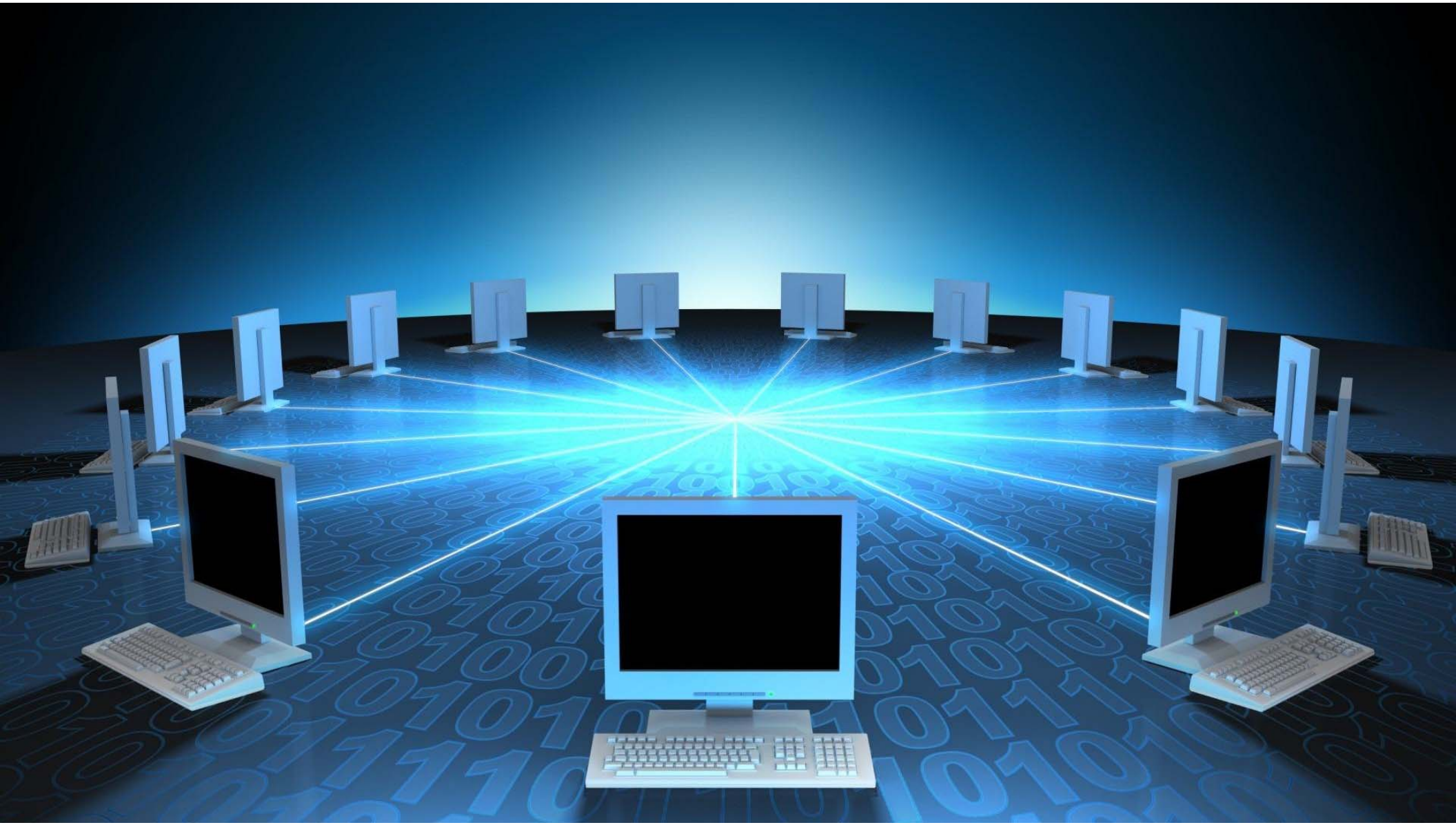
notarius

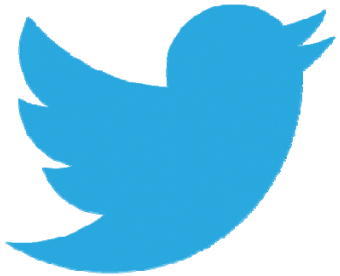
June 12
2018

AMCTO Presentation

Digital ID & Authentication of Documents



So much innovation out there..!



Why is innovation hard in government?

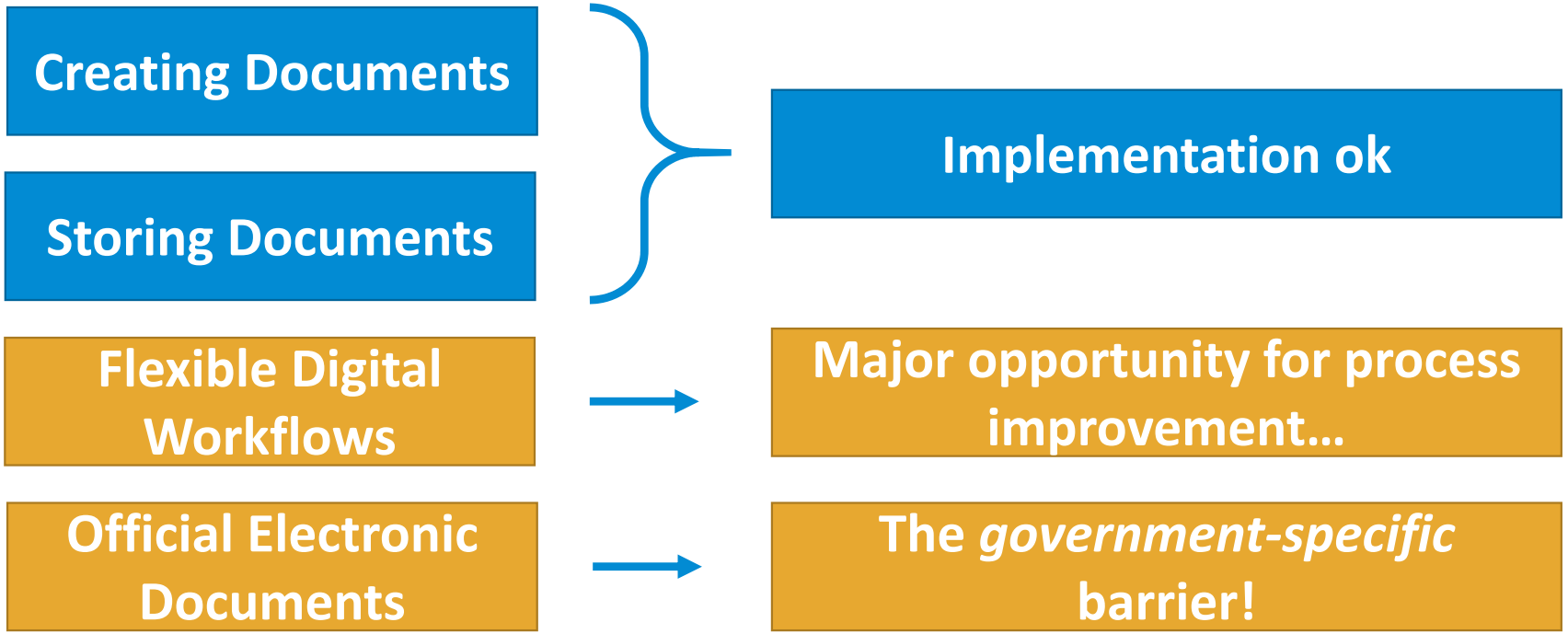


Table of Contents

1.1

Terminology

It all starts with using the same terms

Ever read “How to read a book” from Mortimer Adler?

It’s all about the differences between *terms* and *words*.

Electronic and digital signing and sealing is NOT a universal field of endeavour benefitting from universal shared understanding of the *terms* used.

We have to start there…

Terminology

Signature	Electronic Signature	Digital Signature
Permanent marks bonded to static documents that are traceable, exclusive and personal to persons. They constitute evidence of implicit or explicit intent. *Permanent Binding Static Traceable Exclusive Intent*	*Signatures in the electronic medium. They cover a vast array of use cases and are of varying reliability*	*Electronic signatures in which reliability characteristics have been reinforced with cryptography to augment document reliability*
	Digital Signing Certificate	**Digital Seals**
	Cryptographically protected information in which the veracity of the certificate details is certified by a Certificate Authority	*Digital signatures in which the professional association affiliation is cryptographically asserted and controlled by the professional association*

Terminology (cont'd)

Identifier	Attribute	PDF/A
Information meant to refer uniquely to a person in a system or ecosystem	*Information meant to refer to several persons in a system or ecosystem*	*The ISO 19005 standard ensuring that electronic documents can be opened and read over long periods*
Identity	**Digital Identity**	**Document Reliability**
Social convention linking an identifier (and possibly attributes) with a person	*Technological convention cryptographically linking an identifier (and possibly attributes) with a person*	*Objective degree to which the reader can be sure of the origin, integrity, authenticity and longevity of the document*

1.2

Document Reliability

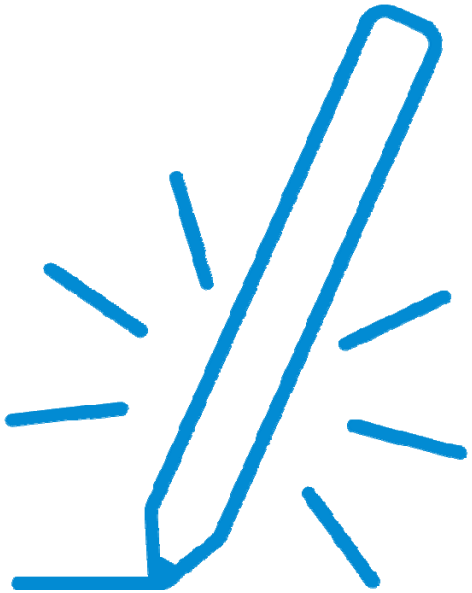
The probative value of electronic documents?

Concepts #1: Identity

When you lay eyes on any digital records, the first thing you do is to ascertain the identity of signers (before assessing its content): who is this from / who signed it? Date and time? Was the signed an engineer, planner, architect, CPA, lawyer? Etc...

Official documents, by their very nature, require readers to TRUST the identity of signers.

Query: How can you ascertain the true identity of signers of electronic documents?



Concept #2: Integrity

When you need to rely on a digital record, you automatically need to be sure it has not been altered since it was finalized / signed.

Digital records, to preserve their value, require their integrity to be PROTECTED.

Query: How can you ensure electronic documents have not been tampered with?

Concepts #3: Authenticity

Digital records move around. They are submitted, transferred, filed and certified copies are requested for onward transmittal. At each step of the way and including final readers, people need to verify the origin and integrity of the document. Authenticity is all about embedding in the document all that is required to prove the origin and integrity of the document.

Digital records simply cannot be considered "official" if they do not include PROOF of their authenticity.

Query: How can you embed proof of signer identity and of content integrity in electronic documents?

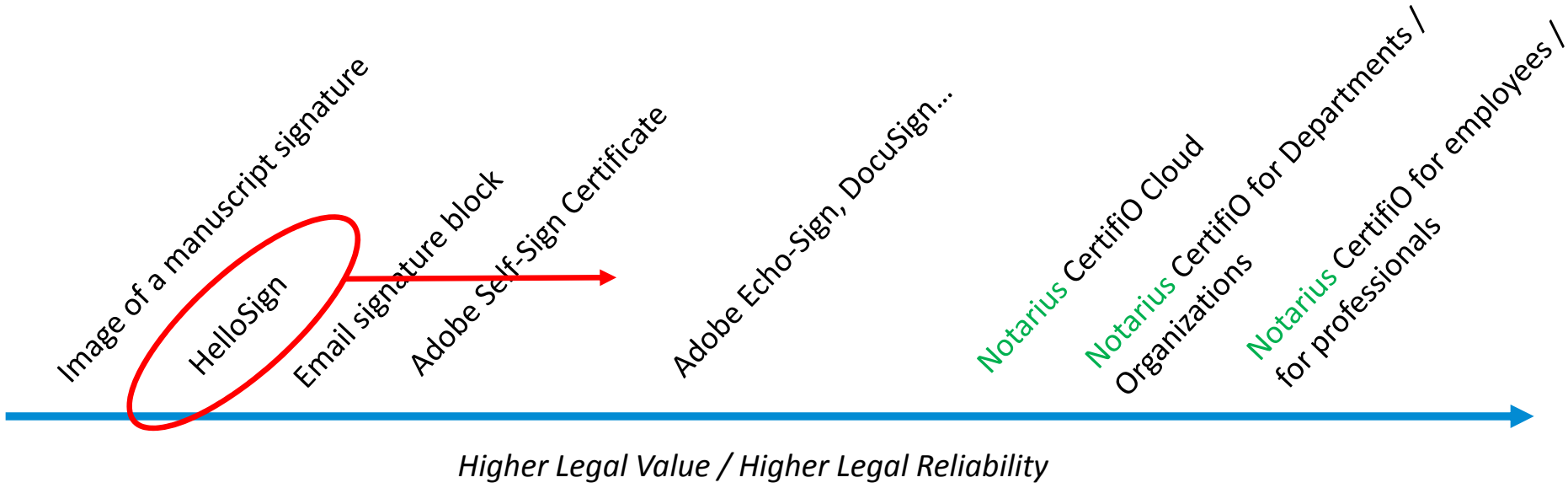
Concept #4: Longevity

In addition to identity, integrity and authenticity, many digital records require longevity or, in other words, need to be opened, read, and their authenticity *verified over long periods of time*.

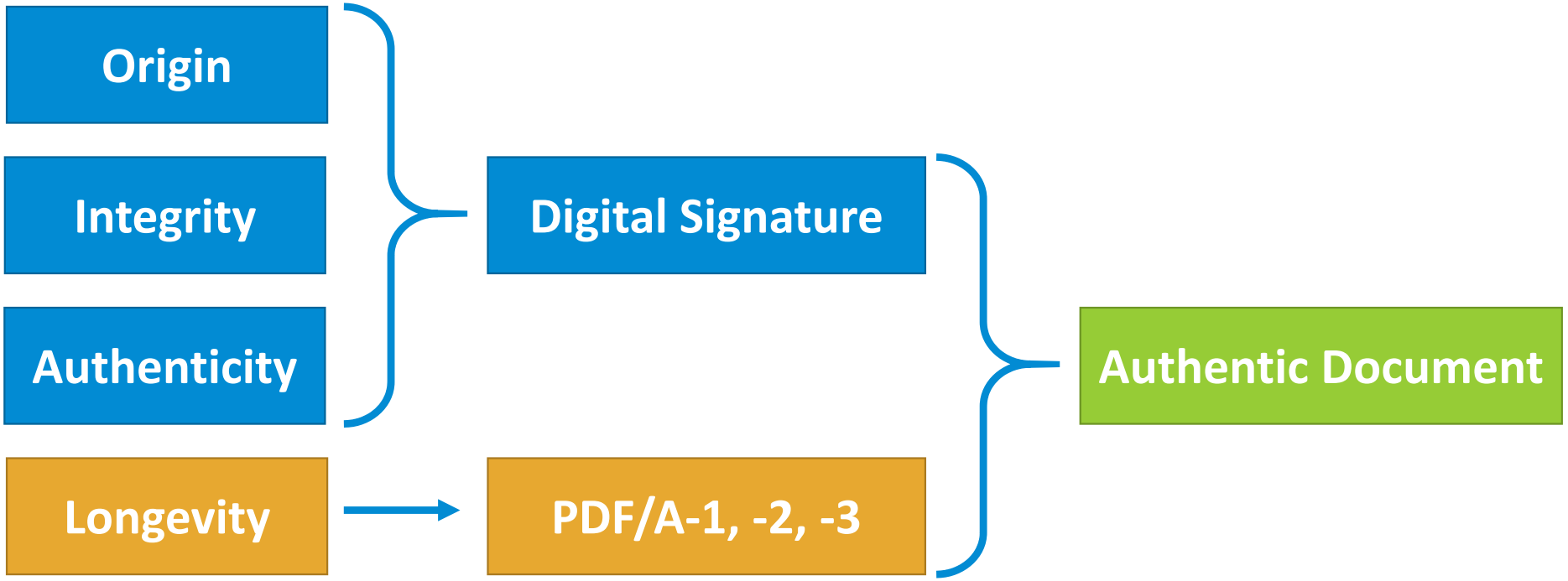
Many digital records, owing to their nature, have a long life and need to be trusted over their entire LIFECYCLE.

Query: How can you ensure that electronic documents can be opened, read and verified over the next 10, 30, 60 years?

The Continuum of Electronic Signing (Examples)



Document Reliability – Technology Recipe



1.3

Reliance on Digital Seals

30+ professional associations across Canada already use professional digital seals.

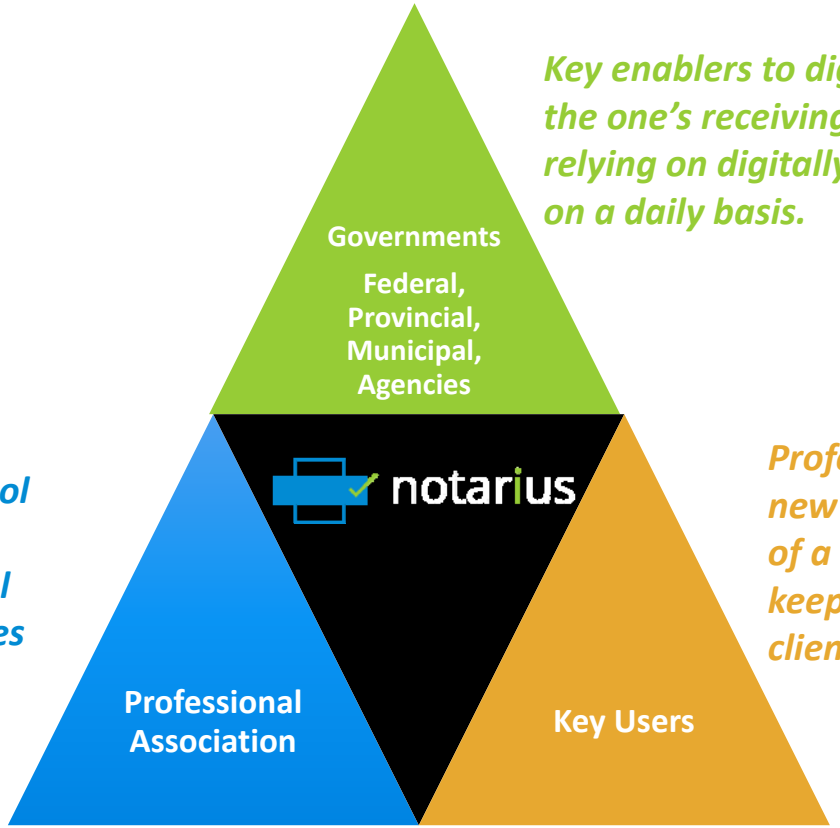
Why should this matter to Ontario municipalities?

The Big Picture

A sustainable digital professional ecosystem consists of 3 key participants:

1. Trusted issuer: Association
2. Users: Professionals
3. Reliance: Client acceptance and reliance

They establish competency profiles, control admission to the profession and ensures members remain competent. They control the issuance of digital seals and signatures needed by professionals.



Key enablers to digital transformation, they are the one's receiving / consuming / approving / relying on digitally signed and sealed documents on a daily basis.

Professionals that thrive in finding new ways to be efficient. precursors of a constantly evolving practice, keeping pace with technology and client's needs.

The Professional Digital Seal

What it means for the Association:

- The Association controls and approves each Digital Seal request
- The Association revokes the Digital Seal if right to practice is lost
- Notarius manages the lifecycle of digital signing certificates
- Notarius offers customer support to planners: webinars, video guide, chat, phone, email

What it means for professional:

- They obtain the Digital Seal from Notarius
- Notarius conducts the identity verification (video conference)
- The Association confirms professional credentials
- Notarius issues the digital signature or seal and related software
- Ready and set to go!

The Professional Digital Seal and Relying Parties

What is means for the Relying Parties:

- For now and for as long as documents are kept, proof that document was authenticated by an engineer is embedded and legally reliable
- Potentially huge implications in terms of accessing professional liability insurance
- Meaningful measure increasing protection of the public

The Employee Digital Seal

What it means for the Municipality:

- The Municipality controls and approves each Digital Seal request
- The Municipality revokes the Digital Seal if employment is terminated
- Notarius manages the lifecycle of digital signing certificates
- Notarius offers customer support to planners: webinars, video guide, chat, phone, email

What it means for the employee:

- They obtain the Digital Seal from Notarius
- Notarius conducts the identity verification (video conference)
- The Municipality confirms employee credentials
- Notarius issues the digital signature or seal and related software
- Ready and set to go!

1.4 Moving forward…

Why are Digital Seals the right step forward for Ontario Municipalities:

- Already recommended by the Association of Municipalities of Ontario (AMO) as the exclusive recommended supplier of electronic and digital signatures to Ontario municipalities following a competitive process;
- It is easy for municipalities to (1) accept; (2) encourage; and eventually (3) make mandatory, the e-filing of *digitally sealed or electronically signed* documents – very few statutory and regulatory exceptions!

What if professional digital seals are not yet available in Ontario and we want it?

- Write to the professional association and state that it would help you, as a relying party, if members of the professional association had access to professional digital seals issued by the association!
- In the meantime, ask for PDF/A documents that are digitally signed according to a vendor neutral specifications to protect the municipality.

Under the current state of technology, digital signatures are the best method to ensure only legitimate holders of digital signatures are able to affix them to electronic documents.

2.1

The Tipping Point

And why consider this now?

We have been talking about the « Paperless Office » for over twenty years.

What makes the transition to electronic and digital signatures more pertinent today than it ever has?

Why adopt digital & electronic signatures?

People expectations:

- Younger generations are, and will continue to be, puzzled and annoyed by the need to sign documents on paper
- Individuals accustomed to work electronically internally and with other service providers have started to require professionals to adapt and evolve their practices
- Municipalities should not have to sacrifice *legal reliability* to obtain *IT convenience*

Increased efficiencies & effectiveness:

- There is no *no need to sacrifice legal authenticity* when finalizing electronic documents. When done properly, it's the oppositice – *you end up with higher reliability documents!*
- Considerable reduction in delays, errors and hassle when adopting a fluid online electronic signing process
- Anticipating relying party requirements / providing reliable documents

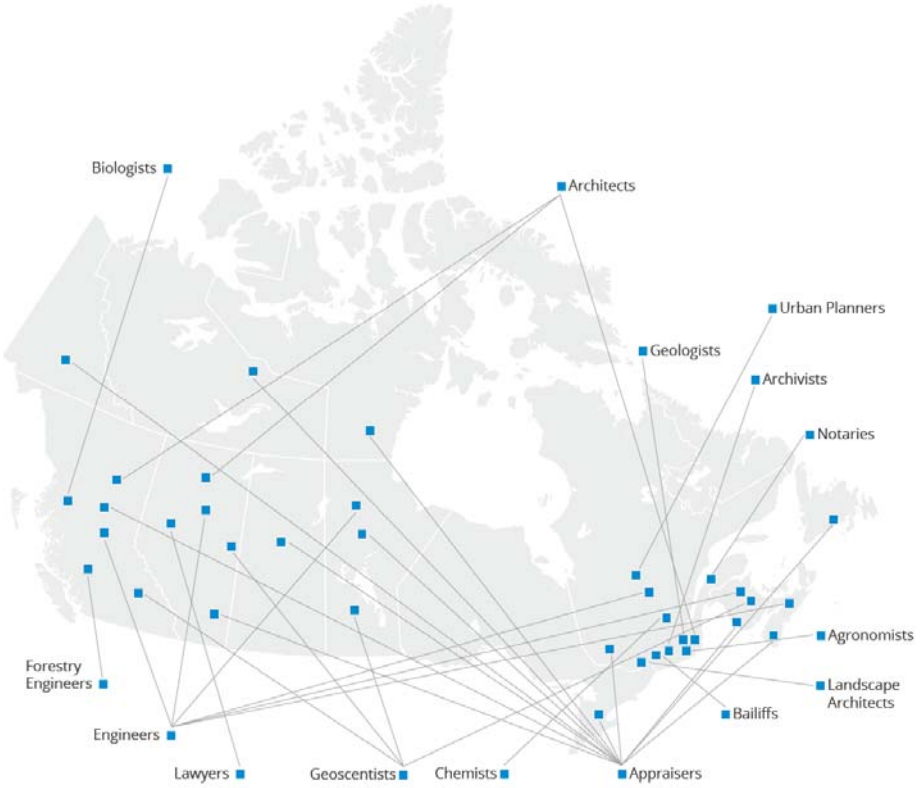
3

The How

What could Notarius bring to Municipalities?

Notarius has developed, since 1998, deep expertise in *electronic document reliability* and the technological means to achieve it.

3.2 Professional Associations Digitally Empowered



3.3 Notarius Solutions

certifiO

Identity

consignO

Productivity

verifiO

Validity

Notarius Examples

Alberta Land Titles Office

- 800K documents filed per year
- 4M documents certified per year
- 106 Examiners
- Micro-billing
- Low Filing fee – sum total of:
  - Notarius fee
  - Cost recovery fee(s)

Quebec Archivisits

- Developing Digital Transformation course for Archivists (Fall 2016)

Manitoba Hydro

- 30K cost -> 1M recurring savings

Key ingredients to successful solutions

Open Standards	Simplicity	Genuine Partner
No « vendor lock in »	Scalability (# docs / # workflows)	Vendor Survivability
No vendor dependency	Highest Document Reliability (Origin, Integrity, Authenticity, Longevity)	TCO Approach
Cost Recovery Option	Real Workflow Adaptability	Vendor Municipal Expertise
Data in Canada Restriction	Cumulative Workflows Capacity	AATL Document Recognition
Data On Premise Option	“Can you explain it? ”	ISO 27001 Vendor Certification

bit.ly/municipal-digital-survey

notarius

Questions?

Patrick Cormier
patrick.cormier@notarius.com

Nada Belhadfa
nada.belhadfa@notarius.com

Notarius

Pricing

	Sign-Up (One-time)	Subscription (Yearly)
CertifiO Pro	$140	$185
CertifiO Employee	$95	$125
CertifiO Department		$220
ConsignO Desktop		*Included with CertifiO subscription*
ConsignO Cloud users		*Competitive tiered pricing*
ConsignO Cloud signers		*No cost*