Digital Credentials and Self-Sovereign Identity Workstream

A Report on the Workshop Series for Enabling Interoperabiltity and Mutual Support for Digital Credentials

by International Association for Trusted Blockchain Applications Governmental Advisory Body (INATBA-GAB)

August 2022

Canada

I N
A T
B A

International Association for Trusted Blockchain Applications

Participants

Abu Dhabi Global Market (INATBA GAB Co-Chair)
Financial Services Regulatory Authority, Fintech and Innovation, Brian Yeoh
Nick Green

Accenture
Daniel Bachenheimer (INATBA Identity Working Group Co-Chair)

BOSA
Frank Leyman

Canada (INATBA GAB Chair)
CIO Strategy Council, Tim Bouma
Global Affairs Canada, Aliénor Fagette
Innovation, Science and Economic Development Canada
 Ratib Abeer
 Qussai Abu-Naqoos
 Derek Alton
 Mario Bonito
 Kathleen Fraser
 Paul Jackson
 Jacqueline Jones
 Christopher Majewski
Treasure Board of Canada Secretariat
 Michael Goit
 Pirth Singh

European Commission (INATBA GAB Co-Chair)
DG CNECT
 Joao Rodrigues Frade
 Luben Kabaktchiev
 Caroline Kaeb
 Helen Köpman
 Rapolas Lakavičius
 Pierre Marro
 Hisanobu Ohtsubo
 Jose Manuel Panizo
 Lukas Repa
 Stergios Tsiafoulis

France
European Blockchain Partnership, Perrine de Coetlogon

Georgia
National Agency of Public Registry, Guga Lomidze

Germany
German Federal Ministry for Economic Affairs and Climate Action
 Andreas Hartl
 Alexander Wajnberg
 Stefan Afting
German Federal Ministry of Education and Research, Jan Renz
Hasso Plattner Institute, Alexander Muehle

Hyperledger Aries Cloud Agent-Python
Ian Costanzo

Hyperledger Aries Framework-Go
        Mike Varley
        Troy Ronda

Incrreda
        Ravindra Kumar

Israel
        e-Gov unit, government CIO, Digital Division, Ofer Ishai

Japan
        Cabinet Secretariat
                Tatsuji Narita
                Yoko Ikeda
        Jun Takahashi
        Suzuki Tomoharu
        Japanese Digital Agency
                Nobuyuki Hiratsuka
                Tatsuji Shimoe
                Toshi Zamma

Jolocom
        Kai Wagner (INATBA Identity Working Group Co-Chair, Board Member)

Kenya
        Blockchain and AI Task Force, Bitange Ndemo

Kunfud
        Ismael Arribas

LACChain/IADB-Lab
        Albi Rodriguez Jaramillo

Liechtenstein
        Office for Financial Market Innovation, Clara Billek

Morocco
        Fahd Salek

Poland
        DLT/Blockchain at Ministerstwo Cyfryzacji, Piotr Rutkowski

Slovenia
        European Blockchain Partnership, Nena Dokuzov

South Africa
        Department of Communication and Digital Technologies, Nokubalela Mchunu

Spain
        European Blockchain Partnership, Pedro Martin Jurado

Stephan Arenz

Vrije Universiteit Brussel
        Andrés Chomczyk

INATBA Secretariat
        Bara Greplova
        Hassan Abou Jawhar
        Xenofon Kontouris
        Ricardo Simões
        Marc Taverner

Table of contents

Disclaimer: *This report does not necessarily represent the opinion or position of all the members of the Governmental Advisory Body. Additionally, the professional affiliation of some members might have changed since the writing of this report.*

Executive Summary

In recent years, world economies have undergone significant changes fueled by disruptive technologies, significantly changing the way that consumers, industries, or businesses operate. More recently this shift to digital has been accelerated due to individuals and organizations facing significant challenges in obtaining and delivering services. In-person services centres were either closed or operating well below capacity, and paper-based documents, such as university transcripts, were not being received in a timely manner due to processing, printing and delivery services operating well below capacity. Consumer consumption rapidly moved online and teleworking became the norm, forcing organizations to adapt.

Transactions in the global economy and society rely upon trust, where each transacting party is confident that the other is who they claim to be, and that the information provided is true. How to ensure this trust in a digital world has become an increasingly important problem faced by governments and organizations around the globe, with massive implications on the health and vitality of the global economy.

To help address this challenge, the Digital Credentials and Self-Sovereign Identity workstream of the INATBA Governmental Advisory Body was convened by Canada. The focus was on leading a series of workshops to examine the technology and policy landscapes for digital credentials of INATBA-GAB members, identify the commonalities and gaps, and then develop recommendations for enabling interoperability and mutual support for digital credentials across borders

The workshops highlighted that there was a good understanding of the digital credentials model, with an acknowledgement that INATBA-GAB members are at varying stages of readiness regarding digital credentials. There still exist technical challenges caused by diverse but fragmented technology and policy landscapes. It was also highlighted that cross-jurisdictional and cross-sectoral discussions with common use cases and specific problems to address will be key to breaking down silos and enabling common baselines and broad interoperability. Furthermore, experts focused on how to support SSI and digital credentials within their existing policy frameworks, while exploring how to address the area of standardization of digital credentials and digital trust services.

The following are the recommendations for advancing interoperability and mutual support for digital credentials globally:

1. **INATBA Task Force for enabling mutual support and interoperability for digital credentials across borders**

    The Task Force is to be guided by principles that facilitate interoperability and mutual support across borders; guarantee privacy and security of individuals and businesses; enable individuals and

businesses to hold and control their information (self-sovereignty); allow individuals and businesses to use the digital wallet of their choice and port their digital credentials from one wallet to another.

2. Playbook to provide a crash course on digital credentials

The goal of the playbook would be to provide a crash course on digital credentials to help those that are less experienced with digital credentials to catch up with those who are at a more advanced level. It is recommended that this playbook be developed by the INATBA Digital Credentials Task Force.

3. Joint demonstrations/showcases for digital credentials

Joint demonstrations/showcases are to show how digital credentials can solve real-world problems and how end users, businesses and governments could benefit. It will help build awareness and adoption for digital credential use cases. It will also help other jurisdictions with exploring, testing and implementing digital credentials. It is recommended that the INATBA Digital Credentials Task Force develop recommendations for how to undertake these joint demonstrations/showcases.

4. International coordination on digital credentials standards and certifications

It is recommended that the INATBA Digital Credentials Task Force develop recommendations for enabling international coordination, including what role INATBA-GAB, INATBA working groups and other international standardization and certification bodies should play in enabling international digital credential standards and certifications.

Background

Trust is key in digital global economy. Governments and other organizations are trusted anchors, enabling trust by issuing documents needed for transactions across economies and societies—such as individual and organization identities, licences, permits, certifications, and educational qualifications. These documents in turn serve as the foundation on which everyday services and transactions depend. However, these services and transactions often rely on costly and time-consuming in-person and paper-based processes, such as manually inputting information, uploading documents, and mail-based and in-person verifications—even when they're done "online". It remains a challenge to provide documents that are easy to use in digital transactions across economies and societies, while preventing fraud and avoiding costly and time-consuming processes.

Governments and other organizations can accelerate the shift to digital by making these documents easy to use in digital transactions while preventing fraud and avoiding costly and time-consuming processes. They can support this trust in digital transactions by providing trusted digital versions of these documents as digital credentials. Digital credentials are portable digital records about an organization, individual or thing that can be held and shared through a portable and secure digital repository known as a digital wallet. They are digital representations of traditionally physical certificates or information such as personal identification, proof of payment (e.g. plane ticket), certificate of incorporation, or a university degree. Digital credentials can be trusted by all entities in the economy and society as they rely upon cryptography to detect fraud and verify the authenticity and the issuer of the digital credential.

International Association for Trusted Blockchain Applications (INATBA)

Governments around the world are taking action to update the technologies and infrastructure they used to support the shift to digital. Many are reviewing and modernizing privacy, trust and data legislation. One of which is the International Association for Trusted Blockchain Applications (INATBA). A global convener of the blockchain ecosystem offering developers, companies, and users of blockchain/distributed ledger technology a forum to interact with regulators and policymakers and bring blockchain technology to its next stage. INATBA has established two advisory bodies as well as six working groups to bring together thought leaders from diverse backgrounds for meaningful conversation, networking, collaborative projects and to produce outputs with an impact.

INATBA-GAB Digital Credentials and Self-Sovereign Identity (SSI) Workstream

The objective of this workstream was to examine the technology and policy landscapes for digital credentials of INATBA-Governmental Advisory Body (GAB) members, identify the commonalities and gaps, and then develop recommendations for enabling interoperability and mutual support for digital credentials across borders. This workstream was convened by Innovation, Science and Economic Development Canada, and consisted of a series of technical and policy workshops that were held from summer 2021 to summer 2022. This report summarizes the results from these workshops, including the findings and recommendations.

Workshop Series

The workshop series brought together two technical and policy experts to explore how to enable interoperability and mutual support for digital credentials and digital trust services across borders. They first focused on identifying and exploring the digital credential commonalities, gaps and challenges across INATBA-GAB members, and then used these findings to develop recommendations for enabling interoperability and mutual support across borders. The process used for the workshop series is as follows:

Workshops (Establish Key Topics):

- Technical #1
- Policy #1
- Technical #2
- Summary

INATBA-GAB & Working Groups (Dialogue):

- INATBA-GAB and government dialogue
- Working groups

Report:

- Draft report
- Consult
- Finalize

See Figure 1 for a visual representation of the process that was used throughout the workshop series.
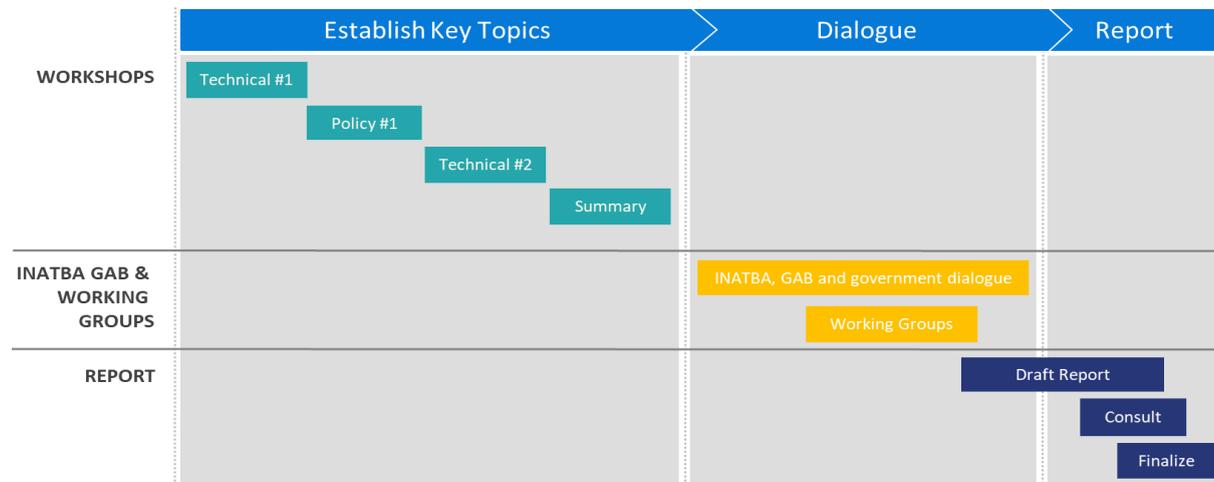

Figure 1: Visual representation of the process used throughout the workshop series

Technical Workshops

The focus of these workshops was on how to enable technical interoperability and mutual support across jurisdictions for current and future SSI and digital credential implementations (e.g. mapping technical architectures and solutions used by each INATBA-GAB member). Specifically, the workshops were focused on developing recommendations for how to address the technology gaps and challenges to enabling interoperability and mutual support across borders.

Commonalities

Dialogue amongst INATBA-GAB members highlighted that there was a good understanding of the digital credentials model, with an acknowledgment that many INATBA-GAB members are at varying stages of readiness regarding digital credentials. Though many jurisdictions have some technology in common, there was a recognition that there are still technical challenges caused by diverse but fragmented technology approaches (multiple non-interoperable ledgers, issuing/verifying services and wallets). It was agreed that enabling interoperability between these various technologies was important and that it would be more effective to frame the discussion with common use cases, with specific problems to address, rather than having an abstract discussion about how to get technologies to work together. It was also agreed that they currently lack a clear path for enabling interoperability across the technology approaches, with many of the existing efforts being done in silos, so cross-jurisdictional and cross-sectoral discussions will be key to breaking down these silos and enabling broad interoperability.

Gaps and Challenges

Technology challenges exist within and across jurisdictions, which are largely caused by diverse and fragmented technology approaches (e.g. multiple non-interoperable ledgers, issuing/verifying services and wallets), and this is further complicated by inconsistent approaches and definitions regarding formats, requirements, protocols and signatures. INATBA-GAB members also identified that there is a lack of a common baseline on which to build interoperability, and insufficient coordination between international approaches to develop standards and certification schemes, with many of the existing efforts being done in silos.

More advanced members are proceeding more rapidly on technical implementations, but less advanced members are struggling to keep up and to take the initial steps. In addition, different SSI and digital credential technologies and approaches are emerging in different jurisdictions, which could create challenges for jurisdictions to know which SSI and digital credential technologies to trust. This is particularly relevant to international travel and trade, where jurisdictions could encounter foreign individuals and businesses who are using the SSI and digital credential technologies from their respective jurisdictions. Since it isn't feasible for jurisdictions to certify each SSI and digital credential

technology in use worldwide, nor to reject all foreign technologies, it will be important for there to be greater alignment and coordination across jurisdictions on standards and certifications.

Policy Workshops

The focus of these workshops was on how to enable interoperability and mutual support across jurisdictions, from a policy perspective, for the issuance, verification and use of digital credentials. Moreover, the experts focused on how to support SSI and digital credentials within their existing policy frameworks, while exploring how to address the area of standardization of digital credentials and digital trust services.

Commonalities

There are many commonalities across INATBA-GAB members from a policy perspective. Unanimously, members were in agreement on the role of the government as a trust anchor for identity and digital trust in general. Further, data protection, privacy and consent were key considerations for all members. To support this, common approaches and issuer capabilities will be needed to ensure that privacy requirements are met.

Members are highly motivated and well-educated in digital trust technologies, have shared values in implementation and many have trust frameworks for digital identity.

Gaps and Challenges

There are common policy gaps and challenges that each of the jurisdictions is facing. For example, there is a lack of standards when it comes to digital wallets. Standards are currently being developed by different jurisdictions, but there is a lack of coordination between these initiatives, which could cause significant challenges in aligning the approaches. There are also different levels of advancement in technology and policy frameworks amongst different jurisdictions, which could result in challenges in enabling alignment and mutual recognition across jurisdictions of digital credentials and related technologies. It was acknowledged that even though there exists an alignment between the policy/regulatory frameworks of some members, there were other members where there is not that alignment.

Recommendations

This workshop series has paved the way for future collaboration and cross-pollination in the field of digital credentials and digital trust services by emphasizing the need to address challenges and provide solutions on multiple fronts. For instance, it highlighted the importance of addressing the lack of guidance/standards, in particular for digital wallets, which if not addressed, could force users to have to juggle many different wallets to do transactions in different sectors and jurisdictions. It also highlighted the different levels of readiness amongst INATBA-GAB members regarding digital credentials, which if not addressed, could make it more difficult to collaborate with one another and ultimately enable mutual support and interoperability for digital credentials.

The following are the recommendations for advancing interoperability and mutual support for digital credentials globally:

1. **INATBA Task Force for enabling mutual support and interoperability for digital credentials across borders**

   To allow for ongoing regular dialogue and collaboration; inform implementation across jurisdictions; and identify and address remaining gaps and challenges regarding interoperability and mutual support, it is recommended that a Task Force is established. The Task Force is to be guided by principles that facilitate interoperability and mutual support across borders; guarantee privacy and security of individuals and businesses; enable individuals and businesses to hold and control their information (self-sovereignty); and allow individuals and businesses to use the digital wallet of their choice and port their digital credentials from one wallet to another. As a part of that work, the Task Force would build upon the findings and recommendations presented in this report by:

   - Further exploring the gaps, challenges, commonalities and potential areas of collaboration for enabling mutual support and interoperability for digital credentials across borders.

   - Developing detailed recommendations for enabling mutual support and interoperability for digital credentials across borders, including building upon the recommendations included in this report.

   - Implementing select recommendations for enabling the mutual support and interoperability for digital credentials across borders, as permitted by the scope and timelines of the Task Force, such as developing the playbook that is recommended by this report.

2. Playbook to provide a crash course on digital credentials

INATBA-GAB members are at various levels of readiness when it comes to exploring, testing and implementing digital credentials. Some members are at an advanced level, where they are actively implementing and using digital credentials, while others are early in the exploration stage. It can be challenging for INATBA-GAB members to collaborate with one another on digital credential initiatives when there are significant differences in the level of readiness, as the less advanced members would likely struggle to take the initial steps and keep up with the more advanced members. The goal of the playbook would be to provide a crash course on digital credentials to help those that are less experienced with digital credentials to catch up with those who are at a more advanced level. It is recommended that this playbook be developed by the INATBA Digital Credentials Task Force.

3. Joint demonstrations/showcases for digital credentials

To help build awareness and adoption of digital credentials, it is recommended that joint demonstrations/showcases be undertaken for concrete digital credentials use cases. It is important to show how the digital credentials model can solve real-world problems and how end users, businesses and governments could benefit. Where possible, these demonstrations/showcases should be undertaken jointly by multiple jurisdictions to build awareness across borders and to better enable international use cases. This will not only build awareness and adoption for digital credential use cases, but will also help other jurisdictions with exploring, testing and implementing digital credentials. It will further create opportunities for additional cross-border use cases, which could ultimately help to advance mutual support and interoperability for digital credentials across borders. It is recommended that the INATBA Digital Credentials Task Force develops recommendations for how to undertake these joint demonstrations/showcases, in particular demonstrating/showcasing international use cases.

4. International coordination on digital credential standards and certifications

To avoid sectoral and jurisdictional silos, it is recommended that there be international coordination on digital credential standards and certifications. There are currently multiple independent efforts underway to develop digital credential standards and certifications, but there is insufficient coordination and alignment between these efforts. Without sufficient coordination and alignment, there could be the risk that the digital credentials and digital wallets in use in one jurisdiction or sector, would not be supported in another jurisdiction or sector. This

would create significant challenges for international use cases, such as international travel and trade.

It is recommended that the INATBA Digital Credentials Task Force develops recommendations for enabling international coordination, including what role INATBA-GAB, INATBA working groups and other international standardization and certification bodies should play in enabling international digital credential standards and certifications. These recommendations should also identify opportunities for INATBA-GAB members to coordinate on digital credential standards and certifications within each of their jurisdictions (e.g. Canada's work on developing a National Technical Specification for Digital Credentials and Digital Trust Services and the European Union's work on digital identity wallets for eIDAS 2.0).

Contact details: