementations focus on **individual users** and lack important features for organizational use.

✅ 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.

Analysis of Digital Wallets



Most cited vendors and digital wallets.

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

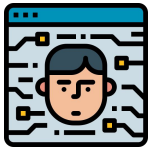
European Blockchain Services Infrastructure (EBSI)

- **Main goals:**
  - **Secure, trustworthy digitisation:** creation of **cross-border digital public services** enabled by blockchain technology.
  - **Verification, authenticity, and integrity:** point of truth for verifying credentials, documents, and official evidence.

EBSI is a distributed infrastructure of blockchain nodes, operated by **EU Member States** and partners in the **European Blockchain Partnership (EBP)**.

Notarisation

Education



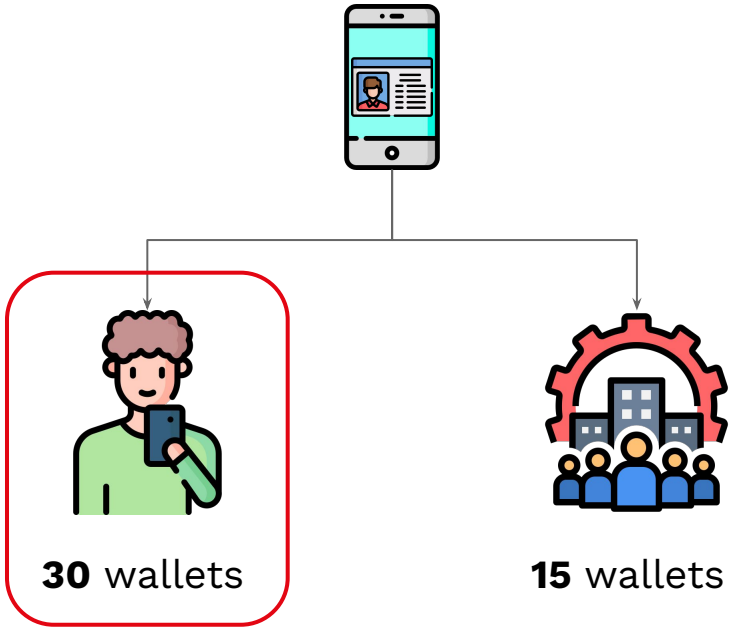
Identities

Trusted Data

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.

EBSI Conformant Wallets

- A **conformant wallet** is a wallet that has passed the **Conformance Test**.
- The test checks compliance with performance and functionality standards.
- The test evaluates the wallet's ability to:
  - **manage credentials** issued by a **mock issuer,**
  - **return** them correctly to a mock **verifier**.



EBSI Conformant Wallets

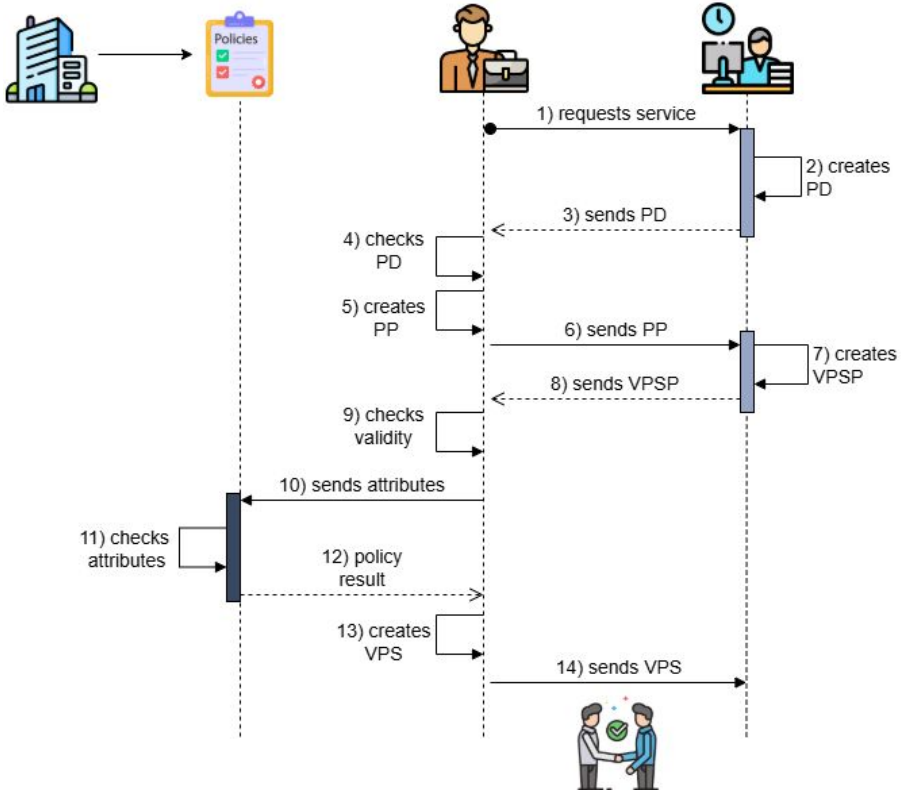
Wallet	Vendor	ToU	License
Talao Wallet	Talao	No	Apache 2.0
walt.id	walt.id	**Yes**	Apache 2.0
IN2 Wallet	IN2	No	Apache 2.0
SimpleIdServer	SimpleIdServer	No	Apache 2.0
Identfy	Izertis	**Yes**	AGPL-3.0/ commercial/ MIT
Masca	Blockchain Lab:UM	No	Apache 2.0/MIT
Triveria SDK	Triveria	**Yes**	Commercial License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

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 Implementation Example

```
termsOfUse": {
        "type": "IssuerPolicy",
        "policyAddress": "0
        xDd9aB71805917FfF3d09301F7…",
        "requiredCredentials":[{
        "vcType": "Company Badge",
        "vcProperties":["organization"],
},
{ "vcType": "Agreement Claim"}],
"prohibition": [
        {
        "assigner": “did:ethr:0x03926441848
        ...6e0702bb471f6ad”,
        "assignee": “AllVerifiers”,
        "target": “credential2459”,
        "action": [“store”]
        }]}}
```

Verifiable Credentials and ToU Fields:

- **policyAddress**: the value is a string identifying the address of the DP that must be called to check the attributes of the verifier.
- **type:** array of strings indicating the policy type applied to the VC.
- **requiredCredentials:** Array of elements containing all required attributes.
  - **vcType:** String identifying the required VC type requested.
  - **vcProperties:** Array of strings listing properties in the “credentialSubject” field.

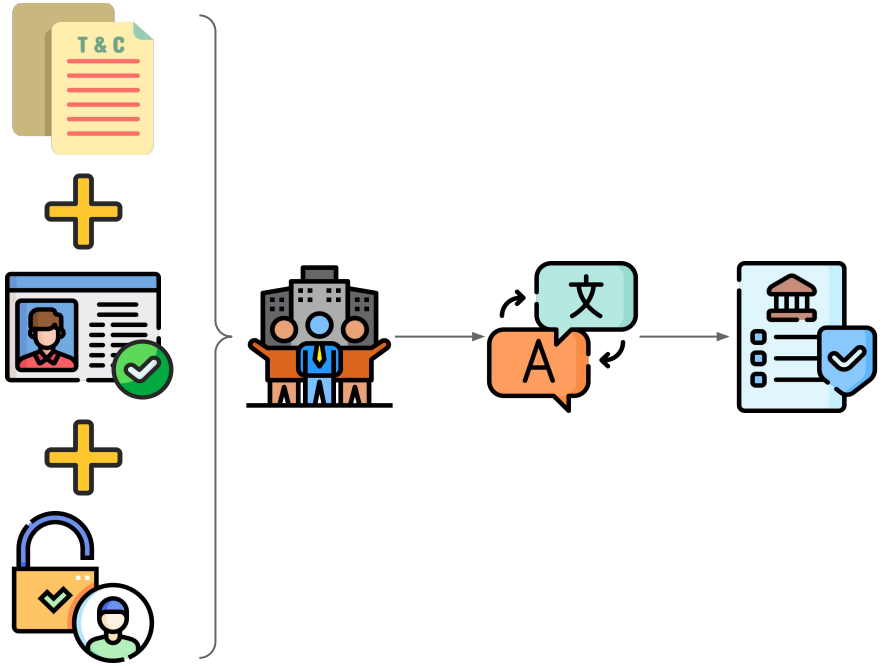
Agreement Claim VC example

- **Self-Claim Requirement:** The verifier must provide a self-claim (**Agreement Claim**), confirming acceptance of the ToU. This step is **mandatory** for the verifier to access the holder's credentials.
- **Legal Proof:** The self-claim acts as **legal evidence** in case of a policy violation by the verifier.
- **Blockchain Logging:** The final verification result is recorded on a blockchain transaction, ensuring **transparency** and allowing third parties to verify access.


```
{
 "@context": [
       "https://www.w3.org/ns/credentials/v2"
       ],
 "id": "credentialAgreementClaim1",
 "validFrom": "2024-01-08T00:00:00Z",
 "issuer":
"did:ethr:0x0654545211...dfewf4578sd4s54"
 "type": ["VerifiableCredential", "Agreement
Claim"],
 "credentialSubject": {
 "holderVC": "holdervc1"
 "agreementClaim": "I have read and agree to
the Terms of Use conditions."
}}
```

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

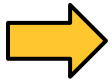
A **boolean/logical expression** that refines an Action and Party/Asset collection or the conditions applicable to a Rule.

+

ABAC

Attributes

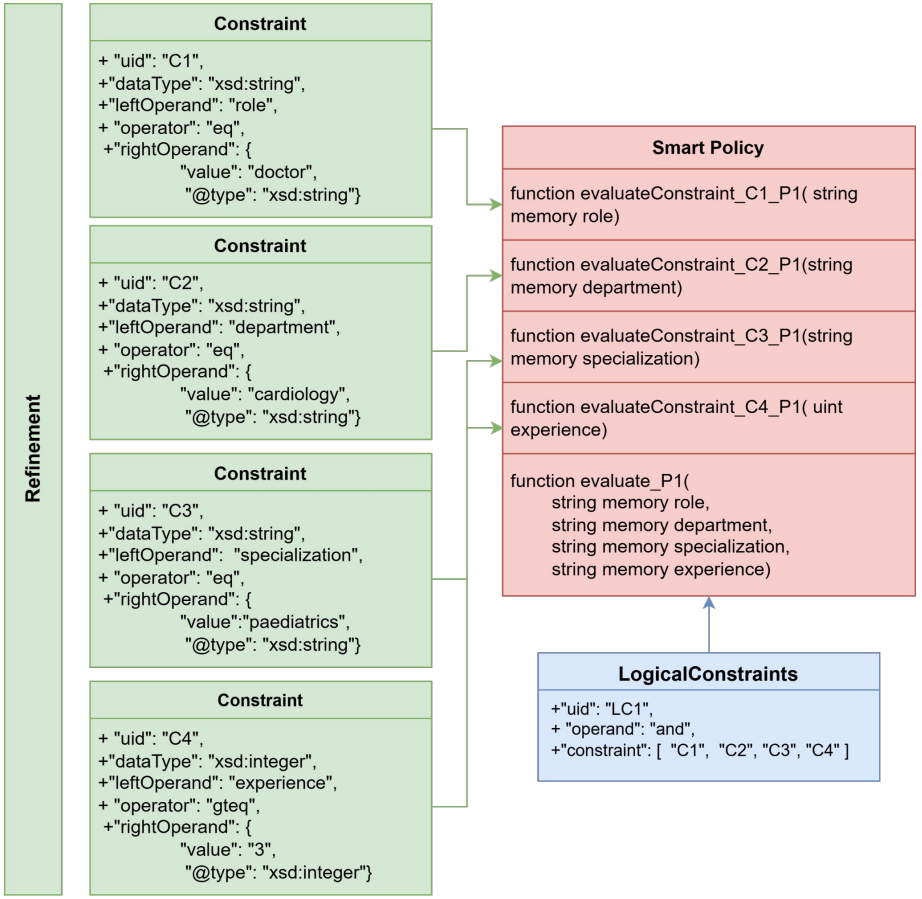
Characteristics of the **subject, object**, or **environment conditions.**




```
{"@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.

Conclusion and Future Works

- Many industrial wallets does not support the ToU feature.
- Definition of a protocol that uses the ToU field
- Translation of ODRL policies into Smart Contracts

- **Semantic Validation** of Verifiable Credentials
- Switching from a **Smart Policy** to a **local policy enforcement**

Thank you for your attention!

chiara.luchini@collaboratori.unipg.it

"A Policy-Enforced SSI Framework Integrating ABAC, Terms of Use, and Smart Contracts"
Stefano Bistarelli, **Chiara Luchini** and Francesco Santini