Harmonization Strategies and Policies for Identity Management
Whitenoise Laboratories (Canada) Inc. Vision

There is a need for a new, flexible, cost-effective online authentication solution that meets a wide range of program requirements.

Dynamic Identity Verification and Authentication [DIVA] provides flexibility to citizens by allowing them to choose the credential provider they use to authenticate themselves to GC programs. It allows citizens to choose the services they wish to access.

Service implementation under this new approach would be based on a federated model and trust framework. This means that stakeholders would collaborate in deploying compatible services that would recognize each other's user credentials.

It is important to note that DIVA can easily be used with any model or framework.

As we choose an authentication solution, we should do so with the knowledge that it can be easily scaled to facilitate international commerce with international partners. The solution needs to address both governmental and commercial needs.

It is critical for cooperating countries to develop a national strategy for Identity Management that will support OECD goals in order to facilitate secure online e-commerce, e-government, and social networking. This paper provides an effective, harmonizing strategy. Sound distributed identity management is a convenient enabler for international commerce and global services so that we better use scarce resources. It will foster innovation and both healthy collaboration and fair competition. A properly implemented dynamic distributed identity (key) system will allow all of this to scale seamlessly as our populations and gross digital commerce continue to increase at dramatic rates that will soon reach compound growth rates.

The goals articulated by the US Cyber Security Policy are shared by Organization of Economic Co-operation and Development countries represented in Seoul. It provides a framework to help harmonize an Identity Management regimen and protocol with our trade partners while safeguarding each country's own national interests. (No country can leave itself digitally vulnerable to another.)

The most challenging substantive issues to address when developing a national Identity Management strategy are well-known. Dynamic Identity Verification and Authentication (DIVA) as a common Identity Management framework can help nations achieve:

- safe online transactions
- better use of resources
- overcoming barriers to growth
- fostering innovation
- enhanced user convenience
- enhanced security and privacy

Harmonization Strategies and Policies for Identity Management
Whitenoise Laboratories (Canada) Inc. Vision

The most challenging functional reality in developing a national Identity Management strategy is to work with the stakeholders to minimize costs and business dislocation. Collaboration between governments, businesses and consumer/citizens will define productive collaborative goals and targets and processes.

All stakeholders need to benefit in order to create favorable conditions for the development of harmonized Identity Management.

The driving force in market-driven, capitalistic societies is money. This has been graphically illustrated in the banking crisis that has so heavily impacted the global recession.

Corporations and manufacturers operate from self interest first. (It becomes a bit more difficult when you add control issues and expectations of responsibility.)

Everyone in the identity ecosystem - governments, businesses and consumer citizens – needs to see where enhanced security and identity management not only is more convenient but that it benefits them financially. A well constructed, flexible identity management protocol will foster innovation, secure collaboration and fair competition.

An over-riding policy should be to phase in higher Identity Management (IdM) security without pushing vendors out of business. They are the fastest channels to ubiquity. Current economies do not need to add business dislocation at this time. All the existing security providers could simply add the identity management protocol to reap additional benefits from their existing offerings and services. It would be interoperable with public services and mandates. It would generate additional revenues for businesses and provide them time to react to market demands.

Since dynamic distributed IdM technologies can run alongside existing systems, or be integrated into existing systems, or be used in lieu of them, market forces and government mandates will determine the levels to which these effective IdM technologies will be configured and used.

Businesses and governments would immediately benefit from a decrease in breaches and cyber crime vulnerability. They would incur fewer costs associated with cyber crime. They will have greater security with less effort. They will have lower security management and maintenance costs. They will have happy clients. They will save on bandwidth and overhead. They will be able to more easily monetize privacy and identity management in the provision of their particular services.

In the Whitenoise vision documents from the US Cyber Leap Year Summit ideas are discussed on how to monetize identity to allow any construct and facilitate anonymity and pseudanonymity while maintaining adjustable shared responsibility between the public/private partnership to address all organizational, inter-organizational, public service, and legal issues.

All businesses remain as the channel. All businesses can prosper from the addition of new protocols as opposed to the elimination of old technology.

Policies can be implemented at any level, or all levels, depending on the balance of security versus convenience versus privacy a particular action requires.

Since effective IdM can be easily implemented and controlled; and since complying with any regulated IdM obligations actually increases operational efficiencies for businesses, good identity management practices and a harmonized dynamic distributed system will foster excellent interoperability across organizations and borders.

It is just as important that users be empowered by using effective Identity Management. Giving users some degree of control and involvement in the maintenance and protection of identity is empowering and makes the system responsive.

The design of distributed key systems means that both endpoints in end-to-end authentication (the service and the consumer - the government and the citizen - the government and the providers) have sufficient-for-the-task identity information stored in a secure manner. Because of the inherent intrusion detection capacity of DIVA, and system design, the stakeholders automatically receive appropriate notification of identity breaches and a logged history of where any breach occurred for forensic and law enforcement uses.

This involvement and transparency of all parties in public/private partnerships or business arrangements will increase both confidence and more effectively serve increased activity.

Identity Management can empower users to participate with business and government in securing their own identities and providing easy and automatic monitoring of their identity.

Dynamic distributed key systems are easy to educate people about because it is what they are already familiar with. Their birth certificates, driver licenses and social insurance numbers are all examples of distributed keys to identity required to access services.

It is easy to educate people about Dynamic Identity Verification and Authentication protocol because it is a simple either-or construct and because all the relevant explanations are available online.

Users, businesses and governments will appreciate and understand that their sensitive data is protected by Identity keys (which can double for unique encryption to ensure safe storage and transit) that are greater than 250,000 bits in scalable strength. This provides embedded identity into quantum computing secure, exponential, identity based cryptosystems. This will justifiably instill confidence in the ecosystem given that sensitive data can only be accessed in storage or transfer by persons who have legitimate authority and purpose.

These dynamic distributed tiered architectures minimize the damage caused by disruption or corruption of data because secure redundant systems can be deployed and because a breach area can

automatically quarantine itself so that there is no cascading effect associated with breaches, denial of service attacks and the like.

A consumer/citizen's unique identity management key uniquely logs and indexes all activity associated with its use and automatic implementation and enforcement of rules and roles is easy to establish. Auditing is automatic and technologically self-monitoring. Revocation to illegal network access and illegal use of an identity is automatic because the inherent intrusion detection capacity identifies any illegal use of an identity.

Auditing, logging and indexing are inherent to the system for easy management.

Since no single party has the entire identity management key, the risks of storing personal information of potentially unlimited lifespan are dramatically reduced. Additionally, user specific encryption, logging and automatic notification of illegal access to information is inherent within the design.

The increased control for all partners allows consumers (where appropriate and agreed upon) some latitude in how to eliminate information and even deactivate their own keys for particular services in the event of concerns about identity theft.

Authentication can be securely done with a single sign on. While unnecessary, Dynamic Distributed Systems can be just as easily configured to request multiple sign ons or different kinds of additional authentication like biometrics. The number of sign-ons (forced authentications) required would just be a choice. We can be certain that high level assurance authentication is not forcibly deployed when only lower-level assurance is needed.

Identity systems must facilitate anonymity and pseudonymity. For example, picture the need of a government to be able to provide anonymity to intelligence agents while still having the ability to be assured of their identity in operations.

The use of anonymous identities raises issues regarding access and what information is available to those with the correct credentials. It raises legal issues. However, these are addressed by the manner in which these identities are distributed, monetized and supervised and the degree of shared responsibility and obligation in relation to these identities. For example, a social networking site can allow psyeudonomic identities to access their services but they share responsibility if their services are used in an illegal manner.

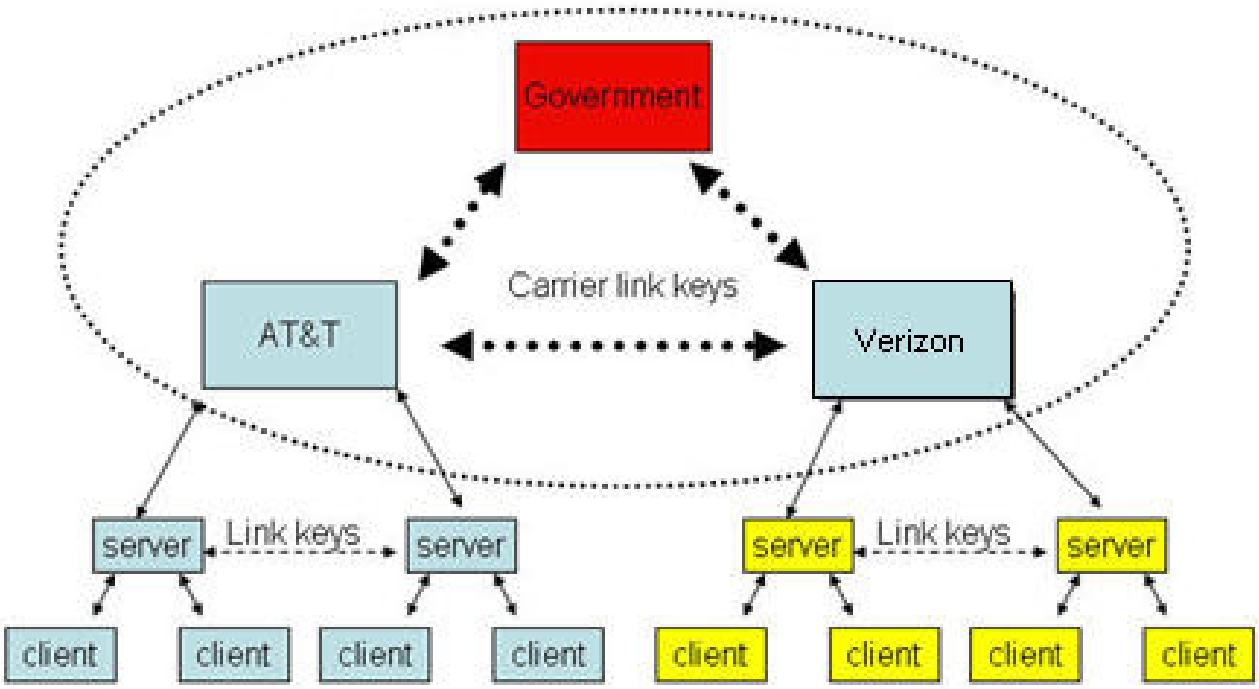
Legislation can address identity management practices and the collection, use and retention of data that rightly distinguish between government's responsibilities and mandates and market forces and citizen's rights and responsibilities.

A strategy for countries to address electronic identity credentials was submitted in the Whitenoise vision presented to the US National Cyber Leap Year Summit.

Harmonization Strategies and Policies for Identity Management
Whitenoise Laboratories (Canada) Inc. Vision

http://www.wnlabs.com/Papers/National_Cyber_Leap_Year_Summit_The_Whitenoise_Vision.pdf

National strategies should contemplate the intersections and relationships between government and private sector systems. The vision paper for the National Cyber Leap Year Summit shows both horizontal and vertical intersections demonstrating the flexibility of the system to be configured according to best practices.



The government issues different kinds of keys and credentials.

The government issues all citizens a unique identity management key. A single identity would allow consumer/citizens to access all services with unique key segments without ever exhausting the key. It is unique for the identity of the person and the associated service.

The government also issues master keys to Tier 1 communication providers. These master keys in turn can be used by the carriers and communications providers to issue an unlimited number of keys/identities to access non-government business services. These relate to services that have been monetized within their commercial systems.

The most difficult challenges to address in the implementation stages of a national Identity Management strategy are productive collaboration with focused leadership.

Governments as operational entities, governments as representatives of peoples, and business providers as commercial stewards for consumers need to be involved in the crafting of appropriate

identity management legislation that safeguards privacy while enabling secure e-government and e-commerce services that benefit all stakeholders.

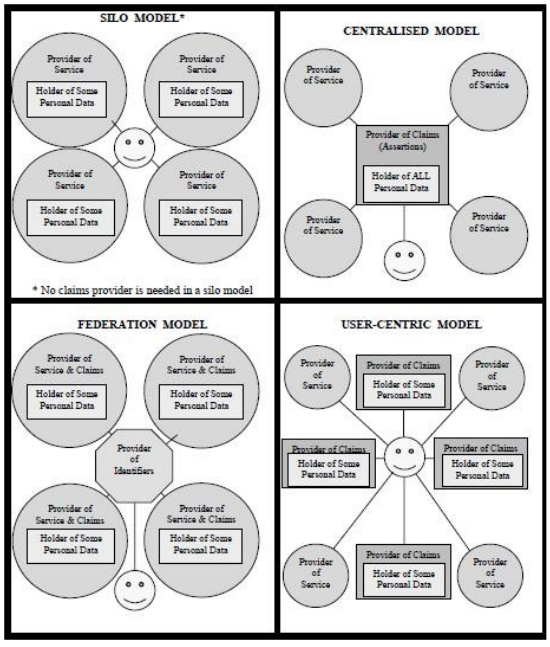
A more secure future is possible with a simple chip or electronic module, at the lowest conceivable costs. It comes down to focus (born of education) to make the standards systems, research systems, business systems and legislative systems more responsive to pressing demands as networks are passing their security limits and risk becoming swamped by cyber crime.

Leadership comes from the top.

National Identity Management strategies are intended to foster innovation because experience has shown that Dynamic Identity Verification and Authentication can work in any kind of digital and electronic context where security and identity assurance is required. It is even possible to secure and identify analog streams by using a digitized IdM key to create a randomized Doppler effect that can be reassembled only with the proper credentials.

DDKI and DIVA should be a common choice of protocols because of its ability to augment the functional requirements at minimal cost for any kind of architecture. As a natural effect, a security cluster will form around this IdM capacity as it enhances the broadest possible range of technologies.

No single architecture is likely to fit all situations. Undoubtedly there is shrewd reasoning behind the choice of network configuration. DIVA's end-to-end authentication allows the protocol to be used between any numbers of endpoints. This allows a simple protocol to be overlaid for secure communications in silo, centralized, federated or user-centric models - or combined models.



The choice of models is influenced by which is the most efficient for a particular service.

A trustworthy and familiar interface will allow service provider-centric models, trusted user-centric models, and trusted third parties acting between users and service providers as appropriate. The choices of those models are influenced by which will most effectively and efficiently allow the enforcement of policies to comply with regulations and the law.

If an identity management solution is a required protocol that is operating system specific and not application specific then it can easily be used in all contexts. All current vendors providing different services on different kinds of networks will naturally work to exploit this capacity to their greatest advantage and this will spur innovation.

Consumers, unconvinced of the benefits of IdM at this time, are unwilling to pay for IdM services. The onus for change then lies with service providers and governments to better educate their constituencies and as a matter of best practices offer secure service.

The IdM investments will also pay off if service providers understand how offering secure services directly leads to increase in profits with less effort.

The tipping point between peril and promise of the Internet is now in delicate balance. The outcome has yet to be determined. Countries will either be properly positioned and leveraged or overwhelmed when compound growth and quantum computing takes over.

Governments needed to be involved to allow nations to build their highway systems. The highway system requires that its users have proper identification and authorization (driver's licenses.) In the same way, governments need to lead in the building of an information highway that is safe and allows our economies to reach the potential of compound growth.

The government through hospitals and birth certification, or the church with birth and baptismal certificates are the initial providers of identity in many societies. They can mandate that a certain subset of nation critical services use certain technologies to access certain services in the national interest. Good legislation can help clarify the requirements for accountability and liability in relation to the use and misuse of identity.

A shared identity protocol facilitates interoperability because it is just a simple, additional, unobtrusive, common authentication factor to add.

Safe data flow and identity exchange is seamless in dynamic, tiered, hierarchical networks. Network servers themselves have identity keys and the servers of different commercial and e-government services have the ability to authenticate themselves and communicate their policies to one another. The processes underlie the architectures and have no discernable, negative impact on the experience of users. Rather, confidence is instilled by knowing there is effective security.

All this will feed an explosion of useful services.

The design of a national strategy enables interoperable Identity Management because any device or service that has access to the Internet can implement effective IdM protocols and mandates.

Devices and applications can download and install the IdM service onto the firmware of these devices. This capacity immediately eliminates any manufacturing problems because devices can be upgraded securely, electronically and at minimum cost.

As importantly, deployment of ASIC chips for distributed identity credentials will create economies of scale and embed the capacity for identity management and key distribution at the point of manufacturing making identity management as easy as the next product release.

The use of standards, norms and good practices for interoperable identity management systems is necessary to achieve the OECD articulated goals. This is the fastest way to prosper from its benefits.

Standards systems need to be responsive to an accelerating technological landscape. Standards are used as often to stifle innovation and maintain market share as to stimulate innovation. There is little reason why efficient, reliable, verifiable and replicable testing of new technological solutions cannot be streamlined so that desperately needed technologies are more readily and transparently tested, vetted and made available. Artificial impediments should be re-thought.

Legislation is currently being modified to reflect the rapidly changing electronic landscape and to address increasing identity management demands of growing societies and economies.

--

Security concerns can now be easily addressed with DDKI and DIVA. Concerns are listed below in italics. Today's realities are listed as counterpoints and recognize that new concerns may arise as online commerce increases.

To have confidence in online services, users will expect identity information to be available when and where required. They will also expect that it is accurate and can only be accessed in storage and transfer by those who have legitimate authority and purpose.

- Identity information is immediately available when required by accessing the Internet with a device embedding your distributed identity management key. In a distributed identity management system a person's private identity information is encrypted in their own unique key. Therefore privacy is ensured because this information is accessible to the individual and those with proper authority and roles (for example when a physician has access to your medical records to treat you.) This holds true even if your data is in the cloud.

Other challenges relate to the need to minimize the impact of the disruption or corruption of an

identity management system. Consistent security policies that can be applied across all components of the services will need to be developed and implemented. Joined-up services may raise particular challenges in this respect.

- In distributed *identity management* structures network access is immediately denied when illegal use of identity is detected. In tiered, hierarchical networks, different layers and services can automatically quarantine themselves when certain defined events occur. It is easy to develop and implement policies that will increase the security across all services and components. It is simple for online services to choose and configure the level of authentication they require. Automated enforcement of user roles and rules in a consistent manner ensures the users the highest level of security with the greatest assurance of privacy.

--

All account use is logged and cannot be spoofed. Auditing controls and maintenance is simple and inexpensive.

Processes and procedures to address the possibility of a data breach will be properly sized to the context. (For example, a breach of a defense system would result in different procedures than the breach of a social networking site.)

Our policy with regards to the security of *identity management* systems and how it is refined is that there should be regular (and simple) oversight and assessment so that identity management systems can always be fine-tuned to address a changing technology landscape.

We can focus on forward looking issues as opposed to always being in a reactive "damage control" mode because misuse of identities is automatically detected and the technical "self protection" response is immediate.

In many ways, designing policies in regards to the security of *identity management* systems and policy enforcement is easier in e-government systems and services. This is because rules regarding information sharing are already established. New identity management enablers can be configured to exactly mirror the existing policies that govern need-to-know and chain-of-command realities. It will simply fill all the gaps and vulnerabilities that currently exist and make the response to irregularities real time or nearer to real time. It is the time between a breach and a well defined response that determines the efficiency and integrity of any system and the amount of harm endured.

These rules have been legislated or are in the process of being legislated.

It is in the process of legislation that the most obvious intersection between government, consumers and businesses is seen. It is the effective use of democratic processes that allow consensus on rules and processes that relate to the use and safeguarding of identity. The hallmarks are flexibility and shared responsibility.

US National Cyber Security Leap Year 2009 technical conclusions

"Technologies now exist to express scalable symmetric key authenticated encryption systems where no single trusted third party knows the final key." **US National Cyber Security Leap Year**

"Robust cryptographic authentication would change the game by employing cryptographic methods which enable secure authentication without transmitting the raw credentials for validation." **US National Cyber Security Leap Year**

Dynamic Identity Verification and Authentication is a quantum computing secure, exponential, identity based crypto system that provides continuous authentication, inherent intrusion detection and automatic denial of network access to criminal behaviour.

It enables a single identity management key to be used securely for unlimited number of purposes and services since the identity management keys are greater than 250,000 bits in scalable strength and generate keys streams greater than 10^{60} (ten to the 60th power) bytes in length. The ultimate strength and security of the system is ensured since the system operates as a one-time-pad which is the only mathematically-proven unbreakable key technology.

As additional benefits, the current deficiencies in existing data communication networks are fixed. These current network weaknesses include:

- Outdated and weak encryption algorithms
- No secure, two-way broadband communication protocol
- Vulnerability to man-in-the-middle attacks
- Vulnerability to side channel attacks
- Vulnerability to spoofing and other kinds of illegal network access
- Poor scalability of network topology
- No one-to-many communication capability
- No inherent intrusion detection
- No integrated identity management
- No continuous authentication
- No automatic revocation
- No simple key distribution and management
- Poor interoperability with other network protocols
- High overhead and bandwidth

Properly implemented identity management systems will always require transparency to multiple parties. The choice of the oversight processes will be determined by government, business and consumer advocacy groups that will impact legislation.

Since no single party has the entire identity management key, the risks of storing personal information of potentially unlimited lifespan are dramatically reduced. Additionally, user specific

encryption, logging and automatic notification of illegal access to information is inherent within the design.

The increased control for all partners allows consumers (where appropriate and agreed upon) some latitude in how to eliminate information and even deactivate their own keys for particular services in the event of concerns about identity theft. This addresses arguments about for opting in or opting out of services moot as these rights and policies are easy to configure.

Identity systems must facilitate anonymity and pseudonymity.

Legislation can address identity management practices and the collection, use and retention of data that rightly distinguish between government's responsibilities and mandates and market forces and citizen's rights and responsibilities.

Good, reliable, accurate and easy auditing with well logged identity usage histories is always a part of best practices. Regular backups and integrity checks of any network system is always wise and in fact a responsibility.

Privacy to the degree that it is granted is a right of citizens in democratic societies. Just as citizens are innocent until proven guilty, privacy should skew to the interests of citizens.

However, the degree of privacy granted within an identity managed network is determined by its rules and policies. These rules and policies tend to reflect the value system in balancing security and privacy that different countries with different kinds of governments that societies choose. Individuals can choose whether to opt in or opt out of most services.

Privacy impact assessments are foundational to creating *identity management* systems that will be used. Dynamic Distribute Key Infrastructures and Dynamic Identity Verification and Authentication protocols have been intentionally designed to embrace all architectures while ensuring the highest levels of security and privacy.

Dynamic distributed identity management architectures facilitate the appropriate use of pseudonyms and private passwords that can allow different levels of anonymity. Offering different levels of anonymity is a service that can be monetized by network facilitators.

Organizations should comply with the Organisation for Economic Co-operation and Development (*OECD*) Guidelines on the Protection of Privacy and Transborder Flows of Personal Data and applicable regulations. The collection, use, storage, transfer, and disclosure of personal information should be limited to what is necessary to accomplish the task and follow well articulated, understandable and available rules and roles.

In distributed identity management systems the endpoints - the consumer and the service providers - have secure copies of identity information. This can enable increased individual control over

personal data. For example, security of data becomes very user centric when consumer/citizens can choose their own secret and private passwords to uniquely encrypt and store their own data.

Individual control over personal data by the authentication subject is encouraged even if stewardship of that data is by a public authority or other third party.

Required identity attributes to access particular services can be constructed. They should be reasonable and sufficient-for-the-task to avoid excessive data collection or transfer. At all times, all of this data can be guarded by using quantum computing secure symmetric key encryption. It is further secured by how different parts of identity are stored or shared across systems.

Dynamic Identity Verification and Authentication structures incorporate privacy and security controls. The design also anticipated the training and education required to instill familiarity and confidence. Full blown system administration training can be accomplished online in under two hours and training for users takes minutes.

One simplifier is to create a DIVA tier that all different identity management systems can access and exploit. This will create one look for users and yet accommodate the architectural flexibility that the markets demand.

The appropriate designed response is that different kinds of digital identification systems can be used with the same digital identification that a consumer is provided. This simplifies the multiple enrollment processes that a consumer must do to increasingly exploit the advantages of e-commerce and e-government.

Different kinds of *identity management* system configurations and rules and policies are chosen specifically because they identify primary accountability in the event of an incident. However the system is strengthened and more robust because the process can be transparent to all components across interconnected *identity management* systems.

The benefits and risks of using *identity management* systems need to be effectively communicated to user/citizens. Education is the key but with massive populations and compound growth a system must be simple to teach and understand. It must also be simple for everyone to comply with the protocols, rules and processes when mandated by governments or required for commerce.

Enrolment for services is easy and intuitive the very first time and consumers will learn that it can be generalized because it will be common to most, if not all, services.

Over time citizens, organizations and government will see the costs of services drop and quality of service increase.

The simplest way to make users/citizens aware of the benefits and risks of IdM systems is to provide them a simple task to reinforce their sense of empowerment and security. Since these dynamic

systems provide end-to-end authentication, either end can actively request authentication and response. In this manner, a consumer can click a button on a cell phone for example and get an immediate status they can SEE as to the integrity of their accounts.

User/citizens will learn that it is a security measure they can invoke.

Over a short period of time, everyone will experience the benefits of identity management because they won't experience identity theft and they will be impacted far less by cyber crimes (like spamming and denials of services.) And, this will be measurable.

They will also experience faster and more accurate services.

When an intrusion or incident is detected there is automatic email notification to authorized persons. For general commercial services a consumer will always be notified. For contexts of greater security, law-enforcement and the like, notifications can be withheld or delayed. Rules and policies for governing this context are determined by legislation or judicial action.

Conclusion and moving forward:

Currently the international standards policies do not contemplate the authentication of documents. They do not include device or domain-level authentication even though they do have linkages. Nor do the policies contemplate authorization or electronic signatures.

This should be open for consideration now since Dynamic Identity Verification and Authentication can easily accomplish those additional security measures with the same quantum-computing-secure identity management keys.