

Electronic Signature Law Comparison

ESIGN · UETA · eIDAS · PIPL — a cross-border reference table for 2026

Publisher: ABSign

Issued: 08 October 2026

Jurisdictions covered: 17

Source: primary legislation and regulatory guidance

General reference only — not legal advice.

How to read this table

The table compares, for each jurisdiction, the primary statute governing electronic signatures, the year it took effect, whether a simple electronic signature is valid for ordinary commercial agreements, the highest assurance tier the regime recognises, whether identity proofing is required to reach that tier, and how the regime treats cross-border recognition. Divergence between jurisdictions concentrates in three columns: identity proofing, the highest tier, and cross-border recognition.

Jurisdiction	Primary legislation	In force	Simple e-signature valid?	Highest assurance tier	Identity proofing required?	Cross-border recognition
United States (federal)	ESIGN Act	2000	Yes	No formal statutory tiers	No	Yes, for interstate and foreign commerce
United States (state)	UETA (49 states + DC, PR, USVI)	1999	Yes	No formal statutory tiers	No	Yes, within adopting states
European Union / EEA	eIDAS Regulation 910/2014	2016	Yes (SES)	QES (Qualified Electronic Signature)	Yes — qualified certificate + QSCD	QES recognised in all Member States
European Union (next phase)	eIDAS 2.0 · Regulation (EU) 2024/1183	2024–2026	Yes (SES)	QES + EUDI Wallet	Yes	EUDI Wallet to be offered by Member States by 2026
United Kingdom	Electronic Communications Act 2000; UK eIDAS	2000 / 2019	Yes	QES	Yes	UK QES recognised domestically
China (mainland)	Electronic Signature Law (amended 2015, 2019)	2005	Yes, if a "reliable electronic signature"	CA-issued certificate-based signature	Yes — real-name verification	Recognised subject to reciprocity arrangements
China (mainland, data rules)	PIPL · DSL · CSL	2017–2021	n/a	n/a	Separate consent; cross-border transfer needs CAC assessment, standard contract or certification	Restricted outbound transfer of personal data
Hong Kong, China	Electronic Transactions Ordinance (Cap. 553)	2000	Yes	Digital signature with recognised certificate	Yes, for recognised certificates	Recognised certificate regime
Singapore	Electronic Transactions Act 2010 (amended 2021)	1998 / 2010	Yes	Secure electronic signature	No statutory requirement	Adopted UNCITRAL MLETR for electronic transferable records
Japan	Act on Electronic Signatures and Certification Business	2001	Yes	Specified certification services	Only where the parties require it	No statutory barrier
South Korea	Framework Act on Electronic Documents and Electronic Transactions	1999 (as amended)	Yes	Certified electronic signature (now voluntary)	Only for certified signatures	No statutory barrier

Jurisdiction	Primary legislation	In force	Simple e-signature valid?	Highest assurance tier	Identity proofing required?	Cross-border recognition
Germany	eIDAS + BGB § 126a; FormAnpG	2016	Yes, unless stricter form is mandatory	QES	Yes	QES recognised EU-wide
France	eIDAS + Code civil arts. 1366–1367	2000 / 2016	Yes	QES	Yes	QES recognised EU-wide
Canada	PIPEDA Part 2 + provincial Acts (e.g. Ontario ECA)	2000	Yes	Secure electronic signature	Provincial rules vary	No federal barrier
Australia	Electronic Transactions Act 1999	2000	Yes	No formal statutory tiers	No	No federal barrier
India	Information Technology Act 2000 (amended 2008)	2000	Yes	Digital Signature Certificate (CCA-licensed)	Yes, for DSC	No statutory barrier
UNCITRAL (cross-border framework)	MLEC 1996 · MLES 2001 · MLETR 2017	1996–2017	Functional-equivalence principle	No tiers — sets the recognition test	n/a	Widely used as the basis for statutory recognition

What the comparison shows

Two conclusions follow from the table. First, the validity of a simple electronic signature is no longer seriously contested in any of the seventeen jurisdictions reviewed; the statutes are technology neutral and do not prescribe a signing method. Second, the differences that remain are not about validity but about evidence: whether identity must be proved, whether a certificate-based or qualified signature is needed for a given document class, and whether the document may lawfully be transferred to the destination jurisdiction.

Four frameworks in detail

ESIGN Act (US, 2000)

- Technology neutral — any electronic mark with intent to sign is valid
- No tiered assurance model; relies on consent and record retention rules
- Does not override wills, court orders or certain family and utility notices

UETA (US states, 1999)

- Model law adopted by 49 states plus DC, Puerto Rico and the US Virgin Islands
- Works alongside ESIGN; ESIGN pre-empts only where state law is inconsistent
- Excludes certain notices — cancellation of insurance, eviction, product recall

eIDAS (EU, 2014)

- Three tiers: SES, AES and QES
- QES has equivalent effect to a handwritten signature across the EU
- Being extended by eIDAS 2.0 with the EUDI digital identity wallet

PIPL (China, 2021)

- Governs personal data, not signature validity
- Separate consent required for sensitive personal data
- Cross-border transfer needs a CAC security assessment, standard contract or certification

Notes and limitations

1. A "simple" electronic signature (also called a standard or basic electronic signature) is broadly any electronic mark, sound or process adopted with intent to sign. It is the tier used by most day-to-day business agreements.
2. An advanced electronic signature (AES) is uniquely linked to the signer, capable of identifying them, created under the signer's sole control and linked to the data so that later changes are detectable.
3. A qualified electronic signature (QES) — the EU tier — is an AES created using a qualified certificate and a qualified signature creation device. In the EU it has the equivalent legal effect of a handwritten signature.
4. "Identity proofing" means the signer's identity is verified against an authoritative source before or during signing. It is not the same as authentication with a login credential.
5. This table is a general reference for commercial planning, not legal advice. Statutory details change and sector-specific rules (banking, healthcare, public procurement, court filings) may impose stricter requirements.

Practical decision checklist

- Identify every jurisdiction the document will be used in — the parties' jurisdictions and the governing law.
- Check whether the receiving authority (court, registry, regulator) imposes a stricter form requirement.
- Decide the assurance tier per document class, not per organisation.
- Decide the identity-proofing level: email possession, knowledge and device checks, or documentary proofing.
- Confirm whether notarisation, apostille or consular legalisation is required, and start that step early.
- Map the personal data in the template and pre-approve a cross-border transfer mechanism per destination.
- Define the retention period for the signed document, the identity evidence and the audit trail.