Perseid E-ID Vision Document

JUNE 2021

ABSTRACT

When e-ID’s are used in conjunction with a well-conceived regulatory framework and paired with a best-in-class technology solution for global interoperability, these e-ID’s could create a digital identity bridge across residents of Bermuda. This is as it provides the ability for individuals, businesses and governments to send and receive relevant and required information and in so doing creating a trust fabric within Bermuda. Therefore, an opportunity has arisen to implement a e-ID platform which will be used for online and offline personal identification and authentication and eventually many more applications.

Glossary

Term	**Description**
Users	Users are citizens or small and medium enterprises that wish to access or use a given service.
Service providers	Service providers deliver the service after delegating user identity verification to the identity provider.
Identity providers	Identity providers authenticate users or verify the information requested according to the level of trust required. Identity verification covers several operations performed jointly or separately, such as identity registration, authentication, and the verification of certain data, attributes or documents (credentials). In some cases, these operations may be managed with (or possibly delegated to) providers of data or secure documents.
Attribute providers	Attribute providers may be public or private, and general or specializing in a type of data, for example proof of address or revenue.
Secure document issuers	Secure document issuers generally issue documents in the public sphere. Their role is sometimes combined with that of identity provider.
Registration authority	Registration authorities are involved (in the case of PKI) in distributing databases and providing an unambiguous link between a given public key and the user.
Certificate authority	Certificate authorities (in the case of PKI) control the issue, management (suspension for example) and withdrawal of digital certificates.
Federation services	In this case, federation services refer to several types of interoperability network, infrastructure, perimeters or rules that create conditions conducive to identity management.

Table of Contents

Introduction

An opportunity has arisen within the island of Bermuda to implement a e-ID platform which will be used for online and offline personal identification or authentication. These e-ID's could create a digital identity bridge across residents of Bermuda as it provides the ability for individuals, businesses and governments to send and receive relevant and required information and in so doing creating a trust fabric within Bermuda.

When these e-ID's are used in conjunction with a well-conceived regulatory framework (for usage of enhanced e-ID's) and paired with a best-in-class technology solution for global interoperability, the result would be Bermuda e-ID's being accepted in other jurisdictions as a valid ID. This is referred to as "jurisdiction as a service".

Purpose

This initiative is aimed at creating a digital identity bridge across residents of Bermuda and therefore the main focus areas will be the following:

- Integrating local public and private partners into a basic access and credentials network
- Initial on-boarding new local users
- Issued a duration and rights managed usable form of e-ID to international visitors to the island
- Remote application and issuing of the Bermudian e-ID to qualifying individuals world-wide

During the implementation of the e-ID project consideration will be given to the different partners, technology and global interoperability; the result would be Bermuda e-ID's being accepted in other jurisdictions as a valid ID.

The aim of this document is to provide an understanding of the proposed project background, opportunities and implementation thereof within Bermuda and the impacts this e-ID platform would have on government, business, residents and eventually any visitors which enter the island.

Background

Opportunity Statement

The vision of this initiative is as follows: Build a phased, highly scalable and compliant identity program to such a high standard, that other countries and businesses globally would recognize and honor the Bermuda e-ID in their own jurisdictions as a truly interoperable and shareable proof of their identity. This can be done by ensuring the seamless integration of a consent framework, successful querying of stores of data and the encrypted return of data and documentation to the authorized parties.

History

Global ICT Trends

Globally, rapid advancements in ICT (Information and Communication Technologies) have resulted in a paradigm shift in the way governments across the globe conduct business with its citizens. This shift in counterparty communication and information distribution lends itself to backwards compatible services within the government realm.

There has also been a steady increase in the need for robust and scalable KYC/AML/ATF (Know Your Customer / Anti-Money Laundering / Anti-Terrorist Financing) options for businesses and governments operating around the globe. This need therefore encourages a platform which will provide common trust between the parties using it.

This digital revolution is impacting all sectors of society. The most visible change is the growing multi-channel access to online services, whether via the internet or mobile applications. As our lives shift towards the digital space, most countries are finding it important to maintain continuity in the way society is organized, improve economic circuits and mechanisms, and develop services to citizens.

For all **citizens**; managing health, organizing children's education, taking out a loan (or investing savings), signing a rental contract or exercising civil rights are significant acts of responsibility. These acts that can be managed in the digital space, as long as this can be done with confidence and peace of mind with regard to their validity and security.

For **companies** (large or small); their role as economic stakeholders, together with their corresponding legal liability for the scope of their business, means they need to make sure their new digitally-acquired agility remains securely rooted. This is so they can improve customer service while safeguarding contractual commitments.

For **public administrations**; the challenge of greater flexibility in public services thanks to the "all-digital" transition and the requirement to better understand user needs are combined together. The task is on government services to be reliable, all the more so as governments must act as guarantors in their sovereign task of preserving public interests and safety of people and property.

This view, shared for some years now by an increasing number of countries, has the advantage of promoting the conditions for digital development centered on people and their changing usage habits, based on two pillars: **trust services** and, above all, **digital identity**.

Improving the deployment of trust services

To enable public administrations, companies and citizens to freely interact while retaining their formal relationships of liability, there needs to be a progressive development in the use of "digital trust" services. Such services make it possible to link decisions and acts of management to those enacting them. Thereby, granting them certain legal validity, and to conserve the elements exchanged by the parties securely.

To this end, regulatory authorities are making great efforts to harmonize such services and promote their legal value. One example is that of the European Union, which recently introduced a regulation on electronic identification and trust services.

In practical terms for citizens, this might mean, having access to the confidential health data shared with a doctor before a medical operation, or being able to transfer money to a third party while complying with declaration obligations. For companies; especially very small, small and medium enterprises; it represents an opportunity for improved management of social and fiscal obligations, as well as improved management of sensitive processes such as supplier purchases and financial transactions.

For trust to be established, both parties must be linked via a secure, unbroken chain. The capacity to demonstrate that you are who you say you are (authentication) is a strategic imperative. An additional step is identity. Identity is in essence the link that connects an individual and the community. Protecting identities against fraud or theft is key to maintaining confidence. The greatest challenge is ensuring that a digital identity matches a real identity, i.e. ensuring that it is authentic and unique. Establishing a digital identify and providing secure access to services can be carried out using a twofold authentication and identification process and in so doing complete the verification of a person’s identity.

The role and responsibilities of governments

The role of governments is fundamental as state entities have both a right and a duty to exercise their sovereignty by virtue of and in compliance with international law and their own constitution. It is therefore logical to assume that this sovereignty shall be exercised consistently across the digital sphere and the physical territory of the nation. Identity is one of the basic attributes of this state sovereignty, responding to the state's role in terms of justice and citizen rights, the organization of civil life and social contract, or even defense and security.

As a result, governments today, just as they did in the past when issuing or regulating "sovereign identities", must provide or approve digital identity solutions in response to the challenges of efficiency and modernization, as well as the longer-term challenges faced by states as part of the digital transformation of civil society.

Short- and medium-term governmental challenges include:

- Providing a high-quality public administration system for citizens and companies. This will include user-friendly public services that are more reliable and more agile thanks to the deployment of identities, making state services more accessible.
- Developing the usage of digital trust services, with more transparent, reliable and structured digital exchanges, and greater technical and legal security for very small, small and medium enterprises, and consumers.
- Enabling greater integration with private sector services.
- Improving data protection and modes of consent in transactions or contracts in the digital space.

The challenges of sovereignty

These digital challenges flow into the core challenges of state sovereignty: the organization of society, economic development and social cohesion.

These long-term challenges can be described briefly as follows, with emphasis on their strategic importance:

- Trusted Digital Identity is at the heart of the digital economy, but also at the heart of societal transformation. Key sectors like healthcare, education, social protection and welfare, as well as simple civil security, can benefit from this.
- Promoting economic development and healthy, sustainable growth. By encouraging high-value usage, digital infrastructure will be used more effectively by the public and private sectors, and the whole economy becomes more productive.
- Upholding values such as the protection of fundamental rights; integration and the social bond; economic, cultural and linguistic influence; and interoperability with other states.

The role of governments therefore, with regard to identity is not restricted to that of issuer, regulator or security operator, but is of strategic importance for the development, reach and influence of each nation. It starts with the digital transformation of administration services, continues with the introduction of trust services that benefit the economy and society as a whole, and persists over the longer term with efforts to harmonize sovereignty between the physical and digital spaces.

Legislative Influence

In Bermuda, 1999 saw the introduction of the ETA (Electronic Transactions Act 1999), which set out the acceptance of digital signatures within the Internet era as a tool to reduce time and cost of doing business in Bermuda. This however, was undermined by the increased scrutiny of business and service providers within the financial industry and there was a move back to tried and tested “wet signatures” as a proof of collection and validation of customers.

“Wet signatures” and the physical information attached to an individual's identity have major downfalls namely: sharing is not efficient, updatable or cost effective; no mode of sharing updates, risk profiles or findings; duplication of on-boarding documents for business executives and citizens and; duplication in the time, energy and cost of validation/verification of these individuals.

The ETA 1999 does however, provide an effective foundation within Bermuda in conjunction with the recently enacted PIPA (Personal Information Protection Act 2016) legislation around data privacy. This legislative groundwork and other legislation implemented around the globe (Example: The GDPR (General Data Protection Regulation) laws of the European Union (EU)) provide a unique opportunity to develop a comprehensive regulatory solution for the Island and in so doing: the ability to leapfrog many jurisdictions.

In December 2014, Estonia became the first nation to open its digital borders to enable anyone, anywhere in the world to apply to become an e-Resident. Estonian e-Residency is essentially a commercial initiative. The e-ID issued to Estonian e-Residents enables commercial activities with the public and private sectors. It does not provide citizenship in its traditional sense, and the e-ID provided to e-Residents is not a travel document. However, in many ways it is an international ‘passport’ to the virtual world. E-Residency is a profound change and the recent announcement that the Estonian government is now partnering with Bitnation to offer a public notary service to Estonian e-Residents based on blockchain technology is of significance. The application of blockchain to e-Residency has the potential to fundamentally change the way identity information is controlled and authenticated.

India has also made a move towards digitizing their nation by giving political and economic rights to citizens through the use of ID cards (utilizing the system Aadhaar) where the users thereof have a digital identity. This enables Indian citizens to be able to complete transactions without physical identification and physical currency with the benefit of less corruption and black money. There however, have been many issues with the use of the Aadhaar system as initially it was centralized and therefore had issues with security, it also only utilizes biometrics with registration and does not have a full authentication model. It also only has a card number and does not have a chip and therefore still has more manual aspects of updating, authentication and authorization.

Other countries which are also looking at implementing some use of digital identity are: Mauritius, Canada, Australia, France, Dubai, Singapore as well as the United States of America. Dubai is looking at creating a self-sovereign ID/Passport to improve security at airports as well as make land registry more efficient. Singapore is hoping to implement a mobile friendly “cashless” system where two step verification is used. The State of Illinois wants to implement secure ID cards with increased efficiency and usability in their medical programs and institutions.

More reference material can be accessed by clicking the below links:

EU E-ID Scheme

http://eur-lex.europa.eu/legal-content/en/ALL/?uri=CELEX:52008DC0798

EU Technical Interoperability Architecture

https://ec.europa.eu/cefdigital/wiki/display/CEFDIGITAL/eIDAS+Profile?preview=/46992719/47190130/eidas_interoperability_architecture_v1.00.pdf

Bermuda Electronic Transactions Act 1999 (Digital Signatures)

http://www.bermudalaws.bm/laws/Consolidated%20Laws/Electronic%20Transactions%20Act%201999.pdf

EID

E-ID Description

The e-ID proposed is an electronic identification document (card) which will be used for online and offline personal identification or authentication. The cards will be damage proof and would have multiple security features within the actual card, but also would extend into an application or Phone based ID that would have enhanced capabilities of data protection, customized provision of data and ability to revoke data as per the GDPR.

Therefore, these will be the ways to utilize the e-ID and its functionality:

- Smart Card with multi factor authentication (Biometrics)
- App based ID with multi factor authentication (Biometrics)

Possible usage of the e-ID includes (but is not limited to) the following examples:

- Bank account opening
- e-Signature of Documents
- Voting
- Fast track Immigration inbound to Bermuda
- Driver's License
- Health ID
-

These e-ID's could therefore create a digital identity bridge across residents of Bermuda as it provides the ability for individuals, businesses and governments to send and receive relevant and required information and in so doing creating a trust fabric within Bermuda.

The e-ID platform and the affiliated digital identities will have three primary actioning points:

1. Claims (Identity claim made by the person, business, or jurisdictional entity)
2. Proofs (Evidence such as a document that provides evidence for the claim. This can come in all forms: Driver's license, passport, birth certificate, utility bills.
3. Attestation (Third party validation of the claim/proof)

Bermuda is in a perfect position to host the visualized e-ID platform as it boasts the following competitive advantages:

- Reduces cost and increases ease for identity related requirements for all Bermuda residents and citizens, as well as businesses and government
- Provides highest levels of "gatekeeping" for the jurisdiction for crypto business by establishing a clear set of world class AML/KYC rules
- Harmonized fully within the toughest global data privacy requirements including PIPA and GDPR
- Significantly increases speed of verification for financial services – as well as all other local companies operating under KYC / AML
- Fast track immigration for Bermuda locals
- Jurisdiction as a service (JDaaS) to leverage and grow the Bermuda economy

When these e-ID’s are used in conjunction with a well-conceived regulatory framework (for usage of enhanced e-ID’s) and paired with a best-in-class technology solution for global interoperability, the result would be Bermuda e-ID’s being accepted in other jurisdictions as a valid ID. This is referred to as “jurisdiction as a service”.

E-ID Benefits

The primary benefit within Bermuda would be that users (customers) of financial institutions and other regulators would not have to produce numerous certified copies of passports, driver’s licenses or utility bills to open or maintain relationships. They would be able to simply authorize the institutions request for identity confirmation and/or sending of encrypted documentation if required.

The “e-ID platform” would therefore have the critical customer data always up-to-date, securely accessible and permissioned by the customer for safety. Over time more documents and trusted entities would be integrated into the e-ID network to provide other efficiency gaining services such as medical health access, fast track immigration at the airport and ultimately voting capabilities.

For international businesses on the island, this e-ID scheme would provide for remote signatures for directors and officers of the companies to execute agreements and vote on matters. Remote governance for organizations would be a lucrative and attractive value proposition.

Further, the ability to provide validation for a legitimate and respected businessperson, who happens to carry a passport from certain high-risk country, which would normally cause problems or delays; could efficiently do business in jurisdictions around the world. This in turn would give recognition to the Bermuda e-ID as being a gold standard of ID and would provide more value than the actual passport of the person. This could therefore have tremendous commercial value for Bermuda.

With the use of all of the above there is also the overarching ability to collect and analyze data based on the e-ID system usage and therefore view trends of the happenings within the island of Bermuda.

E-ID Security

The security of this environment is paramount. Through use of decentralized data sets (blockchains) and distributed ledger technology there would be no single point of vulnerability for hacking. Also, due to the ability to access ONLY certain data from an individual (e-ID holder) with their permission, as stipulated within the PIPA/GDPR requirements, there is a limitation on easily accessible personal information vulnerable to fraud and misuse.

The business model for this is to have a service center model whereby on-boarding is initially done in a highly secure environment where account creation and card issuance is centrally managed. After onboarding several trust agents, such as banks, law firms and unlimited corporate service providers could provide updates to the fundamental data points such as, but limited to address changes, passport updates and change of employer.

Proposed Initiative

Initiative Goals and Objectives

The e-ID initiative is aimed at providing a platform which combines backwards-compatible Digital Identity services across entire jurisdictions with next-generation Digital Identity services and Electronic ID paradigms. The initiative therefore has the following objectives:

- Hybrid between general public and pre-approved Private Sector members and Bermuda Government
- Fully inclusive National ID scheme for people and businesses: covering all local and international Bermuda citizens, residents, tourists and guest workers
- Single aggregation platform for KYC/AML for Bermuda, based on regulatory approved and shareable digital data sets for ID holders between approved / trusted network members and government entities
- Data-rights used by ID holder to allocate specific permissions over exactly which data, for what purpose, for how long and with whom.
- Decentralized trust anchors
- Removes the need for multiple hard copies and “wet signatures”
- Advanced “smart” network protocols reduce risk and increase data reliability and utility by using consensus and attestation
- Not “Big Brother” or an invasion of privacy
- Not giving away “permanent residency” or “status”
- Not a travel document or proof of citizenship
- Offers no rights to any international applicant to do any business within Bermuda or compete with local Bermuda businesses.
- Does not rely on any tax advantage and thus helps Bermuda to build another pillar for its economy which is up to us to decide / grow
- Overseen by regulatory controls imposed by the BMA and government as well as KYC/AML regs and new E-ID Act.
- Verification network to include selected government identity players (TCD, Immigration, Voting, Emergency, etc) plus local utility providers for residency checks, as well as 3rd party global AVV (Authentication, Validation and Verification) providers such as World Check for AML, PEP and related screening and verification.

Scope

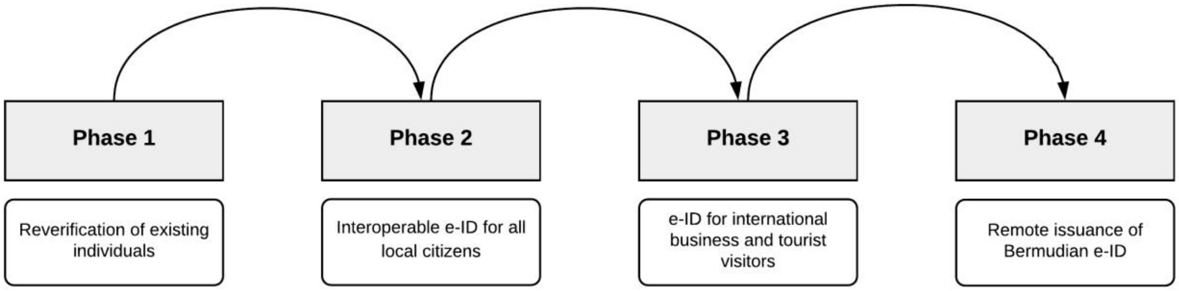
Following the completion of the **POC in Q1 2021**, the roll-out of the e-ID initiative is broken down into four phases and can be primarily scoped as containing the following:

Phase	Scope
1	Reverification of existing individuals Leverages Government Issued IDs and Proof of Residency
2	Interoperable e-ID for all local citizens Additional sources of global data for improved risk evaluation
3	e-ID for international business and tourist visitors Provides additional revenue opportunity for local businesses
4	Remote issuance of Bermudian e-ID Jurisdiction as Service

Below is a list of potential stakeholders which will be impacted by the e-ID initiative:

1. Bermuda Government / Ministry of Finance
2. Registrar General
3. Bermuda Monetary Authority (BMA)
4. National Anti-Money Laundering Committee
5. Transport Control Department (TCD)
6. Mobile Network and Internet Providers (Digicel and One)
7. Electricity Provider (BELCO)
8. Bermuda Business Development Agency
9. Bermudian Residents
10. Bermuda Banks
11. Bermuda CSPs
12. Bermuda Hospitals/Doctor offices
13. Bermuda Law Firms
14. Bermuda Insurance Companies
15. More

Initiative Approach


Phase 1
Reverification of existing individuals
Phase 2
Interoperable e-ID for all local citizens
Phase 3
e-ID for international business and tourist visitors
Phase 4
Remote issuance of Bermudian e-ID

Phase 1: (estimated completion Q3 2021)

In the first phase, the emphasis is in getting local public and private partners integrated into a basic access and credentials network to allow privacy-enabled electronic access to validate local ongoing customer KYC/AML requirements for existing customers of local institutions and companies currently governed by the various regulations and laws pertaining to AML and ATF in Bermuda as well as falling under licensing regimes

per: http://www.bma.bm/legislation/SitePages/Bermudalaws.aspx

This phase will enable the reverification of existing individuals against the database under the simplified requirements of ongoing Customer Due Diligence (CDD) and related authentication, validation and verification capabilities. Primary to this will be the ability to use established technologies and regulatory precedents already approved globally to capture customer consent to enable companies to directly query local datasets held by Stakeholders identified above in order for them to provide assurance under (A) proof of Government Issued Photo ID and (B) Proof of Residency in an all-digital format and near real-time access, without the requirement for wet signature or physical deliver after the fact. The outcome desired is that existing customer of regulated local institutions will, before the end of 2018, be able to use all digital, secure and consent-based authorizations to updated existing CDD requirements with local companies.

Phase 2: (estimated completion Q1, 2022)

Phase 2 will expand upon Phase 1 by adding initial on-boarding new local users (who do not exist in previous databases or local companies) e.g. a new resident or business owner arriving to the island into the e-ID system. This will require the creation of the new users in the system using additional software and hardware solutions on top of the Phase 1 providers, as well as third party solutions for global AML, Politically Exposed Person (PEP), ATF and related CDD to ensure that the individual can be risk rated properly, and their details are valid and have been confirmed as a legal existing person.

The result of this will be the creation of an interoperable local Bermuda e-ID that can be used and shared by all local public and private enterprizes and which is KYC/AML complaint. Equally, Phase 2 expects to be able to then invite all Phase 1 participants to then upgrade their existing local profile to be compliant under the Phase 2 criteria and thus also avail themselves of a fully interoperable local Bermuda e-ID.

Phase 3: (estimated completion Q1 2023)

In the third phase, the e-ID system will be aimed at internationals business and tourist visitors who come to Bermuda for short term stays. The individuals or businesses will be onboarded through the use of selected hardware and software at ports of entry and will be issued a duration and rights managed usable form of e-ID (either digital and/or physical card based) with limits attached that specify their rights and permissions that are sufficient for their stay as a guest and enhance their experience whilst on island. This e-ID can be extended to be used for local payments, gain incentives (loyalty and rewards), transportation and event / physical access - and will of course also enable privacy compliant data collection and targeted marketing resulting in a significant ability to create new services and offerings.

Phase 4: (estimated completion – Q4 2023)

Phase 4 will further expand upon Phase 3 to consist primarily of the remote application and issuing of the Bermudian e-ID to qualifying individuals world-wide. This will allow any legal person or entity to apply for an e-ID under our strict oversight and global best practices requirements, and if approved and once issued use the benefits associated with it to launch good and services from the Bermuda Jurisdiction (our full JDaaS - or Jurisdiction as a Service) offering. This will also enhance the Bermuda FinTech strategy by enabling large scale compliance outsourcing as a service as well to all forms of technology companies including new crypto, digital, healthtech, insuretech, fintech and related entities) to use the Bermuda platform and EID as the bedrock for their strategic growth.

Technical Overview

System Features

System features will include:

- Identity re-confirmation to onboard all users to an Electronic ID-compatible service industry.
- Redundant secure storage systems that function with current technical services as a baseline of compatibility across the network infrastructure.
- Cost-performant use of blockchain infrastructure to expand the compatibility of service offerings internationally.

Technical Stakeholders

Proposed Technical Stakeholders and specialty:

Technical Stakeholder	**Specialty**
Trunomi	Scalable, Secure and flexible Consent Framework and Data Rights Platform giving Data Subjects control & visibility over their data
Shyft Networks	Blockchain-based Digital Identity super-services. Attestations, User accounts, KYC/AML complete payment rails.
BurstIQ	A highly secure blockchain platform that allows individuals to securely share and monetize their data via consent contracts.
Future Partners	In the future we will select hardware and software partners to develop the final solution.

Blockchain-Based Rights and Services Management

Blockchains are an incorruptible digital ledger of transactions that can be programmed to record anything of value. It is considered an open, distributed ledger that can record transactions between two parties efficiently and in a verifiable and permanent way. Public blockchains pose a secure and economically viable solution to the many pain points around digital identity and KYC/AML.

Digital identity transactions consist of three key constituents. These are as follows:

- The Identity Owner, which is an individual or a company.
- Validators, who are trusted third parties who validate others' identities.
- Relying Parties who rely on the work performed by Validators.

Within the digital identity transaction, validators provide utility in the form of KYC/AML procedures which validate the digital identity of the Identity Owner. Public blockchains then store the value of this utility through the use of a token. The token binds the three parties above in a transaction which delivers efficient and secure verification of previously validated Personally Identifiable Information (PII) by trusted Validators, where the Identity Owner retains control of their PII.

Decentralized and self-sovereign digital identity is a foundational piece of the architecture within the new era of decentralized information management. This is as globally there is a trend away from centrally managed identity systems as they present a single point of failure. This will herald the Bring Your Own economy whereby individuals/companies will have sovereignty over their own devices, data, assets, and digital identities.

The issues of sovereignty and cyber-risk can also be tackled through the decentralized nature of blockchains as the provide the following benefits:

- Avoids centralization
- Data Compliance
- Data Minimization
- User Experience
- Innovation Opportunity
- Security offered by hashing of PII including data minimization
- Immutable nature of the public ledger supports self-sovereignty
- Public/private key cryptography provides data portability
- No intermediaries means that the solution has low friction
- Hashing prevents tampering with PII.

With the use of blockchains and the decentralization which comes with them, the sovereignty of the individual will mean control over one’s data and identity through one’s own device. When combined with greater autonomy over financial assets through wallets, this means a Bring Your Own economy can be foreseen.

Tokenization is considered the process of converting rights to real world assets into a digital token on a blockchain. Tokenization therefore is facilitating a number of elements which traditional business strategy can’t, specifically:

- KYC/AML utility can be valued, stored, and traded
- Therefore, digital identity becomes a tradable asset
- The cost of onboarding clients will fall dramatically and become a variable cost
- Traditional cost centers have the potential to become revenue generators. This business model inversion will be a powerful force for innovative expansion to the structure of the economy
- Individuals will have sovereignty over their own devices, data, assets, and digital identity
- Traditional cyber-risk will also be reduced

Success Criteria

For the entire initiative to be deemed as successful, the following criteria need to be met:

1. A digital identity bridge across residents of Bermuda should be created
2. Local public and private partners integrated into a basic access and credentials network
3. The facility and capability to on-board new local users
4. The facilities and capabilities to issue e-ID's to international visitors to the island
5. A platform to provide global qualifying individuals the ability for remote application and issuing of the Bermudian e-ID
6. Support facilities to help with onboarding and use of the e-ID and e-residency
7. Secure exchange of information (cryptography)

Opportunities

The Bermudian e-ID initiative and the proposed implementation approach provides the following opportunities:

- No more centralized data management and therefore individual sovereignty of data and documents
- Facilitation of multijurisdictional data compliance and therefore meeting needs of legislation such as GDPR and PIPA.
- Limited data sharing and therefore greater security and privacy of information
- Increased user experience and data portability
- Potential for major innovation around digital identity
- Constituent right protection and better border control
- Consolidation of real and all digital identities into one user profile "virtual identity"
- Interest in the Bermudian economy: local partnering, taking companies online, online business banking and payment, digital authentication
- KYC/AML abilities and information
- Citizen Health Passport for validated vaccination and health record sharing to protect Bermuda
- Multipurpose, flexible, open-source protocol that will enable dApp solution building
- Develop new Bermuda-based products, solutions and expertise that can be used domestically and exported internationally
- Technology is a borderless resource that can be transplanted anywhere
- Retraining and retooling of Bermuda workforce with a highly demanded and scarce resource expertise
- Reputation and risk profiling
- Voter authentication
- Supply chain management
- Credential validation
- Banking the unbanked
- Make identity a right rather than a privilege
- More…

Challenges

Blockchains

Although blockchains are the way of the future as they are decentralized and therefore encourage control over one's own identity. They do have a number of considerations which need to be addressed. The main ones are listed below:

- There is a possibility of questionable immutability. This is as a user with access to greater than 51% of a public blockchain can overwrite transactions within the blockchain. Procedures need to be put in place to ensure that this is combatted.
- Synthetic identities can be created. There therefore needs to be strict procedures where identity is linked and authenticated to a real person.
- There could be problems with identity verification if the user's private key is lost or lands up in the wrong hands (e.g. stolen or lost phone with the private key contained within an app). There therefore needs to be contingency plans in place where the user can "stop" or "block" their private key as well as get a new one issued after identity has been proven. This could be similar to a fraud hotline in the banking sector.
- Demographics need to be considered as not all people are of equal education and experience and therefore there might be problems with using and understanding the e-ID and the blockchains being used. It is imperative that help options/facilities be available to assist those who need guidance.
- Standardization of implementation and authorization could be problematic and there could also be redundancy of identity authorization. It is needed therefore, to have solid buy in from government and companies (businesses) to ensure that there are not redundant processes within the authentication and authorization transactions utilized.

Biometrics

Biometrics are considered a good way to ensure authentication of an individual's identity and although this is true there are also challenges surrounding this. Biometrics can be difficult to use on infants and young children as well as people who have injuries on the scanned body parts. It is becoming more portable with the use of mobile smart devices with biometric enablement, it however cannot be considered mainstream as yet and therefore could be more costly to implement to cater for those that do not have biometric accessibility.

System Crashes and Problems

Regarding any system implemented, one cannot assume that it will be 100% functioning all the time. It is therefore advisable that there are plans and procedures in place in case of failure. Examples are:

- Critical systems duplicated overseas to ensure immunity over data stored.
- Ensuring an extremely high level of security (e.g. two private keys protected by a user pin) to prevent hacking and misuse of user data.

Privacy and the Law

To implement e-IDs and the digital identities associated with it, it is imperative to have governmental buy in. This is as without laws and policies overseeing the storage of people's data, the data could easily be misappropriated and used as there is no accountability against this. This can be remedied by having laws in place which prevent the ultimate goal of collecting people's data for use and by ensuring that the empanelment of invested agencies is done correctly.

Self-Sovereignty

Overall a self-sovereign identity is positive as it encourages selective sharing of data and trustworthiness of the person, business, government and data being shared. It however needs to be implemented with addressing the following:

- Transparency of transactions
- Consensus of transaction
- Consistency of rights granted versus used
- Standardization of data formats and user interfaces

Most of these can be addressed by the use of blockchains and biometrics.

Project Estimates

The development and implementation costs of the project and new initiatives will be self-funded by Perseid with no new government funding required.

Conclusion

Therefore, by building a phased, highly scalable and compliant identity program, there is the potential for Bermuda to have an e-ID system which can be recognized as a global standard and can be honored among world-wide jurisdictions as interoperable and shareable proof of identity.

By implementing the e-ID initiative: the platform which combines backwards-compatible Digital Identity services across entire jurisdictions with next-generation Digital Identity services and Electronic ID paradigms; there will be a secure and decentralized way for governments, businesses and individuals to manage their identity data and documents link to that identity with validations and authentication.