Draft GDN Governance Framework for Digital Credential Exchange Networks

**** Interim ****

CONSULTATION DOCUMENT

Version: October 10 to 20, 2025

CONSULTATION NOTE:

This revised framework will be published on the GDN website in the governance section from October 10 to 20, 2025 to allow for a final consultation phase for the GDN Project Governance Framework.

Final adjustments resulting from that consultation phase will be made for final board review and approval at the October 28, 2025 GDN board meeting based on community inputs from this phase.

The final approved version from the October 28 GDN board meeting will be published to the Oslo Annual Meeting within the Attendee hub to support the launch at that meeting. The community will be asked to use the Framework over the next year and identify what work, what needs to be changed, and what more needs to be added to support network development and sustainability of recognition and verification of credentials using digital technologies.

---

1. Introduction

In an era defined by rapid technological advancement and increasing reliance on data, organizations are confronted with both vast opportunities and complex risks. Artificial intelligence (AI), big data, and digital platforms now shape how we communicate, make decisions, deliver services, and create value. Yet without clear guidance, oversight, and accountability, these same technologies can exacerbate inequality, erode trust, and compromise privacy.

As digital credential exchange networks continue to emerge worldwide, a **trusted governance framework** is essential for ensuring security, interoperability, transparency, a citizen focus, and long-term sustainability. It provides a coherent set of principles and practices to guide the secure, responsive and effective use of digital technologies.

Through extensive community consultation, the Groningen Declaration Network (the GDN Network) has created the GDN Governance Framework which provides a flexible, principle-based guide for governments, institutions, vendors, associations, indigenous organizations, and citizens as lifelong learners working together to enable trusted, interoperable, and sustainable digital credential exchange networks.

It ensures leadership focuses on:

- **Security** of personal data and records
- **Interoperability** across jurisdictions and systems
- **Transparency** in design and use
- **Citizen and lifelong learner focus** as the guiding purpose
- **Sustainability** for long-term viability

This **GDN Governance Framework** offers a coherent set of **principles and practices** to support the development of **credential ecosystems**. It offers regional, national, and transnational applicability as **interoperability is a fundamental aspect of an interconnected world** where systems, technologies, and institutions must communicate seamlessly to enhance efficiency, innovation, and governance. By aligning around the core principles—Trust, User-focus, Local context, Inclusivity, and Privacy/Sustainability—stakeholders can foster innovation while safeguarding the rights and interests of learners and citizens worldwide.

These **principles** are:

- **Technology-agnostic**
- **Open-standard based**
- **Locally grounded but globally interoperable**

The GDN Governance Framework is **not prescriptive**. It is a **living document** and guide to aid planning, benchmark progress, support dialogue, and enable adaptation to diverse contexts. Each organization in the Groningen Declaration Network (the GDN Network) and beyond is encouraged to embrace these principles as a means of ensuring comprehensive consideration in ecosystem planning.

---

2. Guiding Principles

To anchor governance in shared values, the GDN Governance Framework advances the following principles:

1. **Trusted & Accountable**
    - Ensure transparent policies and responsible data stewardship whether through regulation or agreed upon protocols in trusted ecosystems.
    - Establish and maintain transparent policies and responsible data stewardship through regulation, protocols, and trusted practices.
    - Use data only for its intended purposes, with clear consents, guardrails, and visibility, including for learners impacted, into downstream connections.

2. **User-Focused**
    - Center privacy, security, and learner control by design.
    - Ensure learners control access to their credentials.
    - Guarantee that citizens and lifelong learners retain ownership of their own data.

3. **Locally Situated**
    - Respect local sovereignty, autonomy, context, and authority.
    - Support solutions that align with regional and national priorities and interoperability while maintaining international interoperability.
    - Consider the potential for supporting the multilingual contexts in design as appropriate to context.

4. **Inclusive**
    - Design systems that are usable, and open to participation by all stakeholders as appropriate to their roles and purpose.
    - Consider the global context as an opportunity to advance knowledge and broader interoperability.
    - Pay particular attention to marginalized groups, Indigenous organizations, and under-resourced institutions in an effort to raise all learners towards future rapid access to jobs and learning, key components of a vibrant local and national community and economy.

5. **Privacy Compliant, Technically Interoperable, Secure, Sustainable, Adaptable**
    - Uphold strong data protection standards, with compliance to relevant local and international laws.
    - Support flexible design across a typology of technology models and open standards to accommodate business and stakeholder needs and local regulatory, technical, and institutional landscapes.
    - Consider the opportunities for transformational change due to ongoing innovations, including considering AI and its implications and possibilities.

- Ensure ecosystems are financially and technically sustainable (interim and long term).
- Commit to ongoing risk assessment and related standards.
- Encourage modularity and adaptability to technological advances to help bridge historical contexts and systems to future opportunities and advances.

Operating Practices

To ensure that the **GDN Framework principles** are not only **aspirational** but also **actionable**, clear operating practices are necessary to guide implementation across diverse digital credential exchange networks. These practices address governance models, legal and policy considerations, technical infrastructure and standards, trust and verification frameworks, financial sustainability, and dispute resolution and governance evolution.

The practices help translate principles into **measurable commitments**, **provide consistency** across stakeholders, and ensure that governance remains adaptive to evolving technologies and local contexts. They serve as the **operational backbone** of the framework, supporting **trust, access, and sustainability**.

3. Governance Model

3.1 Multi-Stakeholder Approach

Effective governance requires input from many stakeholders in its creation and delivery which is contextually situated. Fit for purpose matters when considering the stakeholders to consult. Examples of general stakeholders to engage are:

- Global and local experts
- Government agencies (e.g., ministries, regulators)
- Educational institutions (e.g., primary, secondary, CEGEPs, vocational institutes, colleges, universities, and Indigenous credential issuers)
- Workforce trainers (e.g., that provide instruction in upskilling, reskilling, and cross skilling and are possibly also credential issuers)
- Employers and industry (e.g., skills validation, labor market linkages)
- Industry associations and standards bodies (e.g., that are impacted by and relevant to the network being designed)
- Technology providers
- Civil society (e.g., advocacy, privacy, and consumer protection organizations)

- Indigenous and community organizations
- Citizens and lifelong learners (credential holders and data owners)

3.2 Governance Body Options

Depending on context, governance may take the form of:

- Non-profit consortia
- Public–private partnerships
- Government-led initiatives with independent oversight
- Hybrid or other locally appropriate models

Core responsibilities include:

- Defining purpose and issues and opportunities to address with the network;
- Developing mechanisms and methods to engage with stakeholders, manage change, and ensure trust in the planned network;
- Defining relevant early and later stage policies and minimum standards;
- Ensuring compliance with applicable regulations;
- Managing disputes;
- Maintaining technology neutrality to enable choice and local responsiveness.

---

4. Legal & Policy Considerations

- **Regulatory Compliance**:
  - Uphold, support and/or evolve international and local privacy laws.
  - Utilize or create cross-border recognition frameworks.

- **Data Governance & Protection**:
  - Enable ability for credential holders (citizens and lifelong learners) to retain ownership and control over data.
  - Align retention and deletion policies to local law.
  - Enable flexible models (self-sovereign identity, federated identity, centralized repositories).

- **Risk Mitigation**:
  - Implement safeguards against data breaches.
  - Avoid penalties for non-compliance by aligning to applicable laws.
  - Address bias in AI systems through transparency and fairness.

5. Technical Infrastructure & Standards

- Encourage **open standards**.
- Support interoperability across **decentralized, federated, centralized, and hub-and-spoke models**.
- Maintain flexibility for diverse levels of digital maturity.
- Consider location and storage of data to ensure alignment with local regulations and principles of digital sovereignty.

---

6. Trust & Verification Frameworks

- Support existing and establish new **trust registries** (or equivalent) to reliably validate credential issuers.
- Enable **auditing and compliance mechanisms** to ensure ongoing system integrity.
- Allow for **tiered verification frameworks** depending on context and capacity as opposed to centralized models. For example, different entities maintain different authorities or accountabilities over different aspects of credential validation and recognition. As practical examples, a higher education institution needs to verify a credential from an official source issuer for reasons that may be different than that needed by a regulatory body. Different authoritative trust agencies serve different purposes. Verification frameworks need to consider that context.

---

7. Financial Sustainability

- Explore **mixed funding** models.
    - Public sector support for infrastructure
    - Membership-based consortia
    - Transaction-based fees (if equitable and not burdensome)
- Ensure affordability for citizens, lifelong learners, and smaller institutions.

---

8. Dispute Resolution & Governance Evolution

- Define **transparent** processes for dispute resolution, including mediation where appropriate.
- Establish review cycles to **adapt** governance to new regulations, technologies, and lessons learned.
