

Electronic & Digital Signatures

A focus on Notarial Acts and eApostilles

Steve Roylance

Strategic Projects Director – GMO GlobalSign Limited

Liaquat Khan

co-Founder and Technical Director – Ascertia Limited




Agenda

- Steve Roylance – Strategic Projects Director – A more personal introduction.
- GlobalSign - A reminder of what a Certification Authority (CA) is and value added.
- Customer Examples – Business Registry's & Competent Authorities.
- ‘Electronic & Digital Signatures’ – Let’s make sure we know the differences.
- “New” eIDAS regulations in Europe – A top level overview and applicability worldwide.
- “New” Workflow options for Competent Authorities – Signing in the Cloud! (eApostilles)
- Questions?

Steve Roylance – A more personal Introduction

- **Strategic Projects Director - GMO GlobalSign Ltd.**
- 25+ years in the IT industry
- 50% of which has been in the Certification Authority (CA) Industry (Representing 3 well known CAs)
- Founder of the CABForum* 

 Companies Registration Office [IE] <https://www.cro.ie>

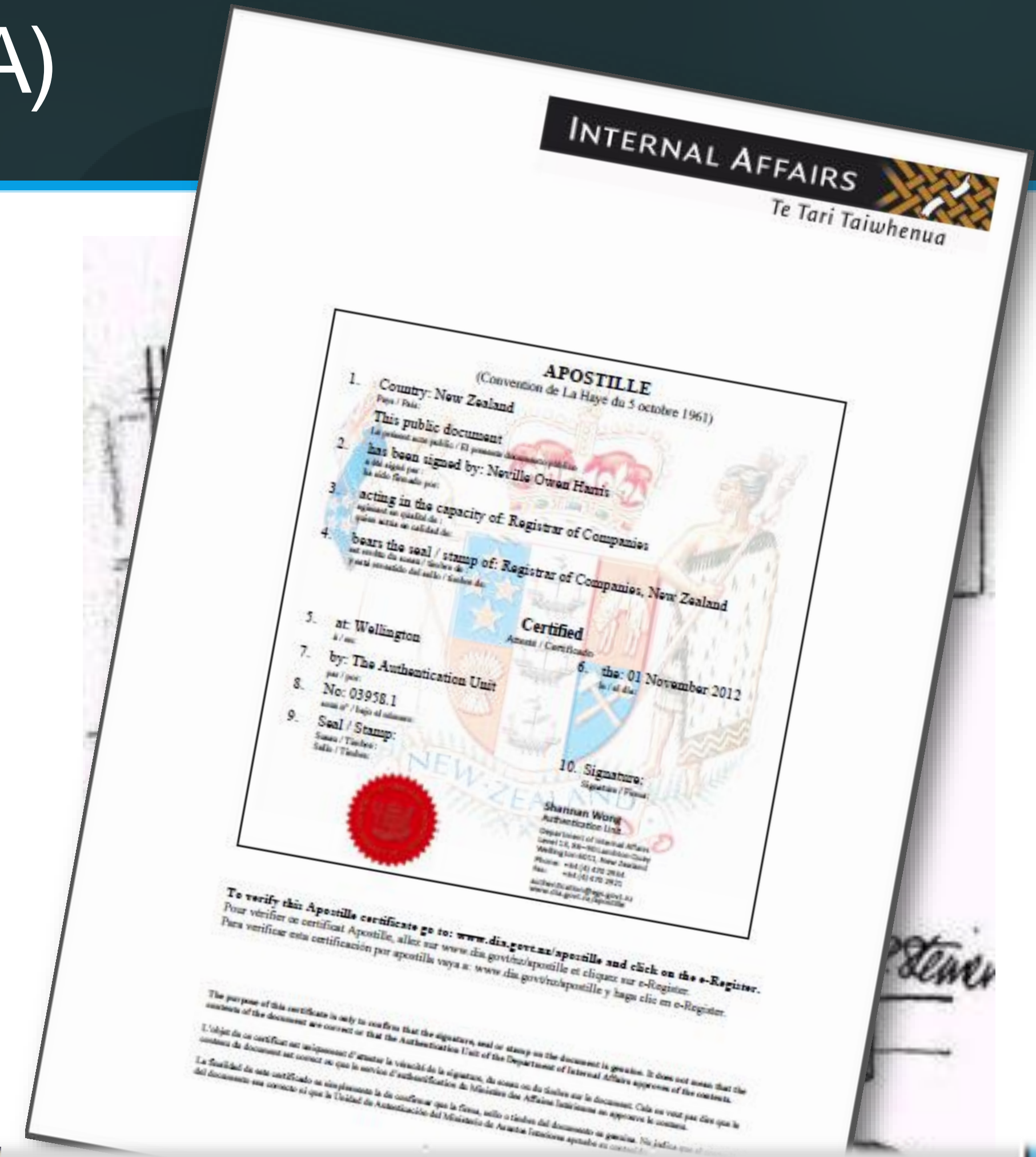
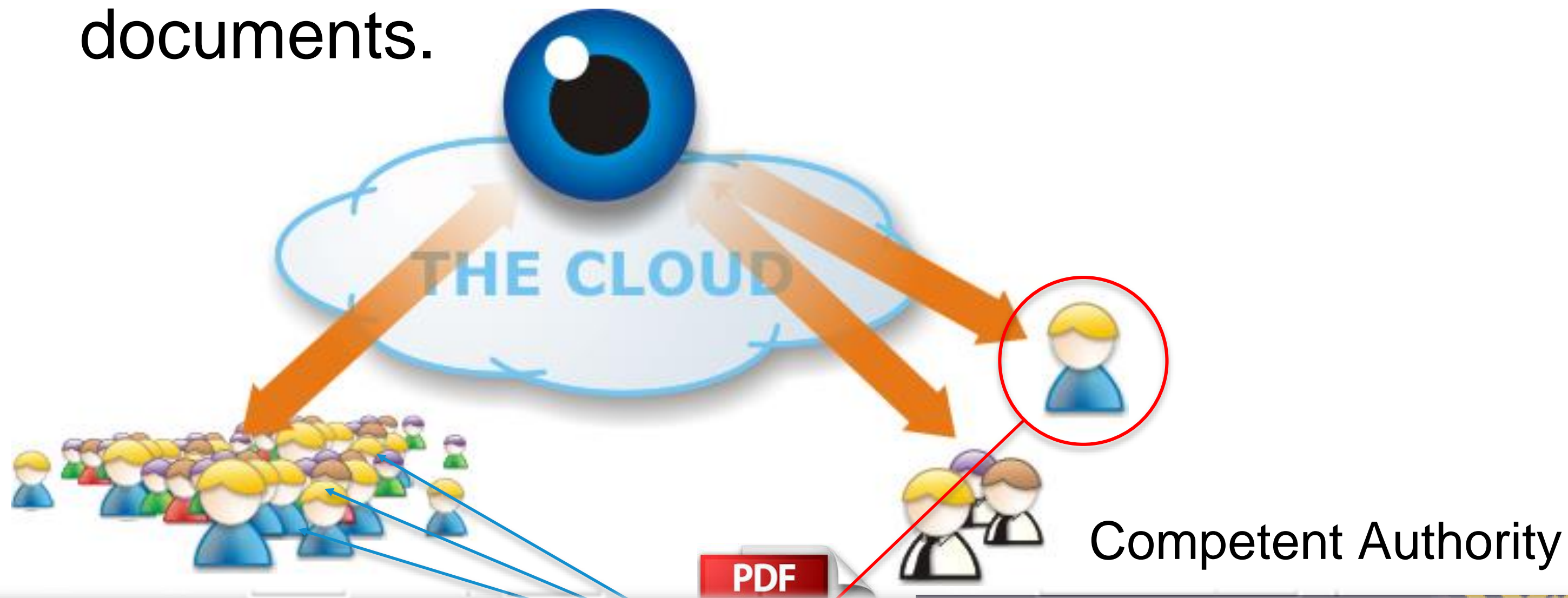
- OneClickSSL – Inventor - Patented Domain Authentication System
- GAuth™ - Inventor – Patented Registry Authentication System
- Technical Evangelist for PKI & Identity management, painter, golfer, husband and father.



**Together with Phillip Hallam-Baker formally of VeriSign*

GlobalSign - What is a Certification Authority (CA)

- A **Trusted Third Party (TTP)** that mediates trust between entities who wish to use the Internet to 'transact' or 'verify the authenticity' of signed documents.



Certified by Authentication Officer <authentication@egs.govt.nz>, Department of Internal Affairs,
certificate issued by GlobalSign SHA256 CA for Adobe.



Signature Panel

Customer Examples – Business Registries & Competent Authorities



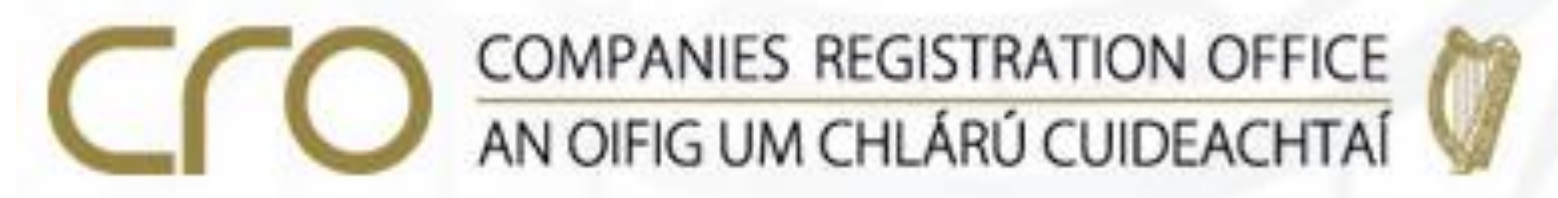
Bolagsverket uses GlobalSign's Certified Document Services solution to digitally Sign e-Certificates of registration for ALL companies registered through the Swedish Companies Registration Office in Sweden.



The Department of Internal Affairs in Wellington NZ uses GlobalSign's Certified Document Services solution to digitally Sign eApostilles in line with requirements of the Hague Convention and best practice from the HCCH. They also protect their eRegister with ExtendedSSL.



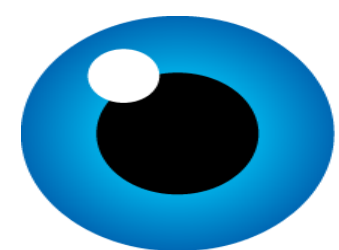
The FCO uses a GlobalSign SSL/TLS Certificate on the 'Verify an apostille' website to help visitors know they are on the legitimate web site for this purpose. Ideally this will soon move to ExtendedSSL to make this even easier.



CRO uses GlobalSign's Certified Document Services solution to digitally Sign extracts for ALL companies registered through the Companies Registration Office in Ireland in compliance with new 2014 Companies Act.

They also protect www.cro.ie with ExtendedSSL.

Alternative formats for Signing



GlobalSign®
GMO INTERNET GROUP



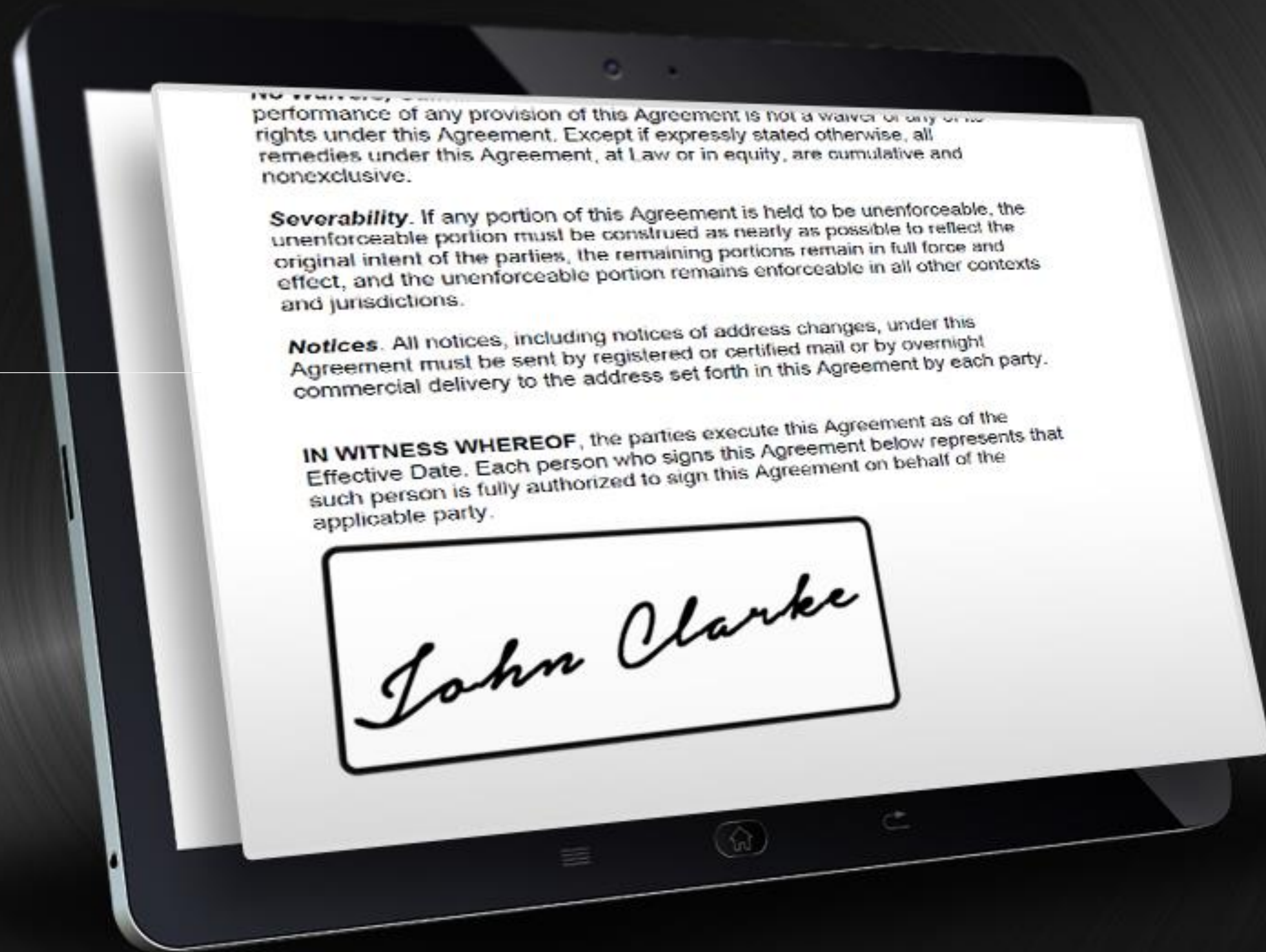
IDENTITY PROVEN
TRUST DELIVERED

Basic e-signatures

Signer makes their
“mark” on the
document

Properties:

- No protection of the document itself
- Signer can claim e-signature was copied from another document
- Signer can claim document was changed after e-signing
- Signer can claim that this is not their signature



Different levels of signatures

EU Qualified
Signatures

Advanced
Electronic
Signatures

Basic
Electronic
Signatures

All can be accepted in court
Higher-levels provide greater trust
and non-repudiation
Higher levels add complexity and
cost

Support different levels of
signatures and select level based
on specific business use case

Meeting the “EU” definition for Advanced Electronic Signatures

Advanced Electronic Signatures are:

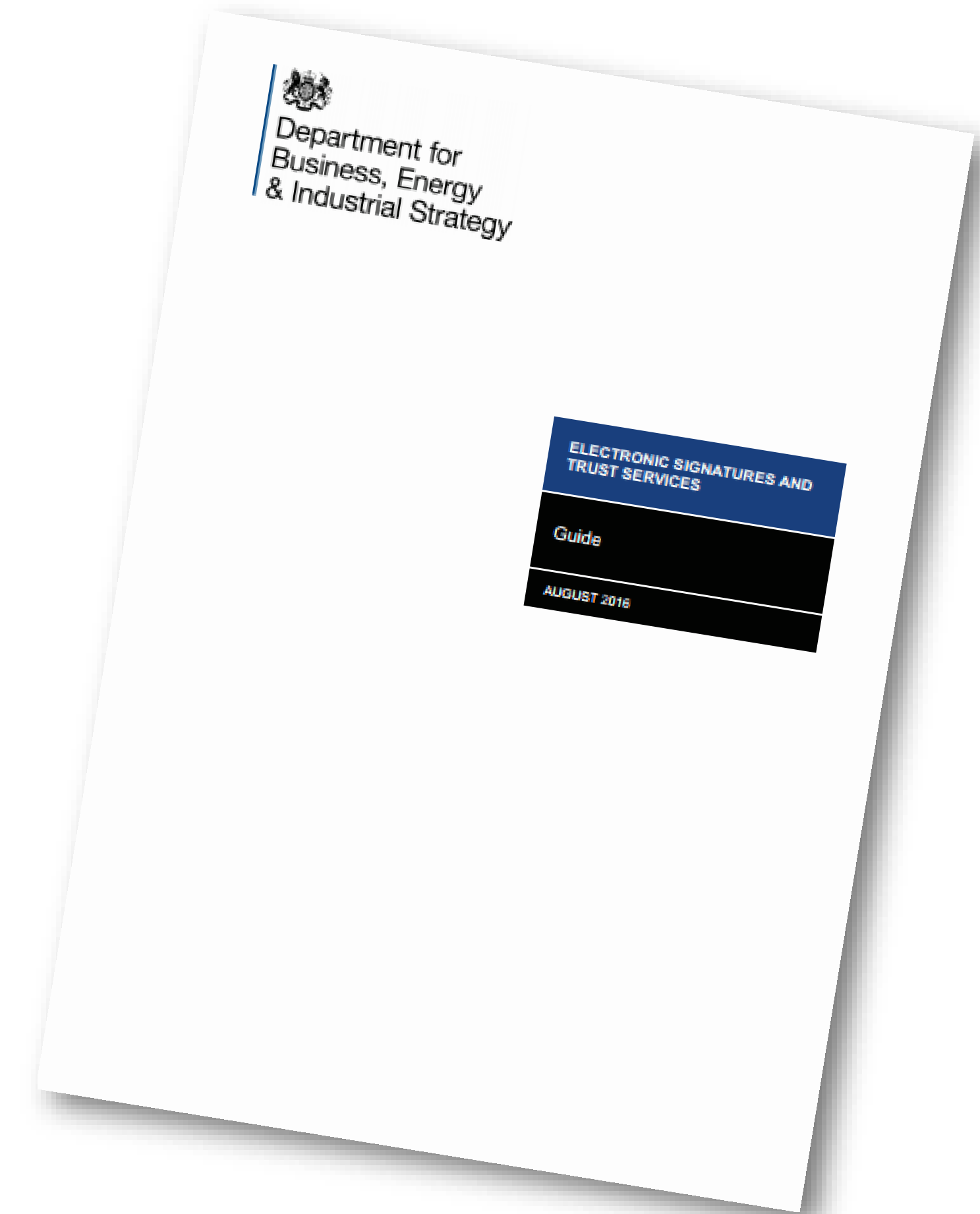
- Uniquely linked to the signer
- Capable of identifying the signer
- Created using means that the signatory can maintain under their sole control
- Linked to the data to which it relates in such a manner that any subsequent change of the data is detectable

Regulations

- As of July 2016 the new eIDAS Regulation supersedes the older 1999 EU Directive on electronic signatures.
- The UK this is covered in a document issued by the Department for BE & IS (Electronic Signatures and Trust Services



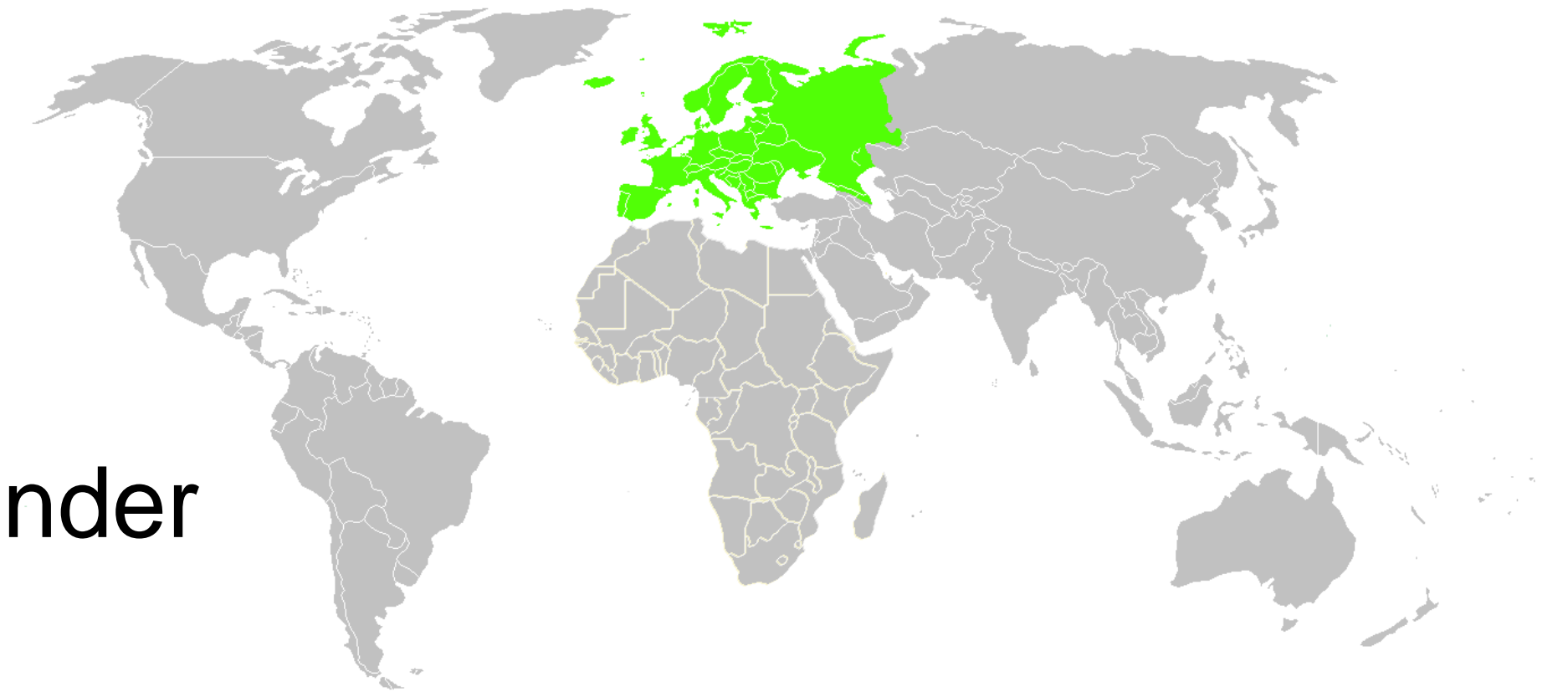
<https://goo.gl/dbPCxy>



Meeting the worldwide definition of Advanced Electronic signatures

Advanced Electronic Signatures are:

- Uniquely linked to the signer
- Capable of identifying the signer
- Created using means that the signatory can maintain under their sole control
- Linked to the data to which it relates in such a manner that any subsequent change of the data is detectable



Other Worldwide Regulations encompassed by AdES

- UETA - Uniform Electronic Transactions Act (1999)
- ESIGN Act - Electronic Signatures in Global and National Commerce Act (2000)
- etc

Understanding the Basic security properties of digital signatures

Signer authentication

- Proof of who actually signed the document. i.e. digital signatures linking the user's signature to an actual identifiable entity.

Data integrity

- Proof that the document has not been changed since signing. The digital signature depends on every binary bit of the document and therefore can't be re-attached to any other document

Non-repudiation

- The signer should not be able to falsely deny having signed their signature. That is, it should be possible to prove in a court that the signer in fact created the signature.



Looking again & applying 'Digital Signature' properties to AdES

Advanced Electronic Signatures are:

- Uniquely linked to the signer Yes if through a “unique” public/private key pair.
- Capable of identifying the signer Yes through a certificate containing the public key
- Created using means that the signatory can maintain under their sole control Yes but dependent on the platform 'Signing' the document. (e.g. Adobe Acrobat, SigningHub etc.)
- Linked to the data to which it relates in such a manner that any subsequent change of the data is detectable Yes, but dependent on the platform 'Verifying' the document. (e.g. Adobe PDF reader, SigningHub etc.)

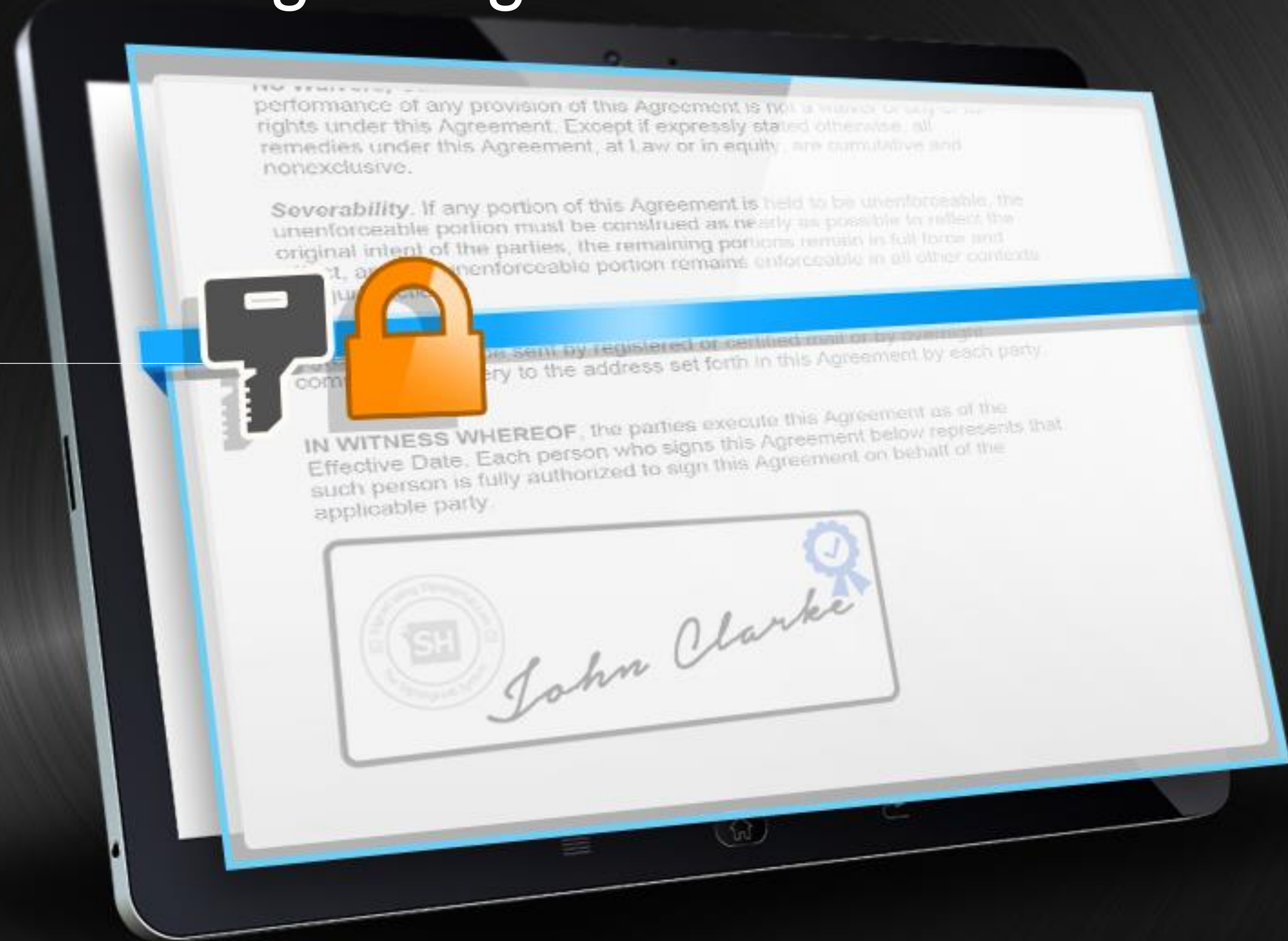
E-Signatures with witness digital signatures



After e-signing, the whole document is digitally signed using a central authority's private signing key

Properties:

- User authentication is not bound with the document (since user did not sign with their own key)
- Document cannot be changed without detection since its digitally signed by the corporate key



E-Signature with user's digital signature



After e-signing, John digitally signs the whole document using his private signing key

Properties:

- User's identity bound with the document (no one else can sign on behalf of this user)
- Document can't be changed without detection
- Signer can't deny having signed the document



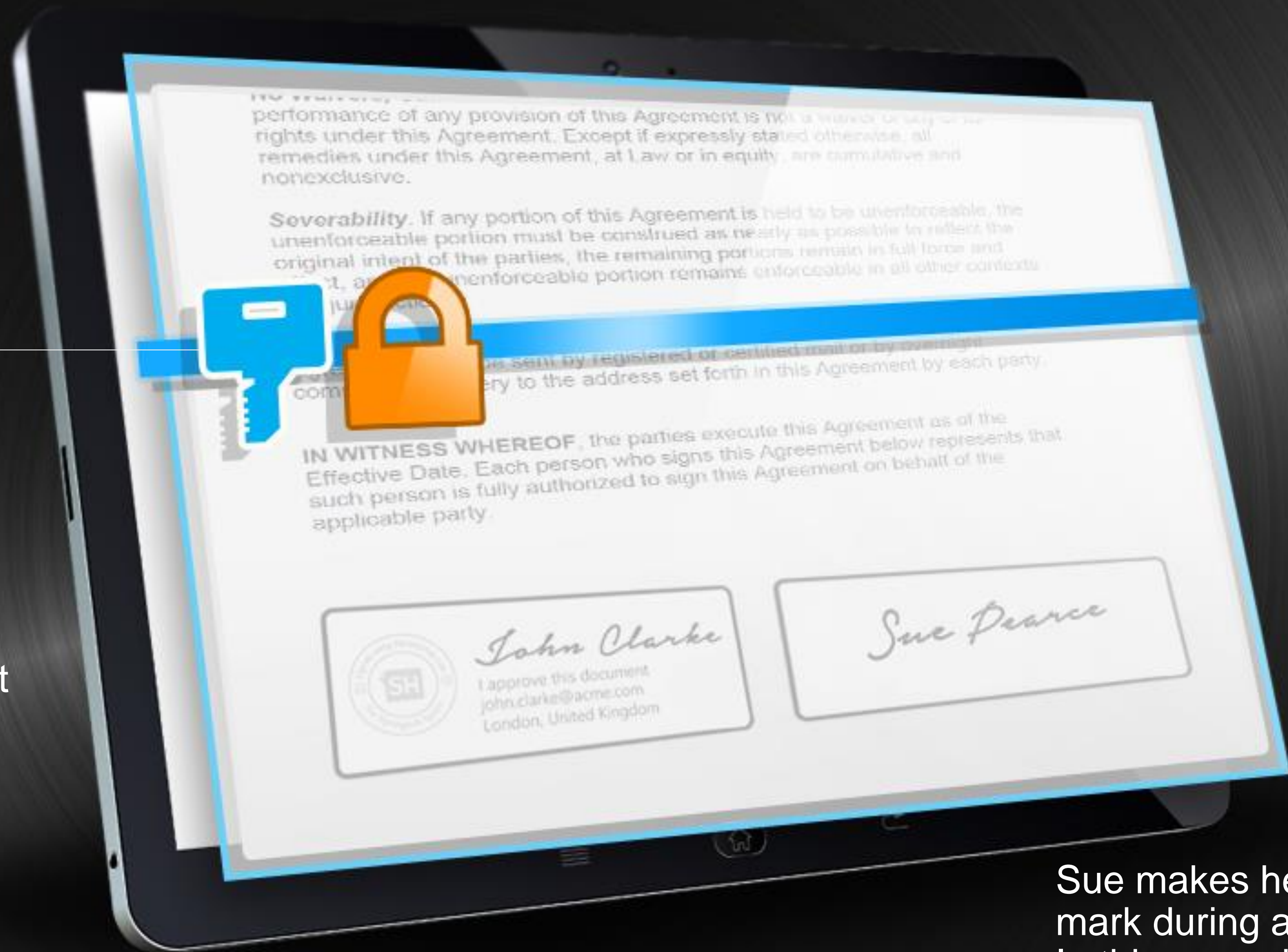
In-Person Signing



John witnesses the in-person signature with his own e-signature mark and digital signature

Properties:

- John's identity bound with the document
- Document can't be changed without detection
- Additional information in the document may indicate who the in-person signer was



Sue makes her e-signature mark during a live meeting. In this case she is not registered on the system

Where to hold user signing keys?

> **Locally**

- > Smartcard/USB token – strong security but complex for user & costly
- > Software container – security issues

> **Centrally**

- > ideal for signing on any device, anywhere
- > Using keys protected by an HSM, or using keys held in an encrypted DB

> **Mobile** (the future)

- > Software apps
- > Secure hardware elements

Support all the options, let the business, security & regulatory requirements decide which is best for the use case!



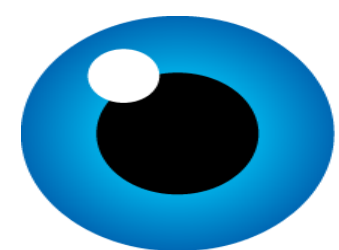
Long-term verification

- Documents need to be verified 10, 20, 30+ years...sometimes indefinitely!
- At the time of verification, certificates will be expired, certificate status information will no longer be available
- Cryptographic algorithms will have weakened since signing and may no longer be trusted!

Use long-term verifiable signature formats which can be extended over time with fresh evidence (PAdES Part 4 and XAdES-A formats)



Alternative workflows for Signing



GlobalSign®
GMO INTERNET GROUP



IDENTITY PROVEN
TRUST DELIVERED

What a Notary needed circa 2007 – 2014 (plus knowledge)

Signature Capture Device



LAN



Scanning of Originals



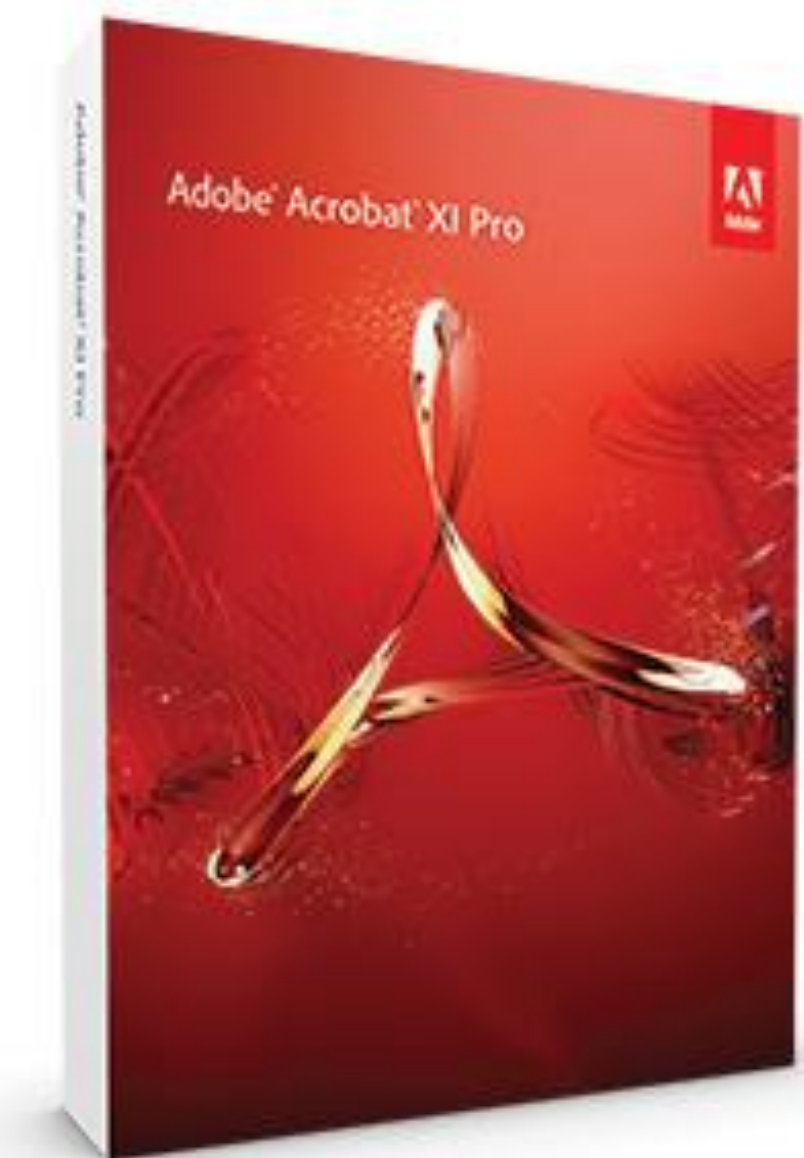
Laptop



**Signing Keys
(linked to the
identity
Certificate)**



**E-mail
clients...**



**PDF manipulation
and signing**

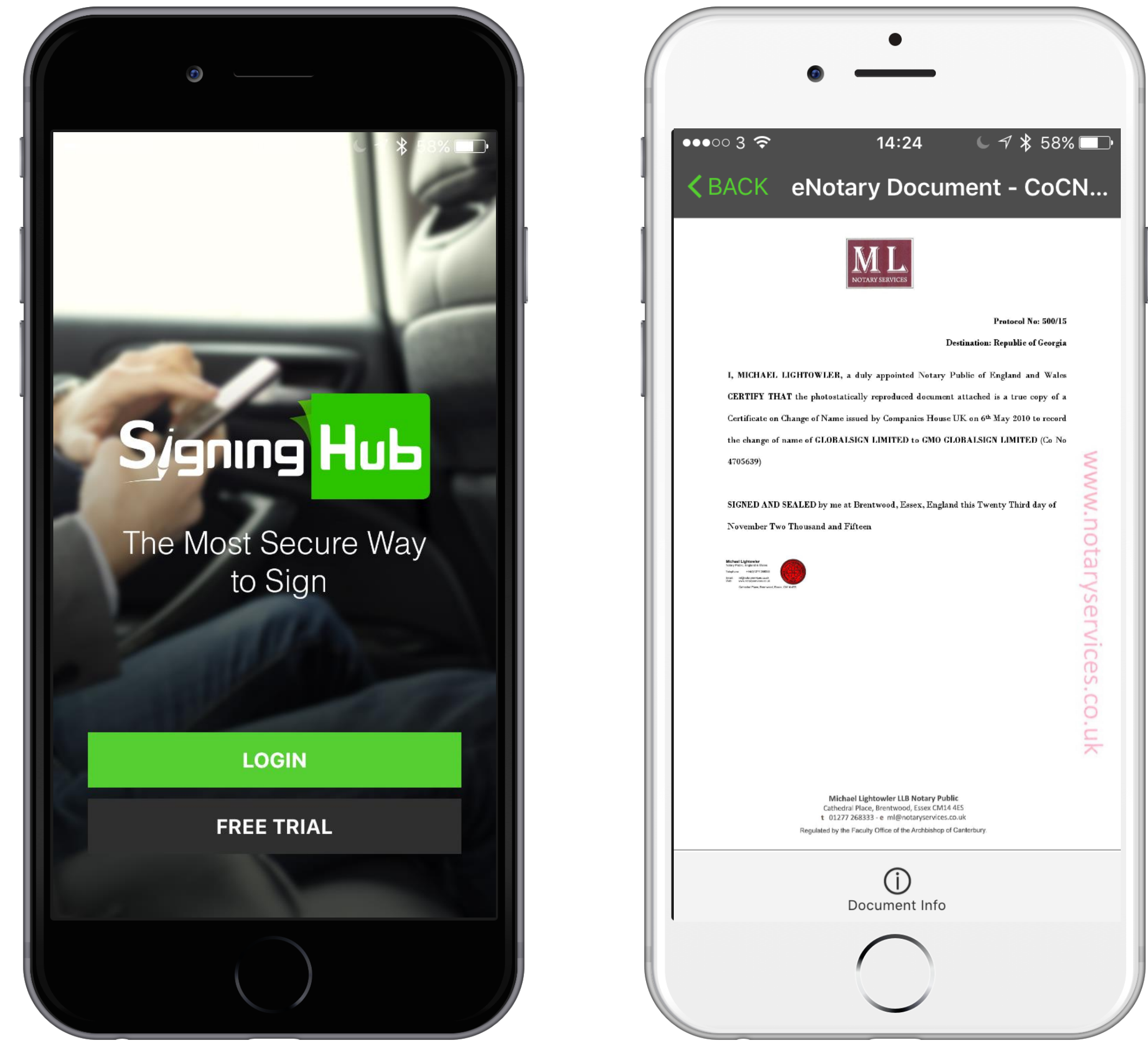
What a Notary needs in 2016 – A SigningHub Account & Phone..

Cloud Based Signing Service (SigningHub)

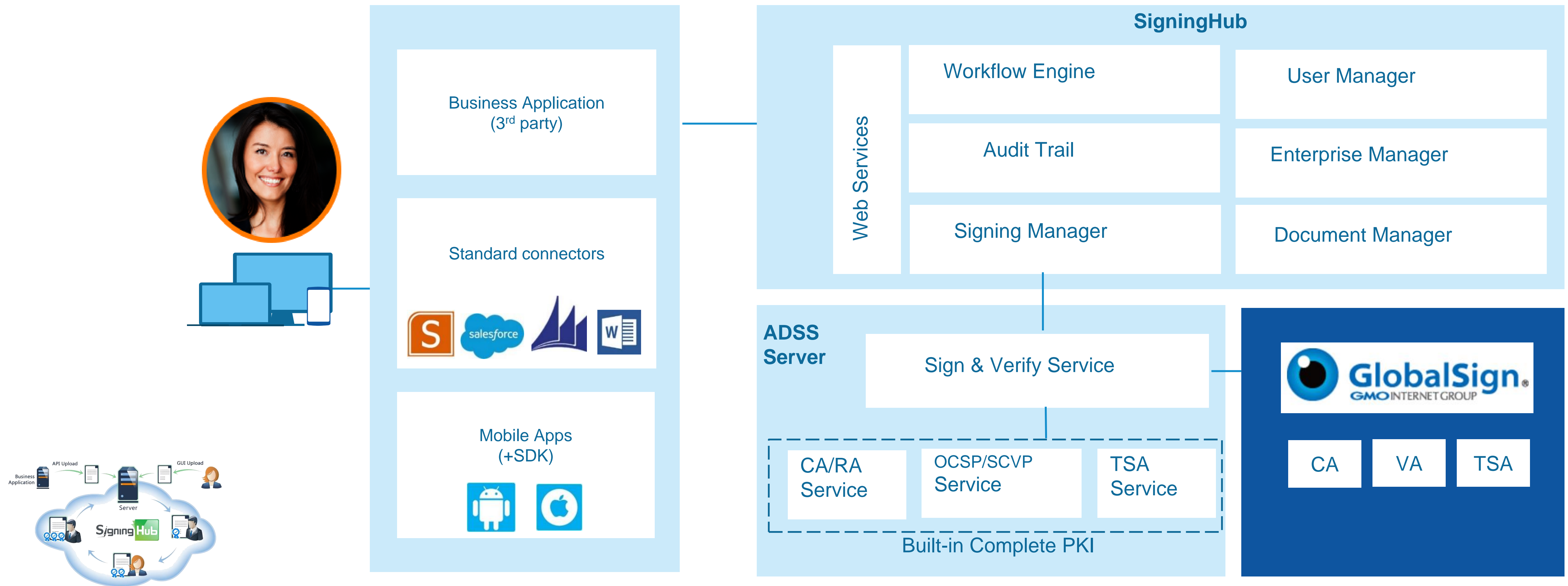
- PDF conversion (All major formats)
- Key Storage (Azure Key Vault)
- Digital Certificates for Signing (GlobalSign)
- Optional Electronic / In person signing options
- Public/Private Cloud options allowing confidentiality or closed loop control (Addressing PII Concerns)
- Automated Allocation of Digital Certificates to Notaries by the Competent Authority.

iPad/iPhone (or equivalent smartphone).

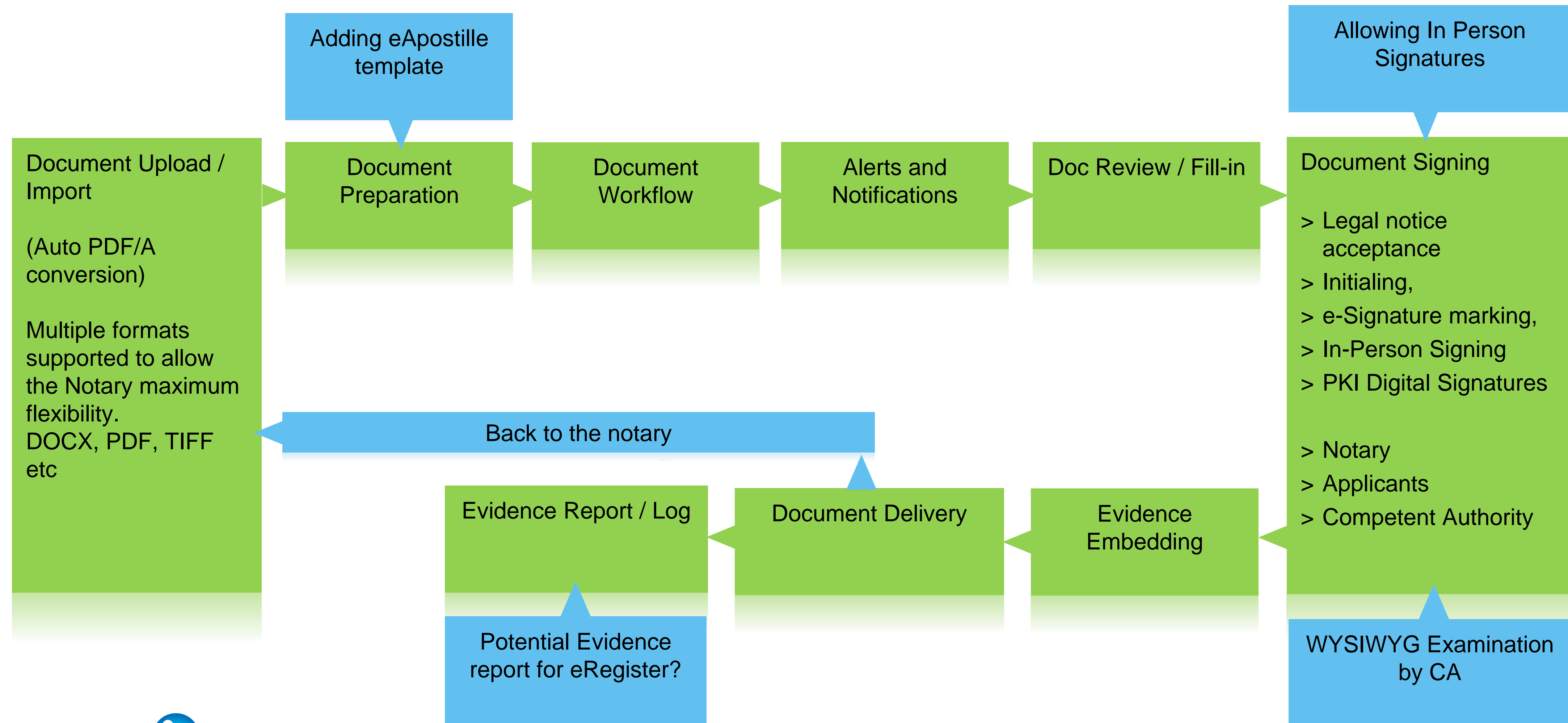
- Hi resolution camera for document scanning.
- 3G or 4G Connection or Wifi / Hotspot.
- Optional stylus or pen for signing on some models



What a Competent Authority can now implement in 2016...



What a Competent Authority can achieve in 2016...



Thank you for your attention. Please direct questions to:-

steve.roylance@globalsign.com

