ascertia
Tinexta Infocert

ASIA DIGITAL TRUST SUMMIT 2026 | COLOMBO

Remote Signing Across Borders:

Standards for Global Interoperability

Fábio Rego

Business Solutions and Compliance Lead, Ascertia | Co-Chair, Advocacy Committee, Cloud Signature Consortium

A Real Case: Genuine Documents, Forged Stamps

Portugal, 2026: Nepali workers applying for residence submitted real police clearance certificates carrying forged embassy stamps.

1 Genuine certificate
Nepal Police issues a real police clearance certificate

→

2 Paper legalisation
No Nepali embassy in Lisbon yet, so attestation went through embassies in New Delhi

→

3 Intermediaries
Brokers charged about €150 to €200 and returned forged embassy stamps

→

4 Detected by AIMA
Forged stamps found in residence permit review. Deportation proceedings followed

The impact

- Over 2,000 people affected, by the Nepali Embassy in Lisbon's count
- Victims of fraud first treated as misuse of the immigration system
- June 2026: after review, AIMA let nearly 2,000 apply again

What digital trust would have changed

- A certificate sealed by the issuing authority can be checked at source, by anyone, in seconds
- No paper stamp chain, so no market for brokers selling fake stamps
- But only if the receiving country can validate the seal. Today it cannot

Lesson: the documents were real. The weak link was paper authentication. Recognised digital seals remove it.

ascertia Tinexta Infocert © Ascertia. All rights reserved.

Trust Stops at the Border

Scenario: a document digitally signed in Sri Lanka is presented in the EU.

1 Signed in Sri Lanka
A company signs with a LankaSign certificate under the National Certification Authority root

→

2 Presented in the EU
Submitted to a bank, court or public authority in a Member State

→

3 Validator checks
No EU or third-country trusted list contains the Sri Lankan root. No path to a trust anchor

→

4 Result
Status INDETERMINATE under ETSI EN 319 102-1. Not qualified, no legal presumption

Legal effect in the EU

- Admissible as evidence: not denied effect solely because it is electronic (eIDAS Arts. 25(1), 35(1))
- No equivalence to a handwritten signature, no presumption of integrity and origin (Arts. 25(2), 35(2))
- Each bank, court or authority decides alone, and carries the risk

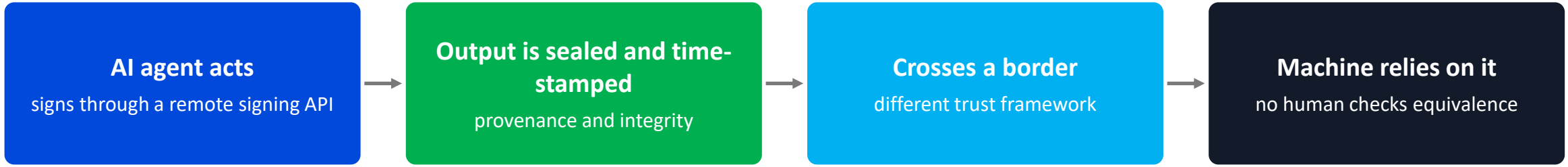
What happens in practice

- Back to paper: print, attest, legalise through the Ministry of Foreign Affairs and the embassy, translate
- Legalisation certifies an official's signature on paper. It does not make the digital signature verifiable
- The same gap runs in reverse: an EU qualified signature in Sri Lanka is assessed case by case under the ETA

Why: 0 Article 14 acts for any third country | 0 Sri Lankan providers on any EU trust list | 0 enactments of the UNCITRAL Model Law

ascertia Tinexta Infocert © Ascertia. All rights reserved.

Why an AI-Driven Economy Raises the Stakes



Machine-readable legal status

An automated relying party cannot weigh foreign law. It needs a trusted list entry that says what a signature or seal is worth.

Seals and time stamps as AI provenance

Qualified e-seals and time stamps give organisations a way to stand behind machine-generated outputs and agent actions.

Mandates and attributes

Wallet attestations can prove who an agent acts for and within which limits. They need recognition too.

Post-quantum fragmentation

Staggered national PQC migrations can split recognition before the cryptography fails. Build algorithm agility into recognition criteria.

© Ascertia. All rights reserved.

Remote Signing: Where Cross-Border Trust Is Decided

The key sits in an HSM at the provider, not on a card in the signer's hand. Trust now depends on how that service is run and proven.

1 Identity proofing
Signer verified once, remotely or in person (ETSI TS 119 461)

→

2 Signer authorises
Strong authentication on a phone produces Signature Activation Data

→

3 Key used in the HSM
The activation module checks that data: sole control at SCAL2 (CEN EN 419 241)

→

4 Relied on abroad
An AdES signature validated against the trust list of the provider's country

The standards stack

- Interface: CSC API v2 and ETSI TS 119 432 protocols for remote signature creation
- Service: ETSI TS 119 431-1 and -2 (server signing policy and AdES creation)
- Devices: CEN EN 419 241-1/-2 (server signing, SCAL2) and EN 419 221-5 (HSM)

Why it matters across borders

- Signer, key and relying party can sit in three different countries
- EU: managing remote QSCDs is now a qualified service (eIDAS Art. 29a); IR (EU) 2025/1567 applies from 19 Aug 2027
- Sole control has to be shown by evidence a foreign assessor can audit, not assumed

Key point: remote signing makes the signature portable. Shared standards make its trust portable.

ascertia Tinexta Infocert © Ascertia. All rights reserved.

Digital Credentials: The Next Thing That Must Cross Borders

Identity, qualifications and mandates are moving into wallets. Their value depends on acceptance abroad.

Person ID | **Mobile driving licence** | **Diplomas** | **Professional qualifications** | **Company attestations** | **Powers of attorney** | **Agent mandates**

European Union

- EUDI Wallets in every Member State by end 2026
- Qualified attestations of attributes: same legal effect as paper (Art. 45b)
- Qualified status recognised in all Member States (Art. 24a)

Sri Lanka

- SL-UDI national digital ID, built on open-source MOSIP
- First IDs to a selected cohort from end 2026; e-KYC for remote onboarding
- Recognition today is domestic only

Common standards

- ISO/IEC 18013-5 mobile driving licence
- W3C Verifiable Credentials
- OpenID for Verifiable Credentials
- ETSI TS 119 602 lists of trusted issuers

First cross-border tests: EU–Japan wallet pilot exchanging academic records (2026); Ukraine's Diia wallet tested in EU wallet pilots.

The gap: a qualified attestation is valid across the EU. Nothing yet says when a Sri Lankan diploma or licence in a wallet must be accepted abroad, or the reverse.

ascertia Tinexta Infocert © Ascertia. All rights reserved.

What Mutual Recognition Actually Requires

Recognition is an assessment of four layers. Technical compatibility alone is not enough.

1 Legal framework

- Legal effect of signatures, seals, time stamps
- Qualified status and presumptions
- Liability and data protection

2 Supervision and audit

- Independent supervisory body
- Accredited conformity assessment
- Breach reporting and termination plans

3 Technical standards

- Policy and security requirements
- Certified signature creation devices
- AdES formats and validation rules

4 Trust representation

- Machine-readable trusted list
- Signed, published, kept current
- Consumable by validation services

The test: functional equivalence, shown by legal and practical evidence. Not textual identity with the other side's law.

ascertia Tinexta Infocert © Ascertia. All rights reserved.

The EU Legal Route: Article 14 eIDAS

Regulation (EU) No 910/2014, as amended by Regulation (EU) 2024/1183

Effect: third-country trust services are recognised as legally equivalent to EU qualified trust services (Art. 14(1)).

Route A Commission implementing act

- New with eIDAS 2 (2024)
- Adopted under the examination procedure
- Unilateral: no reciprocity condition in the text
- Can also cover international organisations

Route B International agreement

- Concluded under Article 218 TFEU
- Council decision, Parliament consent
- Reciprocity: EU qualified services must be recognised in the third country (Art. 14(3))
- The only route available from 2014 to 2024

Both routes (Art. 14(2)): the third country must meet EU qualified requirements and establish, maintain and publish a trusted list of recognised providers.

ascertia Tinexta Infocert © Ascertia. All rights reserved.

Five Lessons from the European Experience

1 Listing is not recognition

Ukraine (2023) and Moldova (2025) are on the EU third-country trusted list. Their signatures validate, but are not qualified.

2 Legacy is the hidden cost

EU4Digital: "even minor technical adjustments to the legacy may require much more effort than expected."

3 Supervision is the bottleneck

Accredited conformity assessment and certified signature devices are the hardest gaps to close.

4 Start unilateral, converge later

Ukraine and the UK recognise EU qualified services; Latvia gives listed Ukrainian QES handwritten effect (2026).

5 Evidence beats text

Assessors need audit reports, supervision records and test results, not only statutes.

ascertia Tinexta Infocert © Ascertia. All rights reserved.

Beyond Europe: Where Other Frameworks Stand

Instrument	Status (Nov 2026)	What it does for recognition
UNCITRAL Model Law on IdM and Trust Services (2022), Arts. 25 to 26	No reported enactments	Recognise foreign services offering a substantially equivalent level of reliability
UN Electronic Communications Convention (2005), Art. 9(3)	In force; Sri Lanka a party since 2015	Functional equivalence for e-signatures in international contracts; no provider recognition
CPTPP Art. 14.6; DEPA Module 7	In force	Encourage interoperable e-authentication and digital identity
EU–Singapore Digital Trade Agreement, Art. 10	In force (Feb 2026)	Non-discrimination of e-signatures; encourage interoperable e-authentication
EU–Korea Digital Trade Agreement, Art. 10	Signed (June 2026)	Adds voluntary cooperation to encourage mutual recognition of e-signatures
EU–Japan cooperation on digital identity and trust services (2024)	Active	Wallet pilots; 2026 talks on mutual recognition of signature providers
ASEAN DEFA	Concluded May 2026; signing due at the 49th ASEAN Summit (Nov 2026)	Regional anchor for digital ID and e-signature interoperability

Pattern: trade agreements commit parties to encourage interoperability. None of them recognises a single certificate.

© Ascertia. All rights reserved.

Sri Lanka: Strong Foundations, No Bridge Yet

Electronic Transactions Act No. 19 of 2006, amended by Act No. 25 of 2017 to give effect to the UN Electronic Communications Convention

What the law already provides

- Technology-neutral signature test: as reliable as appropriate, or proven in fact (s. 7)
- Courts presume the genuineness of an electronic signature unless the contrary is proved (s. 21(3))
- Contracts formed by automated message systems are valid (s. 17(d))
- Sri Lanka CERT designated Certification Authority (2019); LankaSign authorised CSP
- CSP criteria may cover biometric and other authentication methods (ss. 19(da), 24(2)(da))

What would build the bridge

- Regulations on recognising foreign providers, using the existing power in s. 24(2)(g)
- A trusted list of authorised CSPs in ETSI TS 119 612 format
- A remote signing profile referencing CEN EN 419 241 and ETSI TS 119 431
- SL-UDI identity proofing feeding certificate issuance, aligned with ETSI TS 119 461

Design choice: Sri Lanka's flexible, Convention-based test is an asset. A published trusted list and a remote signing profile would make it legible to EU and ASEAN validators.

© Ascertia. All rights reserved.

Remote Signing Across Borders: Five Principles

1 Publish machine-readable trust	Trusted lists in ETSI TS 119 612 (and TS 119 602 for credential issuers), signed and current.
2 Recognise outcomes, not texts	Map reliability and assurance levels. Use the UNCITRAL "substantially equivalent" test as the benchmark.
3 Converge on formats and APIs	AdES baseline profiles with long-term validation, RFC 3161 time stamps, and the CSC API for remote signing.
4 Make supervision and sole control legible	Accredited conformity assessment (ETSI EN 319 403-1), published audit attestations, SCAL2 evidence for remote signing.
5 Validate against many anchors	Validation services that load several trust lists and report legal status per jurisdiction.

ascertia Tinexta Infocert © Ascertia. All rights reserved.

ascertia
Tinexta Infocert

QUESTIONS AND DISCUSSION

Thank you

Fábio Rego fabio.rego@ascertia.com

Head Office – London
33 Queen Street
London
EC4R 1AP
Company No: 04207349
VAT No: GB 777 0072 22

UAE
Ascertia Software Trading L.L.C
Office No: 413
Nadd Hessa IT Plaza
Dubai Oasis Silicon, UAE
Phone: +971 (04) 5704760
P.O.BOX No: 418687
DED License No: 974535
TRN: 100443116700003

Singapore
531A Upper Cross Street #04-95
Hong Lim Complex
Singapore 051531

Pakistan
22 F, Near Main Market,
Gulberg II Lahore,
Pakistan, 54660
REGD. No: 12964/20030902