Policy expression using Verifiable Credentials

Using the ODRL Verifiable Credential Profile

Position Paper for the W3C ODRL 3.0 Workshop

Yassir SELLAMI, Gaia-X

Abstract

ODRL is already extensively expressive for Access and Usage Control Policies. What is missing — and would benefit most evaluators and implementers — is a direct link to an interoperable, generic, and verifiable claims mechanism. The W3C Verifiable Credentials (VC) standard is the perfect candidate for this role. This paper argues that extending ODRL 3.0 with a well-specified binding to Verifiable Credentials, or alternatively defining another generic yet enforceable method to reference specific claims within ODRL constraints, would greatly benefit ODRL policy evaluation in practice and specifically accelerate its integration with Data Spaces. We present a concrete protocol combining the ODRL Verifiable Credential Profile (ODRL-VC Profile), OpenID for Verifiable Presentations (OpenID4VP), the Digital Credentials Query Language (DCQL), and the Dataspace Protocol (DSP) as a working example of what such a binding enables.

1. Introduction

Data spaces are founded on the principle that data should be shared under conditions defined by the data rights holder. Access is therefore granted not solely on the basis of identity, but on whether a participant satisfies specific eligibility criteria. Such criteria may include jurisdictional residence, recognised ecosystem membership, compliance certifications, or specific contractual obligations.

The W3C Open Digital Rights Language (ODRL) has become a foundational policy language for expressing these conditions in machine-readable form. Across sectors, organisations increasingly rely on ODRL to encode permissions, prohibitions, obligations, and constraints. ODRL 2.2 is well-established in this role; the forthcoming ODRL 3.0 presents an opportunity to address a critical gap that limits practical deployments.

That gap is the absence of a standardised, interoperable mechanism for linking policy constraints to verifiable claims about parties. Policies describe what must be proven; but ODRL does not define how proof should be requested, presented, or validated in an implementation-neutral manner. The result is a persistent disconnect between policy definition and enforcement, forcing practitioners to fall back on manual verification, proprietary identity systems, or bilateral agreements that do not scale.

This position paper argues that ODRL 3.0 should close this gap by providing a normative binding to the W3C Verifiable Credentials standard, or — should a more general mechanism be preferred — by defining a generic, enforceable construct for referencing specific claims within ODRL constraint expressions. Either approach would transform ODRL from an expressive policy language into an end-to-end access-control mechanism capable of driving automated, privacy-preserving trust evaluation.

2. The Missing Link in ODRL Policy Evaluation

ODRL's constraint model is expressive: a policy author can restrict an action to parties satisfying conditions on virtually any attribute. Yet the specification leaves a crucial question open — how does an evaluator obtain trustworthy, machine-verifiable evidence that a constraint is satisfied at runtime?

In practice, three approaches are observed in deployed data spaces:

- Manual verification: operators vet participants out-of-band and hard-code access decisions. This does not scale and it's not the most cost-efficient.
- Proprietary identity integration: individual connectors implement custom credential checks, defeating interoperability.
- Trusted-list lookups: ecosystems maintain centralised registries; these introduce single points of failure and governance bottlenecks.

None of these approaches is reusable across ecosystems. Each requires bilateral agreement or custom implementation. The absence of a standard "claim reference" mechanism in ODRL means that the language, however expressive, cannot be the single artefact driving automated policy enforcement in an open environment.

Core position: ODRL 3.0 should define a normative way for a constraint operand to reference a specific claim in a verifiable assertion, together with the semantics of how evaluators must process that reference. W3C Verifiable Credentials, being an open W3C standard with wide adoption in digital identity infrastructure, are the natural candidate for this role. If the Working Group prefers a more abstract approach, a generic "verifiable claim reference" construct whose semantics can be bound to different backends (VCs, X.509 attributes, OpenID...) would equally close the gap.

3. Why W3C Verifiable Credentials are the Right Candidate

Verifiable Credentials (VCs) are a W3C Recommendation specifically designed to represent assertions about subjects in a cryptographically verifiable, machine-readable, and privacy-preserving manner. Their properties align directly with the requirements of ODRL policy evaluation:

- Decentralisation: trust in a credential does not require a shared central authority, only knowledge of the issuer's DID or public key.
- Selective disclosure: using SD-JWT or BBS+ signatures, a party can present only the specific claims required by a constraint, satisfying GDPR data minimization and similar Data Privacy regulations and best practices.
- Semantic precision: claim types can be identified by URIs, enabling ODRL constraint leftOperands to reference well-defined attributes.
- Revocability: VC status registries allow credentials to be revoked, keeping access decisions current without renegotiating policies.
- W3C provenance: alignment with VCs keeps the ODRL extension within the W3C standards ecosystem, reducing fragmentation.

Critically, W3C VCs already underpin major data space trust frameworks, digital wallet initiatives (EUDI Wallet, OpenID4VC ecosystem), and national digital identity programmes. An ODRL 3.0 binding to VCs would therefore connect to infrastructure that is already being deployed and mandated, rather than requiring new implementations.

4. The ODRL Verifiable Credential Profile: A Concrete Realization

To demonstrate feasibility, we present the ODRL Verifiable Credential Profile (ODRL-VC Profile), which extends ODRL by allowing constraint operands to reference claims contained within Verifiable Credentials. The profile is currently used in production data space pilots and serves as a concrete basis for the proposed ODRL 3.0 extension.

4.1 Expressing Verifiable Constraints in ODRL

Under the ODRL-VC Profile, the leftOperand of a Constraint identifies a claim type by URI. The rightOperand provides the required value or value set. The operator expresses the relationship. For example, a policy granting access only to organisations located in France, Belgium, or Spain can be expressed by referencing the country-code claim of an organisational identity credential. The policy remains entirely declarative; no credential query language appears in the ODRL document itself (it could be a potential path for a next version).

4.2 Automatic Translation to Credential Requests

One of the most significant contributions of the “Policy-Driven Contract Negotiation using ODRL and Verifiable Credentials” paper is a deterministic mapping between ODRL-VC constraints and the Digital Credentials Query Language (DCQL), the standard presentation-request language of the OpenID4VP ecosystem. This mapping is formally defined and allows an evaluator to automatically derive a credential presentation request from any ODRL-VC policy without manual configuration.

The consequence is that whenever a policy changes, the credential request generated from it changes automatically. Policy authors maintain a single authoritative artefact; the proof request is always consistent with the governing policy.

4.3 Integration with OpenID4VP

OpenID for Verifiable Presentations (OpenID4VP) provides the transport and protocol layer for requesting and receiving credential presentations. By positioning the data provider as an OpenID4VP verifier, the ODRL-VC Profile creates a seamless bridge between policy governance and deployed digital wallet infrastructure. The consumer’s wallet performs credential selection and presents only the information required to satisfy the policy, preserving sovereignty and minimising disclosure.

5. Integration with the Dataspace Protocol

The Dataspace Protocol (DSP) standardises the negotiation of contracts and the establishment of data-sharing agreements between providers and consumers. It defines states and transitions for offer, counter-offer, acceptance, and agreement but does not specify how eligibility verification should occur during negotiation.

The protocol presented in the companion paper defines a fourteen-step sequence that embeds Verifiable Credential presentation directly into the DSP contract negotiation state machine. Eligibility verification thereby becomes a native step in contract negotiation rather than a prerequisite managed by a separate system.

The implications for ODRL are direct: an ODRL Offer published by a provider encodes the access conditions. The protocol derives credential requests from those conditions, obtains

presentations, evaluates them, and either concludes an ODRL Agreement or rejects the negotiation. The entire lifecycle is machine-executable and auditable.

6. Privacy by Design and Data Sovereignty

A binding between ODRL constraints and Verifiable Credentials enables privacy-preserving policy evaluation by design. The evaluator requests precisely the claims specified by the policy and no more. Using selective disclosure techniques (SD-JWT), the presenting party reveals only those claims. The overall information exchange is strictly proportionate to the policy requirement.

From a sovereignty perspective, the party presenting credentials retains control: the wallet presents information only after explicit consent, and the party is fully aware of what is being disclosed. This is a significant improvement over traditional onboarding processes, which typically require broad document submission.

Furthermore, governance authorities retain the ability to define which issuers are trusted, which credential schemas are accepted, and how revocation is managed. The separation between policy semantics and trust framework governance is clean and principled.

7. Proposed Contribution to ODRL 3.0

Based on the above, we propose that the ODRL 3.0 Working Group consider the following additions:

- A Verifiable Credential Constraint Profile: a normative extension defining how ODRL constraint operands may reference claims in W3C Verifiable Credentials, including the syntax for leftOperand URI definitions, rightOperand value binding, and the semantics of evaluation.
- A standard mapping to credential query languages: normative guidance (or an informative annex) defining how ODRL-VC constraints map to DCQL or equivalent query formats, enabling automated derivation of claim requests from policies.
- If a VC-specific binding is considered out of scope: a generic “verifiable claim reference” construct, with semantics that can be bound to specific credential systems by implementers, preserving the generality of the ODRL core while enabling interoperable evaluation.

We offer the ODRL-VC Profile specification and the companion protocol paper as concrete inputs for the Working Group’s deliberations. Both are available as open specifications and have been considered in data space ecosystems.

8. Conclusion

ODRL has solved the problem of expressing access and usage control policies in machine-readable form. Significant progress has been made in parallel on digital identity standards, Verifiable Credentials, and wallet technologies. What has been missing is a standardised mechanism that connects these pieces into an operational workflow.

ODRL 3.0 is the right moment to close that gap. By introducing a normative binding between ODRL constraint expressions and W3C Verifiable Credentials — or a generic, enforceable claim-reference construct — the Working Group would enable fully automated, interoperable, and privacy-preserving policy evaluation across open ecosystems.

The protocol presented here, combining ODRL, Verifiable Credentials, OpenID4VP, DCQL, and the Dataspace Protocol, demonstrates that such a binding is technically feasible, deployable today, and aligned with existing W3C and OpenID Foundation standards. It represents a meaningful step toward data ecosystems in which access decisions are driven not by manual processes, but by verifiable evidence and transparent policy evaluation.

References

[1] W3C ODRL Community Group. *ODRL Information Model 2.2.* W3C Recommendation, 2018. https://www.w3.org/TR/odrl-model/

[2] W3C Credentials Community Group. *Verifiable Credentials Data Model 2.0.* W3C Recommendation, 2024. https://www.w3.org/TR/vc-data-model-2.0/

[3] OpenID Foundation. *OpenID for Verifiable Presentations (OpenID4VP).* Draft Specification, 2024. https://openid.net/specs/openid-4-verifiable-presentations-1_0.html

[4] Sellami, Y. *Policy-Driven Data Space Contract Negotiation using the ODRL Verifiable Credential Profile and OpenID4VP.* Gaia-X, 2026.

[5] Gaia-X Association. *ODRL Verifiable Credential Profile Specification.* https://docs.gaia-x.eu/technical-committee/architecture-document/

[6] Eclipse Foundation. *Dataspace Protocol Specification.* https://eclipse-dataspace-protocol-base.github.io/DataspaceProtocol/

[7] OpenID. *Digital Credentials Query Language (DCQL).* https://openid.net/specs/openid-4-verifiable-presentations-1_0.html#name-digital-credentials-query-l

[8] W3C ODRL 3.0 Workshop. https://www.w3.org/2026/ODRLWS/index.html