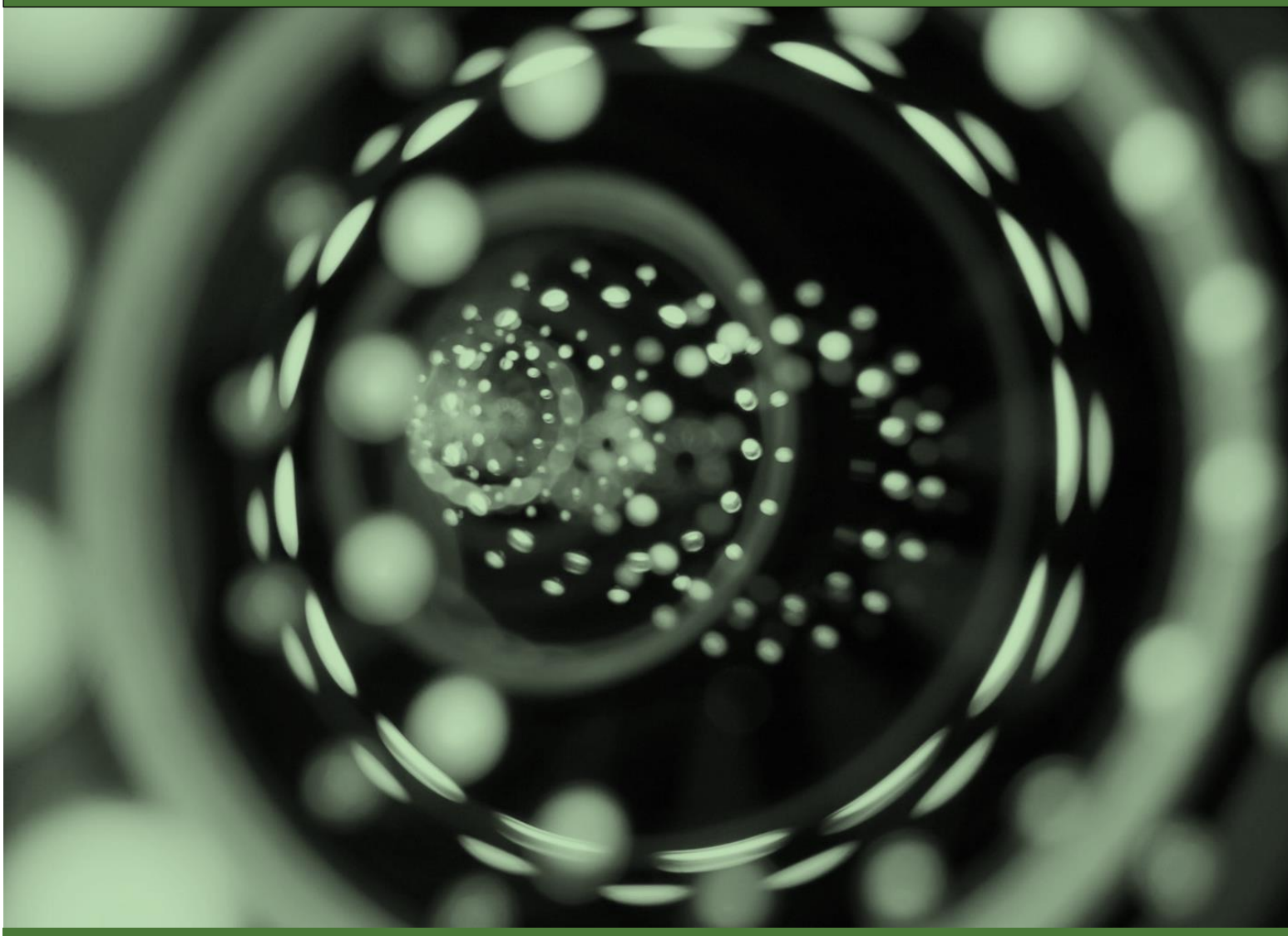

The Groningen Declaration Network

Creating Interoperable Networks and Systems

August 2024

THE GDN NETWORK

Abstract

The report outlines the Groningen Declaration Network's (GDN) efforts to enhance global d
exchange and interoperability within the post-secondary education sector. It emphasizes the importance of fostering global collaboration, adopting open standards, and investing in verifiable credential technologies to facilitate secure, citizen-centered digital credentialing. The report provides actionable recommendations for GDN members, aiming to create a more inclusive and efficient digital credentialing ecosystem that empowers learners and supports economic growth through improved credential portability and data security.

This report was prepared by the Groningen Declaration Network (GDN)'s Technology Interoperability Working Group with support from the GDN Board and support team. It encompasses the collective insights and contributions of various members within the working group, alongside community advocates and industry thought-leaders in the post-secondary education sector.

The GDN Network extends appreciation to the members of the GDN Technology Interoperability Working Group for their work on this report.

- David Moldoff, CEO, Academy One (*Co-chair)*
- Sharon Leu, Executive-in-Residence JFFLabs, Jobs for the Future (*Co-chair)*
- Takis Diakoumis, Senior Director Digitary Engineering, Parchment, an Instructure Company
- Joanne Duklas, Executive Director, Groningen Declaration Network; Researcher/Consultant, Duklas Cornerstone Consulting Inc.
- Victoriano Giralt, Head of Systems Administration Service, University of Málaga
- David Haynes, CEO, International Education Evaluations
- Koichi Nakasaki, Chief Research Officer, Institute for Future Engineering (IFENG)
- Jan Joost Norder, Product Owner - International Division, DUO
- Simone Ravaioli, Director of Global Ecosystem & Innovation, Parchment, an Instructure Company

Peer review was provided by the GDN Network Executive Board Members:

- Jelger de Boer, (Board President), Account Manager, DUO
- Melanie Gottlieb, (Board Vice-President), Executive Director, AACRAO
- Kathleen Massey, (Board past President), Vice Provost (Students), University of Lethbridge
- Anthony Manahan, (Board Secretary), Director Student Mobility, HES
- Alexander Knoth, (Board Treasurer), Talent Group Lead - Public Sector Advisory, Deloitte Consulting

We would also like to extend thanks to the GDN Support Team provided by Duklas Cornerstone Consulting Inc.

- Amadeus Narbutt (Researcher, Editor)
- Joanne Duklas (GDN Executive Director, Managing Editor)
- Sybil Massey (Graphic Design)

Table of Contents

Executive Summary & Key Recommendations

The GDN Network through the support and guidance of the GDN Technology Interoperability Working Group examined the question of how to stimulate and evolve a secure, trusted, and scalable global digital record

exchange spanning borders and boundaries, capabilities and localized differences. This work was guided by the GDN Board approved Terms of Reference for the Working Group (see Appendix 1).

The report provides an overview of the models evident in the ecosystem and concludes with recommendations for moving forward which are intended to inspire and support GDN member efforts to grow their knowledge of digital credential exchange and interoperability and to adopt best practices for organizational, cross-sector, and pan-national network design. The appendices provide resources, illustrative case studies, and critical questions to assist individuals and organizations in thoroughly evaluating governance, expectations, alternatives, implementation, and envisioning potential projects.

One central aspect of the GDN's mission is fostering greater adoption of globally accepted principles and frameworks that support interoperability. A primary objective of the GDN is to champion best practices that embody globally accepted specifications (evolving into standards) for secure, citizen-centered consultation, and the portability of digital student data across the learner life cycle, from enrollment to employment and all phases in between.

The GDN Statement of Ethical Principles provides the underlying rationale for this work. Principle 4 emphasizes that digital student data depositories, service providers, and other relevant stakeholders in the GDN network should collaborate on developing common access methods, common data definitions, and shared best practices as a community, seeking efficiencies and capabilities of electronic records exchange that enable learner digital data portability. For this, the GDN promotes internationally recognized electronic exchange specifications, as well as any future internationally approved specifications. The underpinning ethos to any implementation effort is to avoid closed systems that prevent learner mobility and credential portability.

The GDN believes that there are substantial benefits to economic growth when students possess international mobility. Mobility empowers people, providing them the opportunity to study, live, and work wherever they want or need. When people are mobile, whether as students or jobseekers, it is critically important that the skills and competencies they have previously earned are recognized, regardless of where they acquired them. Concomitantly, credential portability is also beneficial to an array of other stakeholders, including educational institutions, industry and employers, human resources professionals, credential evaluators, and standards bodies. Because of this, there is a growing need for the exchange of digital student data instead of traditional paper-based academic credentials that exist today.

This represents a call to action for GDN members to consider ways to develop and adopt an open and interoperable technical infrastructure for digital credentials, whether formal academic records or skilled credentials, that are anchored in individual agency and control and that transition away from the limitations of closed, inoperable data systems architectures. A thematic summary of the recommendations outlined in this report are listed below:

- Foster global collaboration and harmonization of data exchange through adoption and mapping of standards
- Adopt and promote open standards
- Invest in Verifiable Credentials technologies
- Launch educational training initiatives for stakeholders

After a secondary review of the outcomes of the GDN Technology Interoperability Working Group, as well as additional research, the GDN also presents the following recommendations:

- Design user-centric systems using Privacy-By-Design principles

- Develop change capacity to enable scalable adoption at the national level that embodies new ways of working together and supporting learners through supporting policies, governance frameworks, systems, and technology

These additional suggestions require further study and will serve to extend the research and work embedded in this report.

Definitions

Mobility

Mobility and digital nomadism are becoming increasingly common employment and education modes, with people moving proactively and reactively following their aspirations or escaping circumstances that are negatively impact their wellbeing and social mobility. There are instances where these individuals are seeking studies that span geographic boundaries and who may lack prior credential documentation. Institutions, potential employers, and government agencies face challenges in recognizing achievements, skills, competencies, and experiences gained outside familiar contexts, due to the high costs associated with reviewing and assessing such achievements. These challenges are compounded by fragmented record-keeping practices, lack of standardized definitions, reliance on decentralized truth sources, and the security of records maintained by a limited number of entities.

The transition from paper to digital records, while facilitating access to one's learning history, is hampered by resistance to adopting shared practices, fears of vulnerability, and a lack of ownership beyond core missions. Competing interests further complicate this landscape, including institutional security concerns, manual processing burdens, and the lack of clear benefits. This results in barriers to countries' and economies' ability to leverage the diverse journeys of individuals. Mobility presents unique challenges as individuals navigate different economies, political systems, and cultural landscapes, all while facing financial constraints and more. But mobility also presents an opportunity for the post-secondary sector to act on behalf of all learners to address these challenges.

Credential Portability

Credential portability can be viewed through a spectrum of comparability and familiarity, focusing on how societal participants recognize credentials beyond a surface level. It is crucial for learners transitioning between institutions due to job changes, relocation, or other reasons, to ensure their prior achievements and experiences are recognized.

Credential portability also aids employers in hiring and promotion decisions by enabling easy comparison of qualifications. The process involves the electronic or manual transfer of records between institutions, affirming the recognition and acceptance of the learner's qualifications.

In today's world, learner mobility has become increasingly important given rising trends of mobile lifestyles and immigration. Credential portability allows learners the flexibility they need while still ensuring that their qualifications are recognized and accepted by other institutions.

Interoperability

Interoperability is being defined in multiple ways in other settings. For the purposes of this report, the definition includes enabling distinct information systems to communicate and understand the information exchanged between them by utilizing shared forms of data and protocols. There are four principal types of interoperability: semantic, syntactic, structural, and foundational. Each plays a critical role in facilitating comprehensive and effective data exchange.

Semantic interoperability utilizes a common vocabulary that paves the way for accurate and reliable communication among individual devices and their software. This fluent machine-to-machine communication depends on the ability of different source data systems to map different terms to shared semantics, or meaning. *Examples: Credential Engine CTDL.*

Syntactic interoperability allows two or more systems to communicate and exchange data. Syntactic interoperability refers to the packaging and transmission mechanisms for data. *Examples: IMS, SIFA, SPEEDY, and EMREX.*

Structural interoperability represents the ability of the recipient system to interpret information at the data field level. *Examples: IMS, PESC or SIFA transaction schemas.*

Foundational Interoperability is the basic level of exchange of information. The received information is not interpreted without user intervention. It enables the digital information transition from one channel to another at the most basic level. Examples: Institutions sending semester or term reports in a requested format; or an institution sending a PDF student transcript to another organization to verify degree completion.

Interoperability is achieved when two or more systems exchange and make use of data in a secure and effective manner. This, in turn, enhances communication efficiency, improves access to critical information, and supports better decision-making. Interoperability is also instrumental in streamlining operations and delivering superior services to learners by allowing easy access and exchange of data across various systems, including colleges, universities, training organizations, credential evaluators, and learner-facing tools.

Interoperability enables organizations to more easily access and exchange data across different systems and platforms, such as colleges, universities, training organizations, credential evaluators, and learner-facing tools. By allowing different providers to access credential records more easily, interoperability also helps to improve the quality of decision making. Ultimately, interoperability can be a powerful tool for organizations to streamline operations and deliver better learner services.

Interoperability is a goal that emphasizes the importance of efficiently sharing and reusing data, as well as organizing processes in a way that makes systems easy to use and tasks straightforward to complete. This goal often involves bridging the gap between different systems or applications, each designed for specific purposes, which can present challenges. Addressing these challenges requires a significant amount of engineering work to ensure these various systems can operate together seamlessly.

By focusing on interoperability, institutions can ensure that a wide range of academic and administrative tasks—from managing course content and admissions to handling student records and financial aid—are more integrated and automated. This not only improves the experience for users, such as students, faculty, and staff, but also helps the institution run more smoothly and efficiently.

Educational institutions use numerous applications and digital services that cover both core and supplementary functions, including everything from curriculum planning and human resources to student services and facility management. The effort put into making these systems interoperable pays off by making operations more streamlined and aligned with the institution's goals. However, achieving this level of interoperability is an ongoing challenge due to the need to continuously update and refine these systems.

The Progress of Interoperability

This section outlines how digital credentials (like diplomas and certificates) can be seamlessly received, stored, and shared by individuals, no matter where they were obtained. This process, known as digital credential interoperability, gives people control over their own educational data. It requires connecting different data systems in a way that ensures the details about the credential, the organization that issued it, the person who owns it, and any additional information it contains are kept intact, reliable, and meaningful for whomever is responsible for verification. However, the development of this interoperability varies widely around the world. Five key abilities are necessary for achieving full interoperability:

Trust through Digital Signatures: Using digital signatures to verify the authenticity of documents.

Registry of Credentials: Having a detailed list or registry that includes all credentials and their issuing organization.

Shared Format for Content: Ensuring there is a common format for the information contained in credentials.

Common Protocols for Communication: Establishing standard methods for various actions like authenticating identities, making requests, sending and receiving data, and updating information.

Understanding Credential Value: Making sure credentials can be compared and understood in terms of the skills and knowledge they represent, which is often determined by specific qualification frameworks and the requirements of communities or industries.

These capabilities are essential for creating a system where digital credentials are easily and universally exchangeable, bolstered by technological setups such as Application Programming Interfaces (APIs) that facilitate the smooth transfer of data.

PDF Digital Signature

PDF documents with Digital Signatures provide portability across different hardware, operating systems, or applications, making them a foundational method for sharing achievements and credential information. This widespread accessibility means that for most global citizens, showcasing credentials through PDFs is a convenient and universally accepted practice. The interoperability of Digital Signatures relies on a mathematical scheme that verifies a document's authenticity, ensuring the signer's identity, the content's integrity, and non-repudiation. Legislation in various countries, such as the eIDAS in Europe, the e-Sign Act in the US, and the Electronic Signature Law in China, alongside widespread adoption across numerous applications, underscores the Digital Signature's role as a highly interoperable solution.

However, PDF Digital Signatures primarily facilitate human-to-human interactions. For machine-to-machine interoperability, PDFs can be embedded with XML[1] or JSON[2], though agreement on the XML/JSON data model is essential. In the United States, a voluntary organization – the Post-Secondary Education Standards Council (PESC)[3] was established in 1997 and has led major efforts for XML/JSON standardization, though there has been siloing and fragmentation in the standards landscape. Just within the US, XML digital credential data models are currently

[1] Extensible Markup Language

[2] JavaScript Object Notation

[3] Postsecondary Electronic Standards Council: PESC | HOME

fragmented into 6 different models[4]. Outside of the United States, adoption is even more fragmented and marginal.

Open Badge

Addressing the issue of fragmented data models, the Open Badge initiative offers a disruptive solution by leveraging the psychological impact on individual learners. Open Badge, a technical specification for embedding learning records within PNG images, aligns with contemporary social networking practices, enabling learners to visually share their achievements. This approach not only enhances the sense of accomplishment but also advertises the service and data standard through social media, encouraging a shift towards a de facto standardization.

Rapidly adopted by over 1,450 institutions since its introduction by the Mozilla Foundation and the MacArthur Foundation in 2011[5], Open Badge has significantly outpaced other technical specifications in terms of adoption. The subsequent launch of the Badgr open-source project by Concentric Sky further accelerated this spread, with more than 200 million credentials issued to date, far surpassing the volume of other digital credentials technical data models and specifications[6].

Open Badge has not only expanded technical specifications but also fostered new educational opportunities, contributing to the integration of traditional and lifelong learning. With the Open Badge's interoperability that allows each educational module to openly express and share the sense of learning accomplishment consistently across multiple education providers, it has spawned new educational providers such as MOOCs (Massive Open Online Courses), corporate partnerships (such as Google and Goldman Sachs), non-profit organizations, and international organizations (such as the World Bank).

Despite its success, the high interoperability and openness of Open Badge present challenges, including its vulnerability to tampering and reliance on hosting vendors, potentially risking digital credential loss if vendors exit the business. These issues highlight the need for balance between openness and security in the evolving landscape of digital credentials.

"Blockchain Credentials" (An Example)

Blockchain credentials have emerged as one solution to the challenges of ensuring tamper-proof documentation and reducing dependency on hosting vendors, building on the foundation of the Open Badge 2.0 data model. The Blockcerts initiative, launched by the Massachusetts Institute of Technology in 2017, leverages the Bitcoin blockchain and Open Badge standards to issue verifiable degree credentials. This approach guarantees the tamper-proof nature and immutability of credentials on the blockchain's public ledger, allowing graduates to independently hold and verify their graduation certificates without the need for intermediary hosting services.[7]

Developed collaboratively by the MIT Media Lab and another company formerly called Learning Machine, the Blockcerts framework was introduced to the public along with its source code and design concepts via GitHub in

[4] S. Stanfield, National Student Clearinghouse (personal communication, 2022)

[5] Skipper, W. (2002). Personal communication.

[6] Clements, K., West, R. E., & Hunsaker, E. (2020). Getting started with open badges and open microcredentials. *The International Review of Research in Open and Distributed Learning, 21*(1), 154-156.

[7] Duffy, K. H., Schmidt, J. P., & Nazaré, J. (2016, June 3). *What we learned from designing an academic certificates system on the blockchain*. MIT Media Lab.

2016.[8] This release coincided with advocacy for the concept of *Self-Sovereign Identity* (SSI), a model of identity management that places the control of personal information in the hands of individuals, thus enhancing privacy and autonomy over data sharing.[9]

Chris Jagers of Learning Machine highlighted the significance of this innovation in 2018, noting that blockchain technology could prevent the monopolization of credential verification and empower individuals with ownership of their identity documents, free from reliance on the original issuers or any specific vendor.[10]

This approach has garnered support not only for its technical merits but also for its potential to protect the educational qualifications of refugees and others affected by crises, aligning with the *Sustainable Development Goals* (SDGs) and addressing concerns over the monopolistic control of personal data by major technology platforms.[11]

The broader adoption and development of the Blockcerts, the SSI model, and other distributed models have fostered a global ecosystem supportive of decentralized identity. Notably, in 2018, the Blockcerts team contributed to the World Wide Web Consortium (W3C)'s development of "DIDs: Decentralized Identifiers," a technical specification that further solidifies the framework for SSI. The formation of the Digital Credentials Consortium (DCC) in 2019, comprising MIT, four other U.S. universities, and four European institutions, marked one of the significant steps toward establishing a robust, globally recognized ecosystem that champions the principles of SSI.[12]

Verifiable Credentials Data Model

The formation of the DCC was influenced by the parallel development of blockchain credential technical specifications across Europe and North America.[13] To harmonize these efforts, DCC brought together contributors such as Concentric Sky, the architects of Open Badge 2.0[14], the IMS Global Consortium, a leader in the open badges ecosystem, and the Groningen Declaration Network (GDN), with a collective goal to create an interoperable data model that moves beyond the environmentally burdensome proof-of-work blockchains like Bitcoin.[15]

This collaborative effort aimed to establish the W3C's Verifiable Credentials Data Model as a technical standard. The IMS Global Consortium has declared its support, stating that future iterations of the Open Badge (Open Badge 3.0 and Comprehensive Learner Records (CLR) 2.0) will align with the Verifiable Credentials Data Model. This

---

[8] Ibid.

[9] Power, R. (2021, November 10). SSI: Self-sovereign identity explained. *Medium*. https://blog.cheqd.io/ssi-self-sovereign-identity-explained-9969cdd0c5d

[10] Schembri, F. (2018, April 25). Digital diplomas - Blockchain technology gives grads control over their academic credentials. *MIT Technology Review*.

[11] Der, U., Jähnichen, S., & Sürmeli, J. (2017). Self-sovereign identity - Opportunities and challenges for the digital revolution. *Computer Science*. Published in ArXiv, abs/1712.01767.

[12] World Wide Web Consortium. (2021, August 3). Decentralized identifiers (DIDs) v1.0 - Core architecture, data model, and representations. *W3C Proposed Recommendation*.

[13] Digital Credential Consortium. (2020, February). Building the digital credential infrastructure for the future. https://digitalcredentials.mit.edu/wp-content/uploads/2020/02/white-paper-building-digital-credential-infrastructure-future.pdf

[14] Skipper, Wayne. (2002). Personal communication.

[15] Digital Credential Consortium. (2020, February). Building the digital credential infrastructure for the future. https://digitalcredentials.mit.edu/wp-content/uploads/2020/02/white-paper-building-digital-credential-infrastructure-future.pdf

alignment signifies a pivotal move towards integrating blockchain credentials and others like it with open badges, illustrating a clear path of convergence.

Rooted in the principles of SSI, the Verifiable Credentials Data Model is designed for scalability across various sectors, including education, retail, finance, insurance, professional certification, and legal affairs. It promotes data openness and ensures the autonomy of credential holders while offering tamper-proof, timestamped, and expiring credentials with enhanced legal validity compared to Open Badges.[16] By addressing the limitations associated with Open Badge, such as vendor dependence and privacy concerns, Verifiable Credentials pave the way for a new era of digital recognition that acknowledges skills and achievements universally.

The evolution from blockchain credentials to the Verifiable Credentials model, catalyzed by the disruptive influence of Open Badge, suggests a shift from traditional organization-driven standardization to a more learner-centric approach. This shift indicates that a focus on the needs and rights of learners is not only viable but essential for fostering interoperability and inclusion on a global scale, whilst also recognizing the need for credential integrity through links to issuing bodies.

Key Recommendations & Conclusion

The following recommendations are proposed to advance the goals of the Groningen Declaration Network (GDN) and its stakeholders in enhancing global digital record exchange and interoperability within the post-secondary education sector.

Foster Global Collaboration and Harmonization of Standards: Encourage and facilitate collaboration among educational institutions, government, standards bodies, industry stakeholders, and technology providers to develop and adopt a unified series of standards as appropriate to technology contexts and credential purpose to enable interoperable digitization. This should include the establishment of common data definitions, access methods, translation mapping, and interoperability protocols that can transcend local and national differences, leveraging insights from successful organizational approaches and technological models.

Adopt and Promote Open Standards: Advocate for the adoption of open standards for digital credentials, which will foster interoperability and translation mapping. These approaches have shown promise in enhancing portability, accessibility, and control over digital credentials for learners, which aligns with modern privacy regulations and the GDN's mission of facilitating secure, citizen-centered credentialing and digital data portability.

Invest in Verifiable Credentials Technologies: Support the research, development, and implementation of verifiable credentials technologies as viable solutions for creating tamper-proof, universally recognizable, and portable digital credentials. This recommendation is informed by the successful case studies of Blockcerts and the evolving Verifiable Credentials Data Model, which offer scalable, privacy-respecting, and environmentally sustainable alternatives to traditional credentialing systems.

Launch Educational Training Initiatives for Stakeholders: Implement comprehensive educational programs and training initiatives aimed at policymakers, institutional management, government stakeholders, and business leadership across the education sector. These programs should focus on raising awareness of the benefits of digital credential interoperability, providing guidance on best practices for system implementation, and offering standards guidance for adopting interoperable technologies . These trainings should be cross-cutting, emphasizing the multidisciplinarity of credential

[16] O'Neill, K. (2021). Digital credential vendor selection: An organizational fiduciary responsibility.

digitization. Such initiatives could help overcome barriers to adoption, mitigate fears of vulnerability, and foster a culture of innovation and collaboration in digital credentialing.

There are two additional recommendations that emerged after a secondary review of the outcomes of the GDN Technology Interoperability Working Group and additional research. These are not intended to suggest a comprehensive list but illustrate that the work continues to help advance next stage discussions and work.

Design User-Centric Systems With Privacy-By-Design: To advance digital credentialing, systems should be designed with a user-centric approach, incorporating Dr. Ann Cavoukian's "Privacy by Design" principles, which prioritize user control and data security from the outset. The integration of SSI frameworks ensures that individuals maintain ownership and control over their personal data, fostering trust and usability.

Develop Change Capacity for New Systems and Technology: Institutions, organizations, and governments have enduring legacy systems and standards which enable current state operational effort and support for learners. There is an opportunity for the GDN, through leveraging its network, to support the bridging of legacy systems to new technologies through education, supporting standards development, and facilitating capacity building for nation-state digital credentialing efforts.

The findings and recommendations of this report underscore the importance of interoperability, global collaboration, and the adoption of innovative technologies such as distributed ledgers and verifiable credentials to overcome the challenges of credential portability and data security. The report emphasizes the need for a harmonized and informed approach to standards and protocols that can bridge localized differences and foster international mobility and recognition of qualifications.

By advocating for open architectures, open standards, user-centric models, and investment in new technologies, alongside educational initiatives for stakeholders, the GDN aims to lead a transformative shift towards a more inclusive, equitable, and efficient digital credentialing ecosystem. The recommendations offer actionable insights for GDN members and the wider educational community to implement, promising to enhance the portability of learner digital data and contribute to the economic growth and empowerment of individuals worldwide.

As the landscape of post-secondary education continues to evolve, the collective effort and commitment of all stakeholders to these goals will be critical in realizing the vision of a globally connected and accessible education sector. The journey ahead is ambitious but, with the foundation laid by this report and the ongoing work of the GDN and its partners, it is a journey that promises to unlock new opportunities for learners and institutions alike.

Appendix 1: Terms of Reference for Groningen Declaration Network (GDN) Technology Interoperability Working Group

Vision

Supporting the GDN's vision of student mobility through trusted electronic data exchange, integration, open standards, and interoperability.

Purpose

This working group is tasked with:

- Consult an expert panel of GDN members and experts in technology, data privacy, and international credential exchange to understand the current and planned efforts to promote interoperability of digital credentials (by April 2023);
- Develop a white paper describing principles of interoperability of digital credential portability (by August 2023) that will provide a framework and recommendations for exploring new technologies that enable data sharing while promoting individual agency, security, and privacy by design;
- Develop recommendations for future GDN activities and collaborations to advance credential portability through technology interoperability (August 2023);

Scope

This group serves an advisory role and has no decision or financial approval authority or budget. The group reports to the GDN board through the GDN executive director.

Principles

The GDN principles and statement of ethics guide the work of the group as available at https://www.groningendeclaration.org/statement-of-ethical-principles/. It is expected that the final report and work be anchored in these explicitly. Further, members of this working group should be current signatories to the GDN or become signatories by GDN Jordan.

Appendix 2: Key Concepts for Interoperability

This appendix is designed to aid in the planning and organization of a digital credentialing project, as well as to offer a review of existing digital credentialing systems and structures for policymakers and institutional

management. It is divided into two main sections: the first explores various organizational approaches adopted worldwide, and the second delves into the current options and trends in digital credential technology.

Organizational Approaches

The move towards digitizing higher education credentials began in the 1970s but was initially limited to a small number of institutions. It wasn't until the 1990s, with the launch of national projects in select countries, that the digitization of credentials began to be implemented on a national scale. Early adopters of such national projects included Sweden, the Netherlands, and the United States, with countries like China and several European nations following suit in the 2000s. The 2010s saw the United Kingdom, Australia, New Zealand, India, Singapore, and Canada initiating their national digital credentialing projects.

These national projects vary in their organizational approaches to developing and operating digital credential systems. A typology of these approaches, focusing on the organizational form and role, is detailed below.[17]

Diagram 1 Organizational Approaches[18]

The various organizations operating digital credential systems on a national level can be categorized into four main forms:

- Government agencies
- Independent non-profit organizations
- Associations of higher education institutions
- Individual higher education institutions without centralized oversight

The role these organizations serve is to either (a) develop and operate the digital credential system or (b) select vendors for the digital credential system and oversee its development by the vendor. Some organizations have blended these responsibilities, such as the 'Hybrid Approach' described below.

The exemplar projects employing these organizational (as seen in Diagram 1) can be grouped into the following approaches:

[17] The research into the different organizational approaches is included in this paper with permission by K. Nakasaki and results from a presentation delivered at GDN Groningen in 2022.
[18] This image is credited to K. Nakasaki.

State-owned Organizational Approach: Countries like China, India, Finland, Norway, and France have seen state-owned organizations develop and internally manage digital credential systems, achieving comprehensive digitization across higher education institutions.

Independent Non-profit Organizational Approach: Sweden and the Netherlands, where independent non-profits have developed and managed the systems, successfully digitizing credentials for all higher education institutions within their borders.

Hybrid Approach: The United Kingdom, the United States, and Singapore have combined in-house development with competitive vendor selection, leading to significant digitization achievements within their higher education sectors. In the UK and the US, an independent non-profit organization centrally manages a verification service for the use of recipients (employers and others), while issuing digital credentials is left to each institution's vendor selection. In Singapore, a consortium has implemented a Blockchain-based credential for all higher education institutions with a commercial IT firm, while each institution independently takes some initiatives.

Association-led Approach: In Australia, New Zealand, and Canada, associations of universities or registrars have led vendor selection and management, promoting extensive digitization efforts on behalf of all higher education institutions within their borders.

Individual Institutional Approach: South Korea and Japan exemplify where each institution independently selects and manages vendors, with varying degrees of digitization success.

Technology Options and Trends

This section offers a technology guide aimed at supporting the planning of new projects or the evaluation of existing services within digital credentialing. This guide does not delve into specialized technologies but rather divides digital credentialing technology into four key components for a comprehensive overview beneficial to policymakers and institutional management. These components are Architecture, User Experience, Document/Credential Type, and Interoperability. Each of these components have various potential options, each with their own advantages and disadvantages.

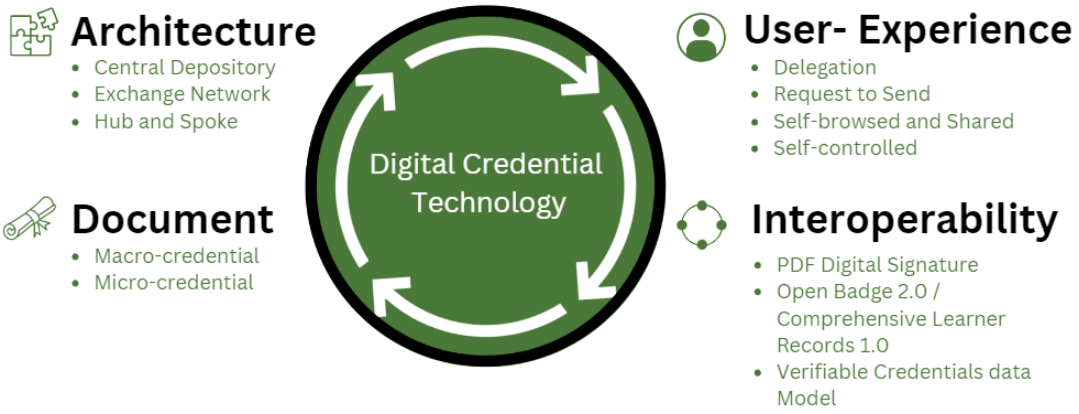

Diagram 2 Digital Credentialing Technology – Components

Architecture

This area outlines the design concept of the entire system, featuring three technological options.

Central Repository

Central Repository is the system architecture in which all student data is stored in a central data warehouse. Countries that have been early adopters of national projects tend to adopt this architecture. Some examples are China's CSSD[19] data warehouse, NSC's[20] verification service in the United States, India's NSDL[21] database, and others.

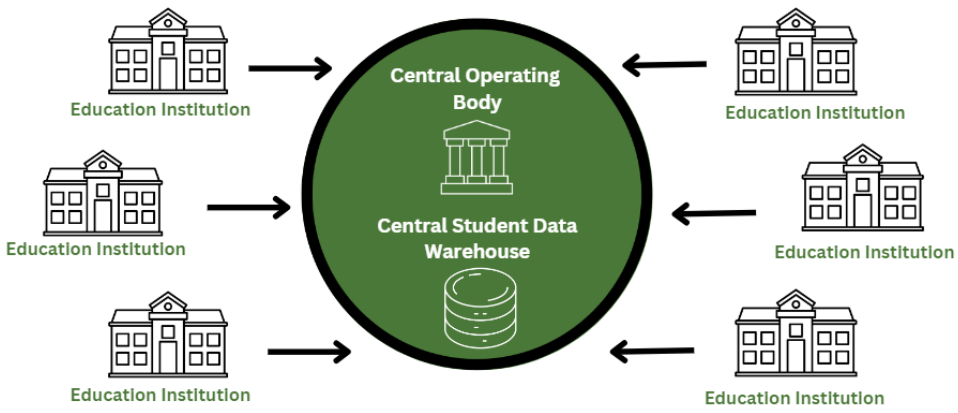

Diagram 3 Architecture – Central Repository

Exchange Network

This model facilitates data exchange among multiple networks and access points, often used for international connections of national central repositories, like EMREX, which links several European countries and China.

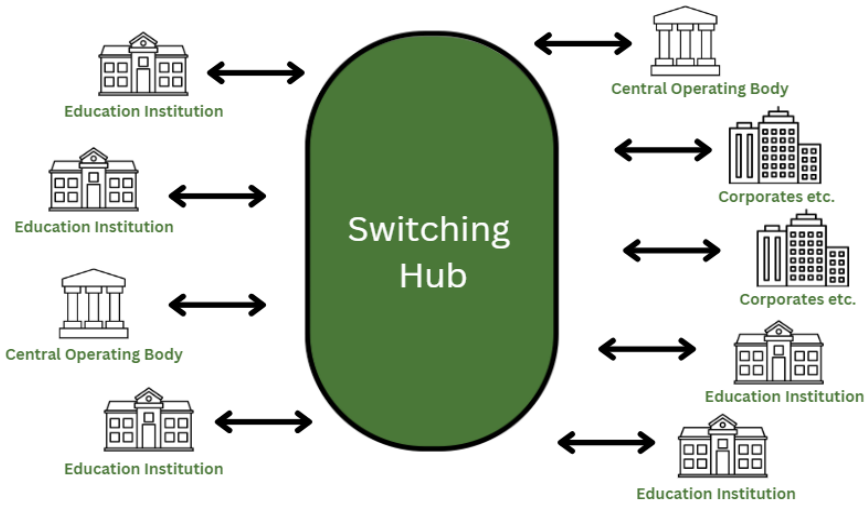

Diagram 4 Architecture – Exchange Network

Hub-and-Spoke

This is a model where a software services platform is shared among institutions, each managing its credential data. This architecture is increasingly adopted by new entrants into the digital credentialing space, including countries like Australia, New Zealand, and Canada.

[19] Center for Student Services and Development

[20] National Student Clearinghouse

[21] National Securities Depository Limited

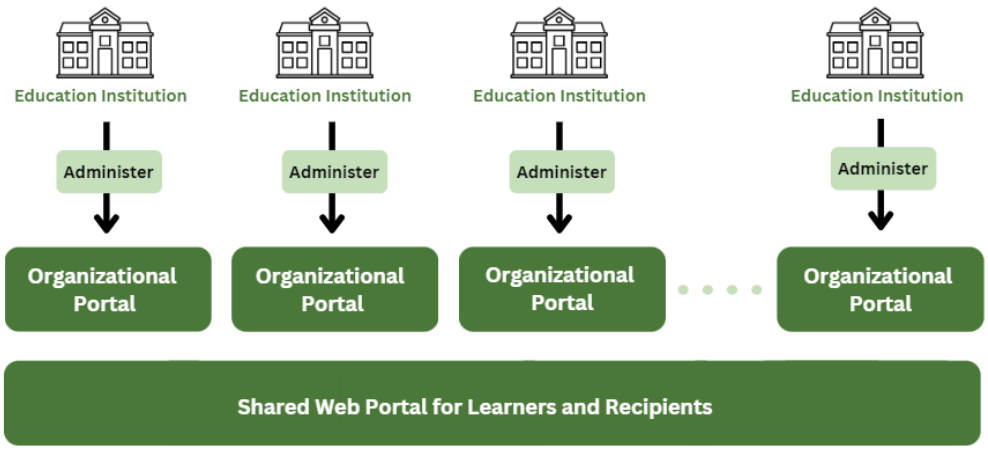

Diagram 5 Architecture – Hub-and-Spoke

User Experience

The second technological component of digital credentialing technology is user experience. In this case, user experience refers to the way in which a learner interacts with the digital credentialing network, including how they can share, view, and request documents.

Delegation

Learners delegate the task of sending their academic records to the managing organization, playing a passive role in the process. This approach is part of the NSC user experience in the USA.

Diagram 6 User Experience - Delegation

Send-Request

Learners actively request the organization managing their academic records to send their credentials to a designated destination, a feature of the EMREX user experience.

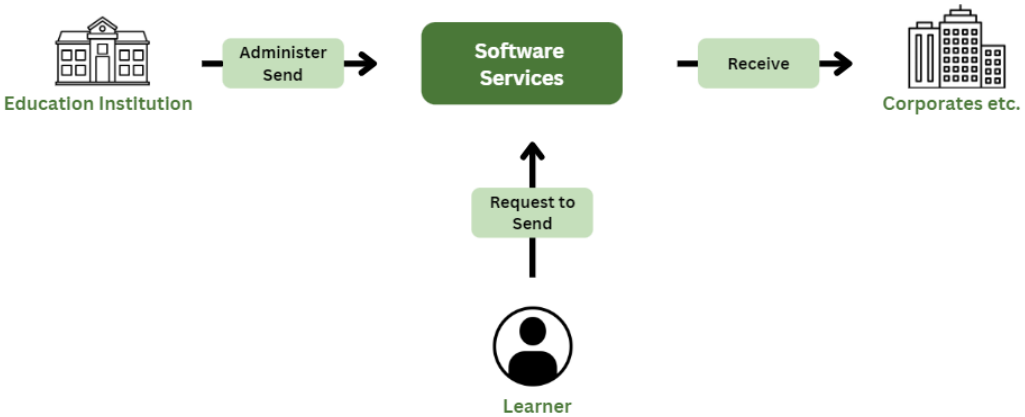

Diagram 7 User Experience – Send-Request

Self-Browsed-and-Shared

This user experience format enables learners to view and share their credentials via browsers, SNS, or email, with recipients able to verify the credentials' authenticity. This model has been implemented in Australia, New Zealand, Canada, and China.

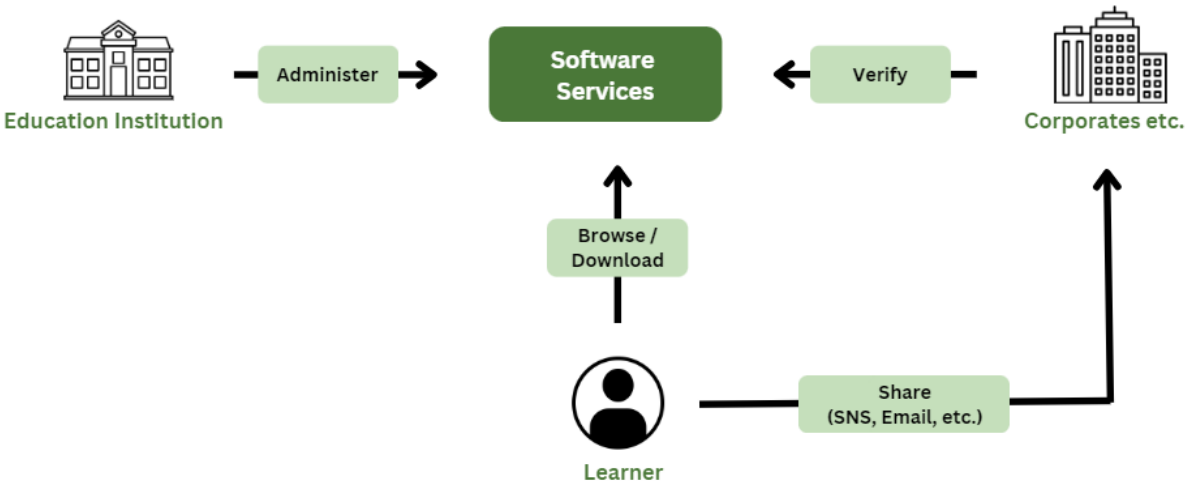

Diagram 8 User Experience – Self-Browsed-and-Shared

Self-Controlled

Self-Controlled is the user experience based on the concept of Self-Sovereign Identity (SSI) of the World Wide Web Consortium (W3C: World Wide Web Consortium). In this user experience, learners (Holders) apply to the issuer of their education data (Issuer) to obtain credentials. Once the Issuer issued the credentials, the Holders can then hold and manage the credentials in their own digital wallets[22] and can share them as needed. The Self-controlled user experience was originally designed as a Blockchain-based technology but today is considered a user experience that can function without the use of Blockchain. Singapore's national project has delivered such a user experience through Accredify's vendor platform; MATTR from New Zealand is also supporting the Canadian MyCreds™ solution in the same manner as it has been integrated into the technology offered by Parchment, an Instructure Company.

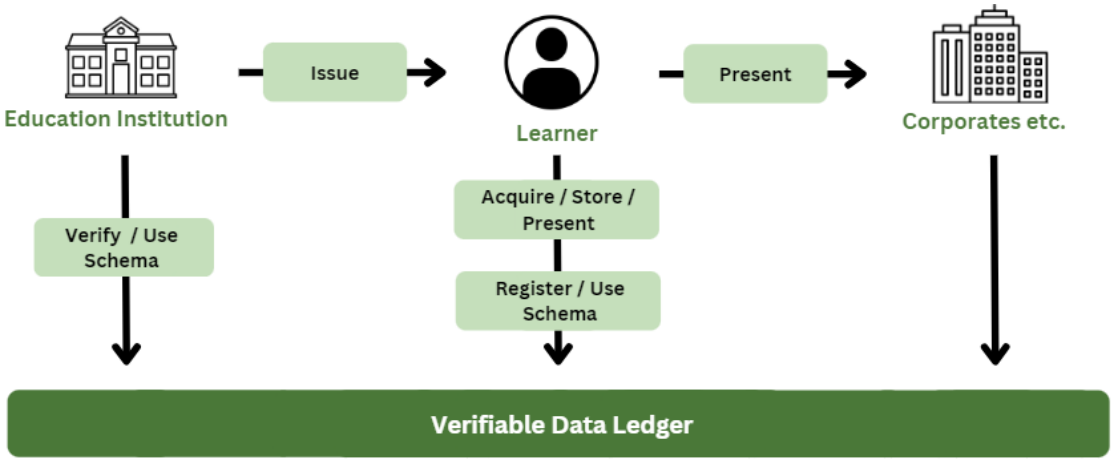

Diagram 9 User Experience – Self-Controlled

[22] An information technology term for a virtual and conceptual place where assets are stored online. In the case of this paper, it is used in the sense of an application on a learner's computer or smartphone that stores personal assets such as learning achievement records.

Document

The third component of digital credentialing technology is the Document itself (or Credential Type). This model suggests simplifying all documents for digital credentialing into the two categories of macro and micro-credentials.

> **Macro-credentials:** Represent traditional degrees issued by accredited institutions, traditionally on paper and now increasingly in digital formats.
>
> **Micro-credentials:** Cover a range of shorter courses and professional training, acknowledging learning achievements that are less extensive than traditional degrees but equally significant.

This simplified terminological structure of digital credentials has the advantage that it is more compatible with inclusive and equitable education and lifelong learning, as called for United Nations' Sustainable Development Goals (SDGs). This model can incorporate inclusive education and lifelong learning, enhancing the integration of non-traditional courses with conventional academic awards.

Interoperability

The earlier discussion on interoperability highlighted the effective use of PDF Digital Signatures, and the trend towards merging fragmented XML data models, Open Badges, and Blockchain credentials (for example) into the Verifiable Credentials Data Model, mapping out the future direction of interoperability within digital credentialing systems. Diagram 10 highlights these trends.

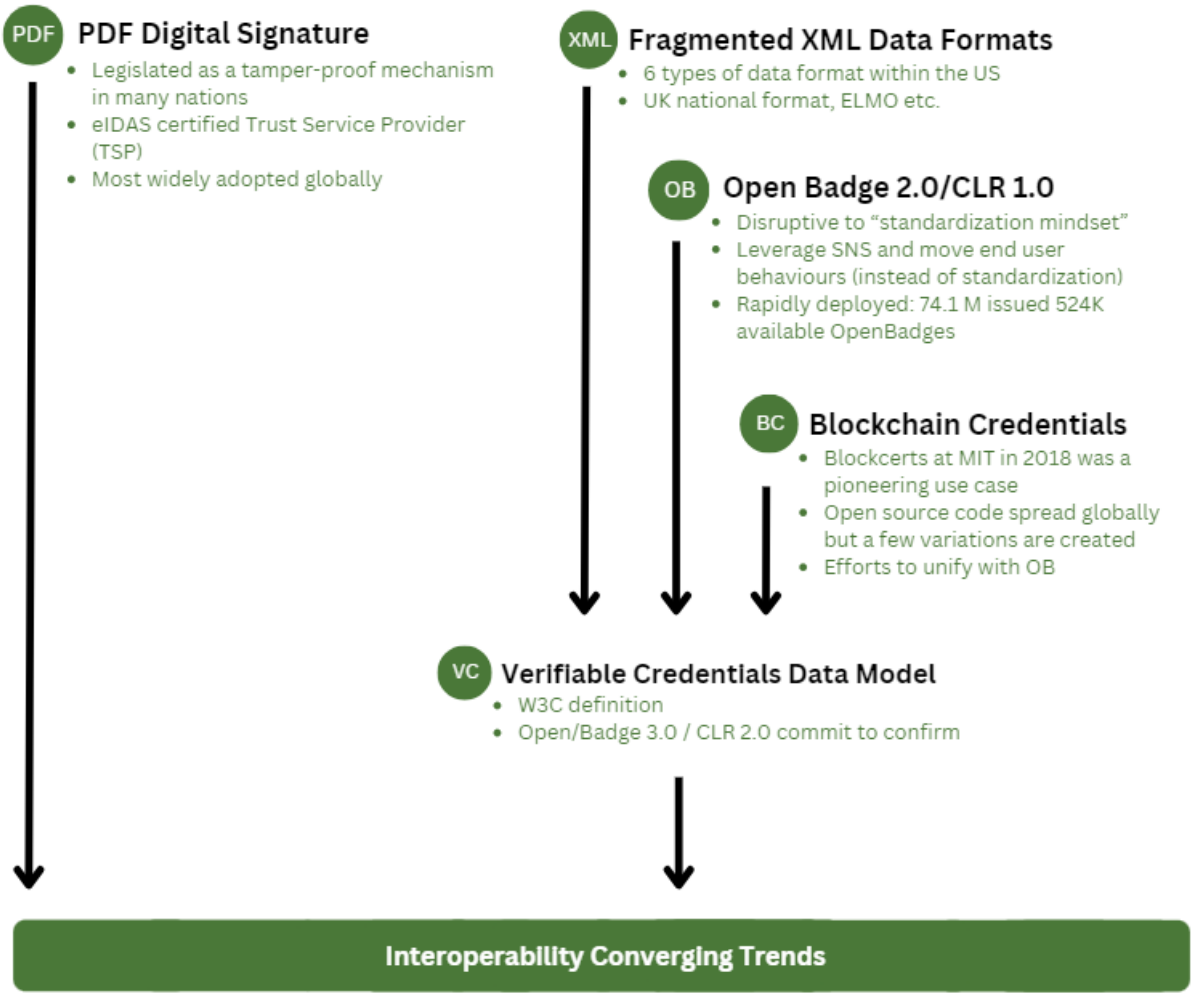

Diagram 10 Interoperability

Appendix 3: The Groningen Declaration Network (GDN): Organizational Outline & Principles

What is the Groningen Declaration Network (The GDN Network)?

The GDN Network is an international, non-profit federated trust located in the Netherlands. It represents a voluntary network of like-minded organizations and individuals that seek to make digital student data portability happen. It is a network of thought leaders from around the globe who are working in concert to support, advise, and offer innovative changes in the ways we share artifacts of academic learning, a focus that is sometimes framed as Digital Student Data Portability (DSDP). The GDN Network seeks common ground in best serving the academic and professional mobility needs of citizens worldwide by bringing together stakeholders in the digital student data ecosystem. It seeks to develop and support best practices and globally accepted standards for safe and citizen-oriented convenings and information exchanges.

The GDN Network represents a group of people that is committed to advancing citizen mobility through the ethical, standards-based digitization of documents and credential data exchange.

Why does The GDN Network exist?

The GDN Network is convinced that the international mobility of students drives economic growth. Mobility also empowers people, enabling them to study, live, and work wherever they want. Students want their competencies recognized, regardless of where they acquired them, and for this, there is a growing need for the acceptance of digital student data instead of the paper-based authentications and academic credentials that exist today.

Document and organizational fraud are increasing at alarming rates. It is critical to advance a quality assured academic credential exchange ecosystem which requires trusted chains of custody for academic documents and data. The GDN Network is convinced that a trusted exchange ecosystem is a critical component of a successful digital ecosystem.

The GDN Network serves as an important enabler and inspiration in the digital ecosystem to advance creation and adoption of trusted, quality assured digital academic credentials and data to ensure rapid access to the labour market and further education.

Trusted Academic Document and Data Portability + Citizen Mobility = Social Mobility

Looking Forward to the Future

The GDN Network has traditionally offered an international convening opportunity as an Annual Meeting in regions around the world which continues into the present day. The following themes sit at the heart of the GDN: building digital capacity across states and countries, providing sustainable technology solutions for digital credential exchange that transform organizational capacity, communications, and services for citizens.

To advance engagement in the digital ecosystem, The GDN Network supports the following priorities:

Knowledge: Enhancing digital fluency as it relates to the digital credential network ecosystem

Standards: Pursuing greater supports for open standards by collaborating with standards bodies

Interoperability and Collaboration: Advancing interoperability and encouraging collaboration between networks to enhance sustainable development goals and supports for mobile learners, including for displaced persons and refugees

Thought Leadership; Contributing to thought leadership through expert advice, research, briefs, presentations, and white papers

Access and Currency: Organizing convening opportunities and expanding GDN participation in other events in a way that achieves diversity and supports capacity building whilst remaining mindful of the GDN Network's sustainability and fiscal context

Research and Application: Identifying, endorsing and stewarding research and special projects that practically advance the overall mission of the GDN

What grounds the approach of the Groningen Declaration ("Declaration")?

The GDN Network mission is guided by a formal Declaration which is a set of digitization principles individuals and organizations endorse through formal signing. By signing the Declaration, individuals and organizations signal their commitment to The GDN Network vision in a manner that admittedly has no binding contractual power, but that signals a shared intention across government, institutions, industry partners, and other organizations committed to citizen mobility.

The Declaration's primary aspirational focus is to ensure commitment to the view that ***citizens worldwide should be able to consult and share their authentic educational data with whomever they want, whenever they want, wherever they are***.

How does The GDN Network achieve its goal today?

The GDN Network brings ideas and people together to accelerate innovative thinking and change through research, thought leadership, curated convenings, support or endorsement of digital innovation initiatives, and inspiring the creation and global convergence of digital student data depositories. It does this work by

- Respecting organizational and government autonomy, authority, and diversity
- Supporting privacy rights including citizen's personal ownership and stewardship of data, identification, and access
- Curating research and special projects that advance the goals of the GDN Network
- Endorsing open standards and best practices that facilitate the forwarding, sharing, and intelligent compatibility and comparability of data
- Enabling quality assured comparability assessment practices and contexts

The GDN Network has been inspired by, and been the inspiration and/or the supporter and endorser of significant initiatives and national level networks that exist for the purpose of exchanging trusted and quality assured academic credentials. It has also been a significant participant in research and activities that have encouraged, defined, and delivered quality assured approaches in the digital education sphere. Examples include helping support the DigiRec project, UNESCO consultations on digitization principles for microcredentials, MyCreds™ in Canada, the Chinese Credential Verification Services (CSSD), My eQuals in

Australia and New Zealand, the National Student Clearinghouse in the United States, DUO in the Netherlands, EMREX, Parchment, an Instructure Company, and many more. Through its work, it has also contributed to important calls for input related to lifelong learning, microcredentials, refugee resettlement, and more.

Creating trust, engaging in collaborative initiatives, and ensuring quality data exchange sit at the heart of The GDN Network.

What types of organizations support The GDN Network mission?

Organizations and individuals that espouse the following principles participate in the aspirational vision of the GDN Network. They tend to be people who are committed to advancing access and digital learning opportunities with consideration for quality assurance and privacy compliance. They work collaboratively across sectors and geographical boundaries to advance these goals through actions and intent.

Declaration Principles

Those who can are welcome to become signatories to the Groningen Declaration as a way to demonstrate formal commitment to democratic principles that support citizens achieving their dreams while respecting local autonomy and authority. By signing, they commit to working together to advance trust, quality assured practices, and social mobility through enabling technology, research, and collaborative opportunities. They communicate a willingness to contribute to and deliver value in the digital space when working with international and national organizations from around the world. They indicate support for creating convergence of ideas in the digital innovation space through participation in convenings, research, initiatives, and other opportunities. They support technology solutions for credential documents and data exchange that put the learner at the centre to ensure evidence informed and learner focused delivery of services and programs. They understand and support the various privacy dimensions in the design and execution of solutions for academic document and data exchange. They express a willingness to work together transparently, with integrity, good fellowship, and respect for diversity. In conclusion, they formally commit to the 12 principles outlined in The GDN Network's Statement of Ethical Principles.

Principle 1: Student Centered
Principle 2: Privacy and Data Protection
Principle 3: Transparency and responsibility
Principle 4: Interoperability
Principle 5: Openness
Principle 6: Freedom to Choose Delivery Options
Principle 7: Integrity
Principle 8: Diversity
Principle 9: Respect for the Law
Principle 10: Auditability
Principle 11: Good Fellowship
Principle 12: Access

We encouraged those who wish to learn more about the GDN Network to visit our website at groningendeclaration.org.