



Demystifying e-signatures: legality, trust & digital identity

John Jolliffe | Sr. Manager Strategic Development

Lorie Groth | Sr. Technical PMM Adobe Sign, Enterprise



Key take-aways

1

Understanding the legal effects of e-signatures is critical

2

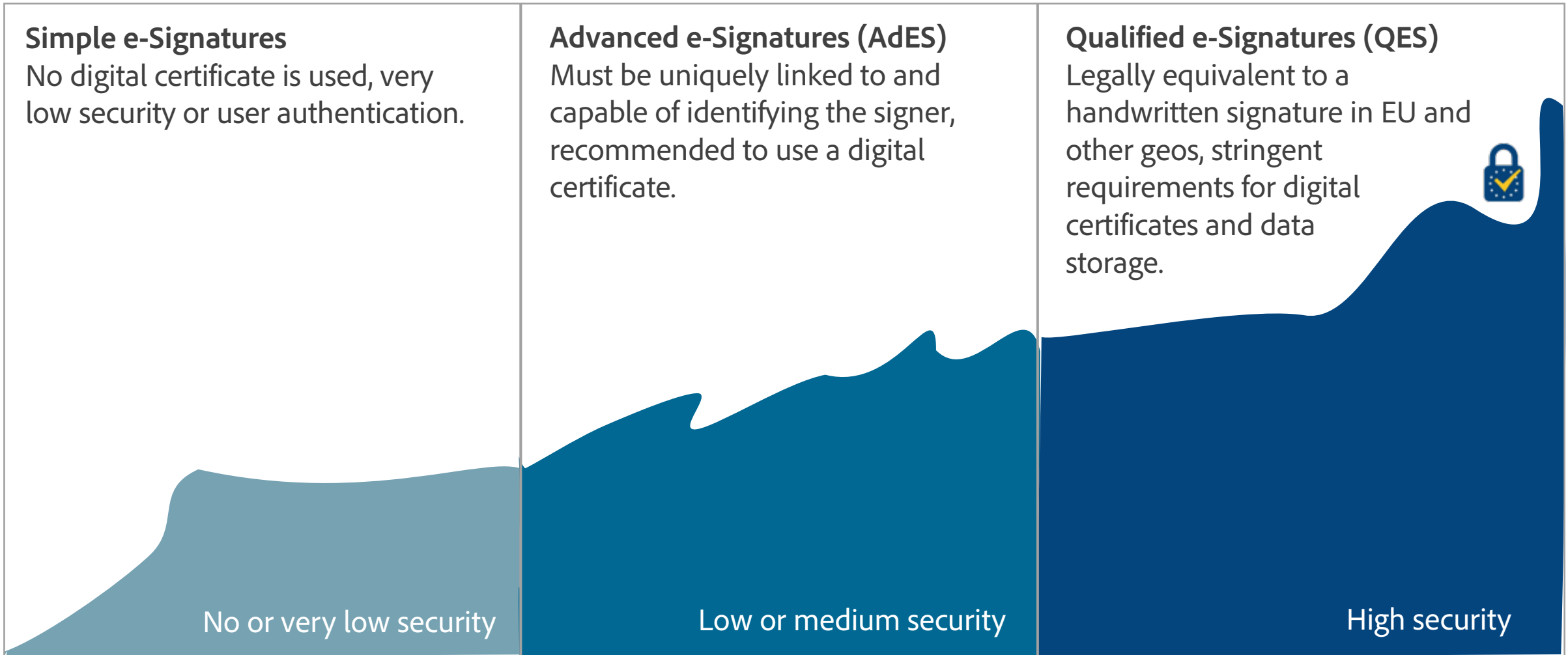
Key considerations for managing e-signature risk

3

Why identity assurance is so important

Understand the different types of e-signatures

Many jurisdictions share a similar approach to e-signature definitions and legal validity .



What type of e-signature should you use?

RISK

What consequences if a signature is challenged?

AUTHENTICATION

Who signed?

INTENT

Did they demonstrate intent to sign?

PROOF of SIGNING

What did they sign?

CONSENT

Did they consent to do business electronically?

EXCLUSIONS

Are there any excluded document types?

Demystifying e-Signature Legality

The rules on which signature types are allowed in different situations are defined on a country by country basis.



Argentina



Australia



Austria



Bangladesh



Belgium



Brazil



Bulgaria*



Cambodia



China



Colombia



Denmark



England



France



Germany



Greece



Hong Kong



Hungary



India



Indonesia



Ireland



Israel



Italy



Japan



Kuwait



Luxembourg



Malaysia



Mexico



New Zealand



Netherlands



Norway



Philippines



Portugal



Romania



Saudi Arabia



Singapore



South Africa



South Korea



Spain



Sweden



Switzerland



Taiwan



Thailand



Turkey



UAE



USA



Ukraine



Vietnam



Wales

*Guide coming soon.

Beyond legality, considering security and risk.

- What is the risk appetite of your organisation? Or the department?
- What is the difference between signer verification, authentication, and authorization?
- Are all digital certificates equal?



Identity fraud is not new, it's just gone digital.

The New York Times

5 Indicted in Identity Theft Scheme That Bilked Millions From Veterans

The defendants obtained Social Security numbers and bank account information from a technician who worked for the military, the Justice Department said.

BBC

'Having my identity stolen cost me £10,000'

THE LOCAL 

Identity fraud in France: Tourists inundated with speeding tickets after renting car



E-signature trust is (roughly) based on 3 parts

Security

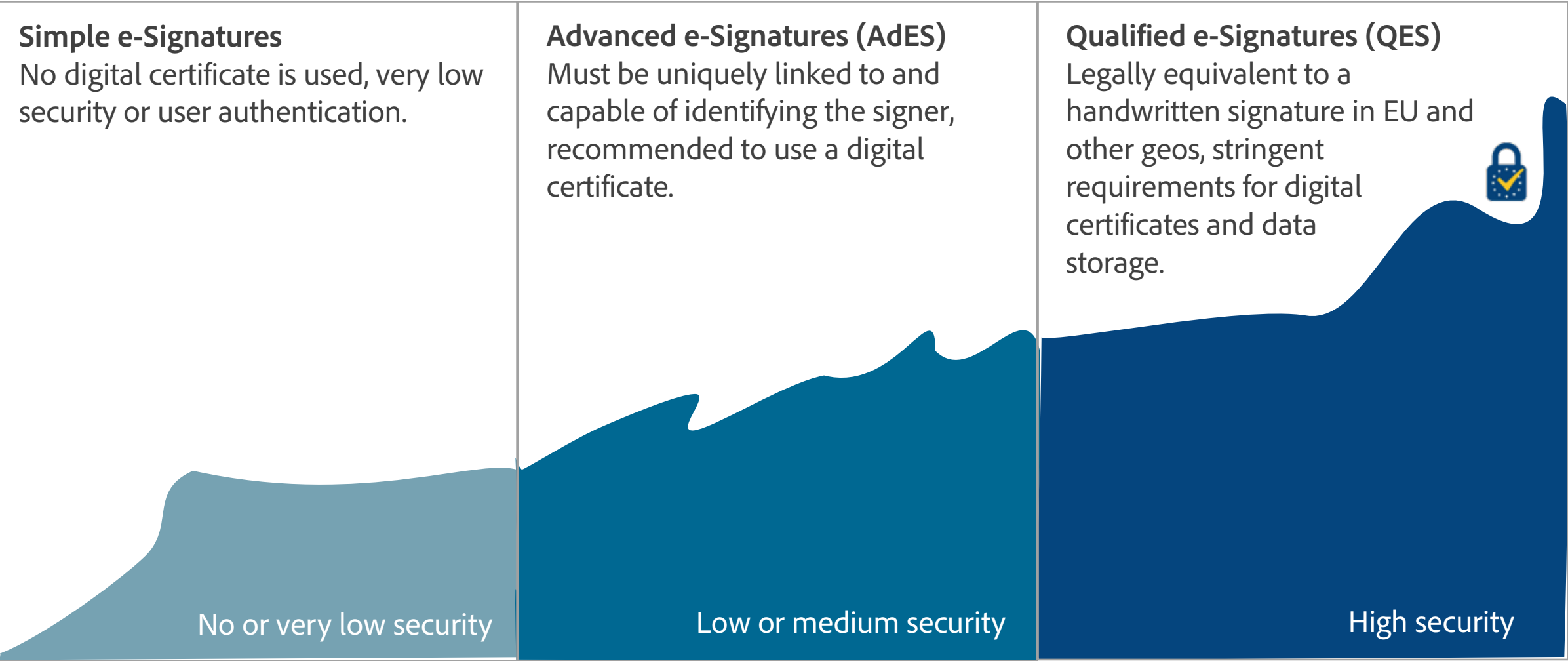
Industry Standards

Identity Assurance



eIDAS: also a baseline for e-signature security

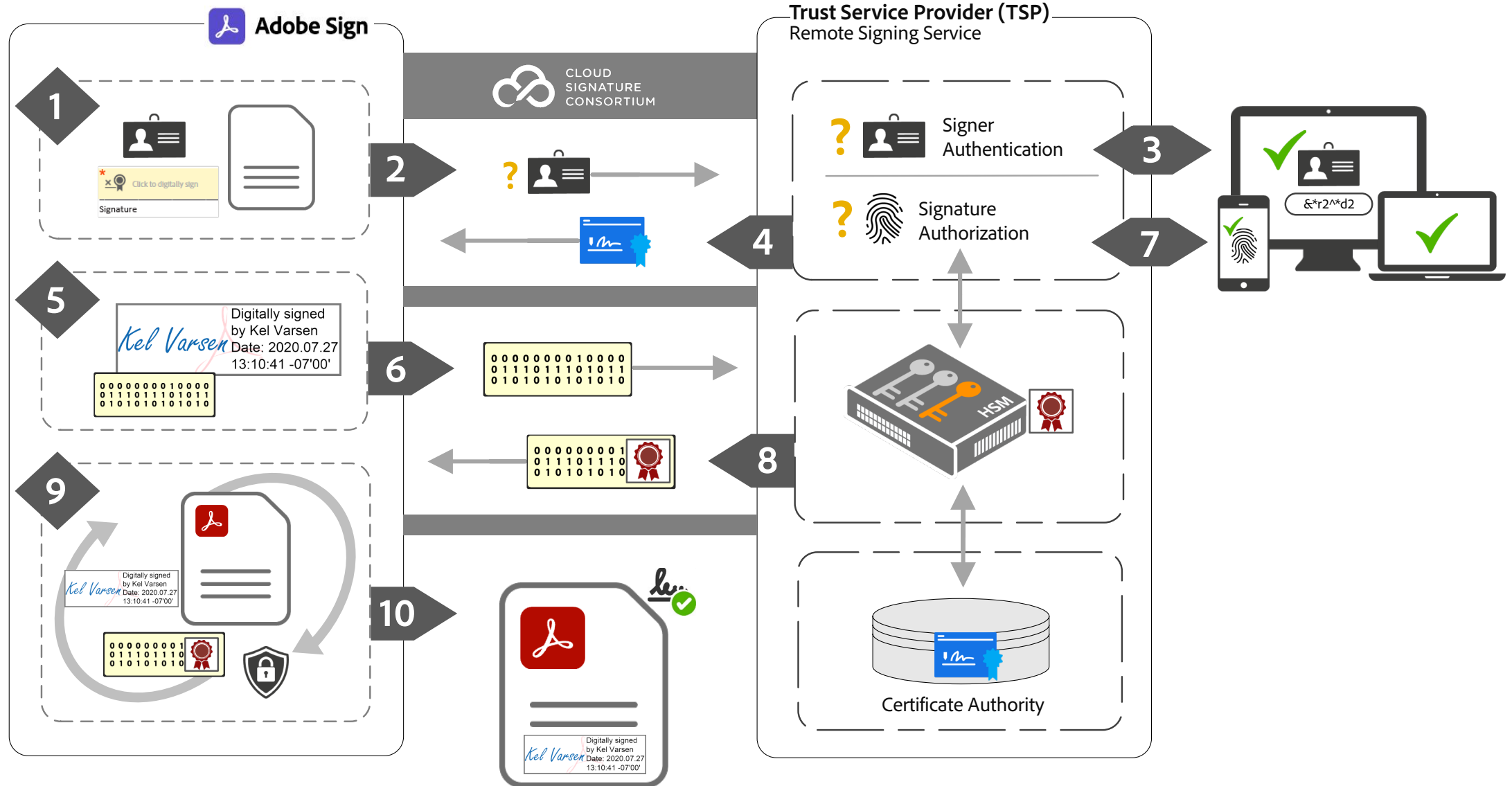
The EU's eIDAS Regulation has become the global baseline for e-signature quality, with many markets adopting eIDAS-inspired definitions and use of digital certificates for identity assurance.





Cloud Signatures

How they work with the CSC standard (ETSI TS 119 431)



Compliance backed by industry standards

Adobe Sign cloud signatures allow for flexible, compliant, remote signing backed by leading trust service providers (TSPs) and electronic identities (eIDs) around the world for flexible, compliant, remote signing.



eIDs



NEM ID



TSPs



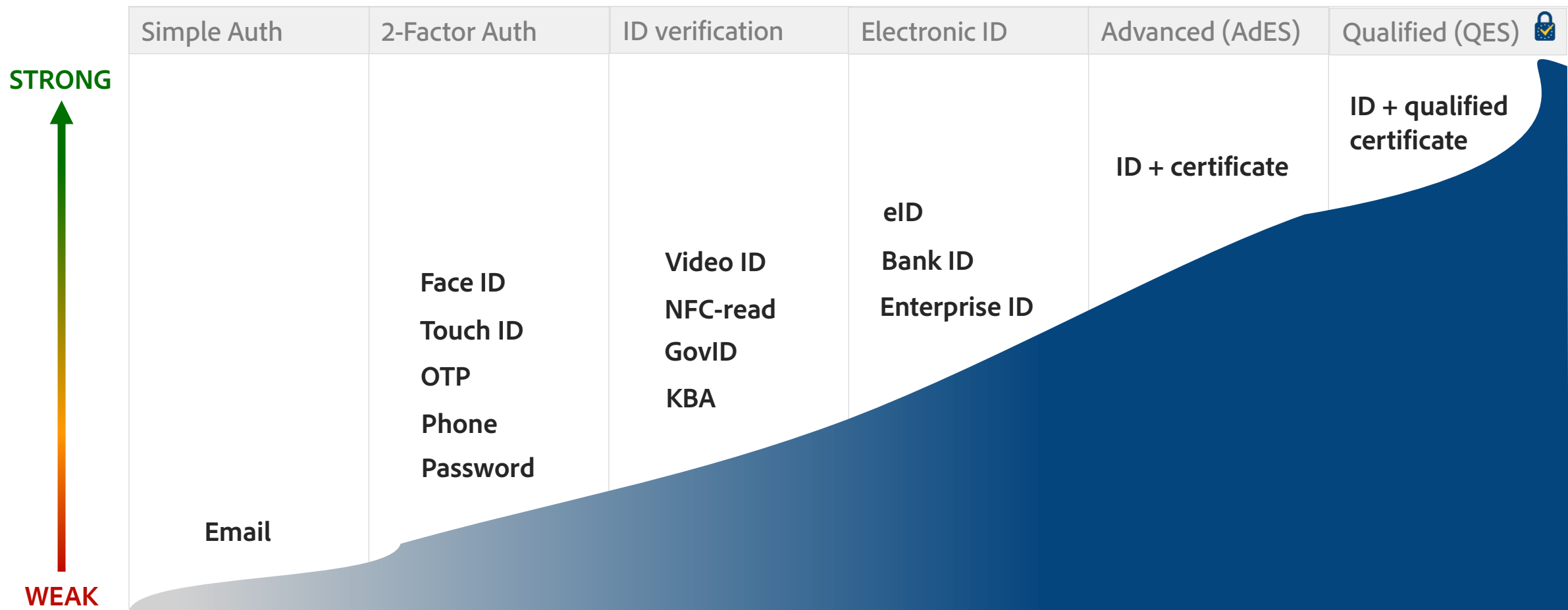
Ein Unternehmen der Bundesdruckerei



SEIKO

Identity assurance methods

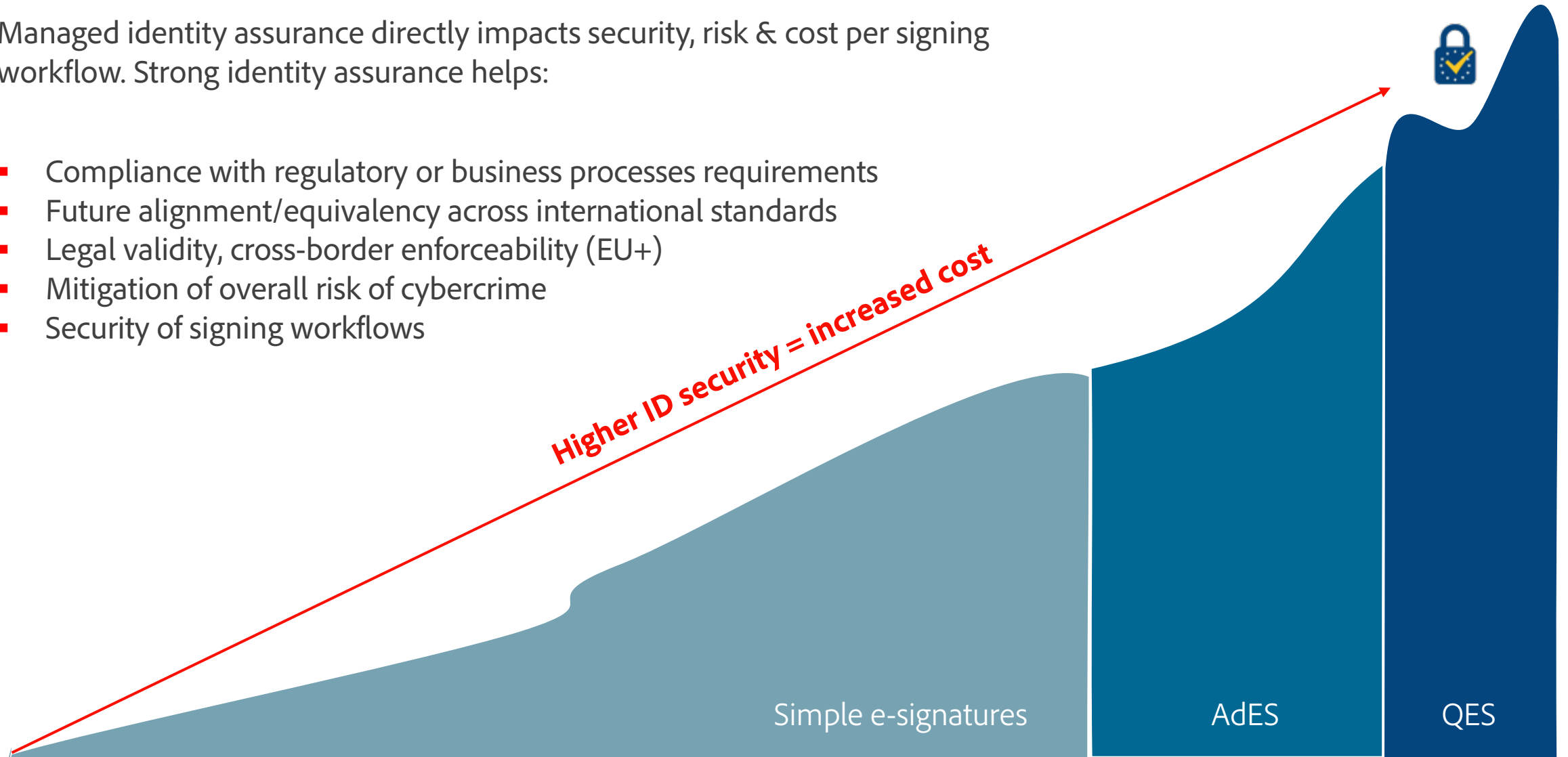
The following spectrum shows identity verification methods per security assurance level. Identity verification methods are often combined to increase strength or comply with legal requirements.



Why strong identity assurance is so important.

Managed identity assurance directly impacts security, risk & cost per signing workflow. Strong identity assurance helps:

- Compliance with regulatory or business processes requirements
- Future alignment/equivalency across international standards
- Legal validity, cross-border enforceability (EU+)
- Mitigation of overall risk of cybercrime
- Security of signing workflows





Legal compliance

Security

Industry standards

ID assurance

