Electronic signatures and their acceptance around the world

Electronic signatures are broadly accepted throughout the world as an electronic replacement to handwritten signatures. Most laws define an electronic signature as electronic data that's logically associated with a document and used by the signer to indicate their agreement.

For most use cases, customers and locations, a 'simple' electronic signature is sufficient. However, some transactions in certain countries, in heavily regulated industries or with governmental entities may require or prefer digital signatures, a type of electronic signature that offers a heightened level of identity assurance and security.

United States

Electronic signatures have the same legal status as handwritten signatures throughout the United States, thanks to the E-Sign Act and the Uniform Electronic Transactions Act (UETA).

What is the E-Sign Act?
The E-Sign Act, signed by President Bill Clinton on June 30, 2000, granted electronic signatures the same legal status as handwritten signatures throughout the United States.

The E-Sign Act allows the contract to be used as evidence in a court of law and prevents the denial of legal effect, validity, or enforceability of an electronically signed document solely because it is in electronic form.

European Union

The Electronic Identification and Trust Services Regulation (eIDAS) makes any type of e-signature legal and enforceable.

eIDAS sets a foundation for all electronic signatures by asserting that no signature can be denied legal admissibility solely because it's in electronic form. This requirement can be met with typical e-signatures done on SpotDraft.

An "electronic signature" is defined (eIDAS Art 3-10) very broadly as "data in electronic form, which are attached or logically associated with other data in electronic form and which the signatory uses to sign."

An electronic signature is appropriate for most use cases, such as internal documents, business-to-consumer transactions or agreements with existing partners or signers. It's simple and has few requirements associated with it, making it an efficient form of e-signature for most agreements.

Singapore

In Singapore, the use of electronic and secure electronic signatures is governed by the Electronic Transactions Act, Cap 88 (ETA).
Under the ETA, electronic signatures are enforceable and admissible. Judges are

familiar with the laws surrounding e-records and e-signatures. Electronic signatures are widely accepted as evidence, and judges frequently cite the ETA in cases pertaining to signatures and contracts.

India

In India, electronic and certificate-based digital signatures are regulated by the Information Technology Act, 2000 (IT Act).

The IT Act distinguishes between electronic signatures and certificate-based digital signatures, but both have the same status as handwritten signatures under Indian law.

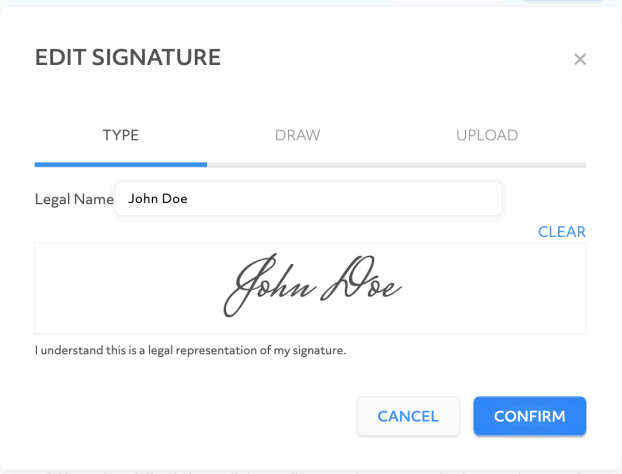
SpotDraft eSignature Compliance

The various measures undertaken by SpotDraft to ensure compliance of its e-signatures with various global e-sign laws include:

1. **Multiple Signing Methods** - When signing a document, users have an option to add their signature using multiple methods: draw, type, and upload.

   With this, to insert their signatures, users must also include an affirmation from the user which indicates that what they are inserting is a legal representation of their signature.

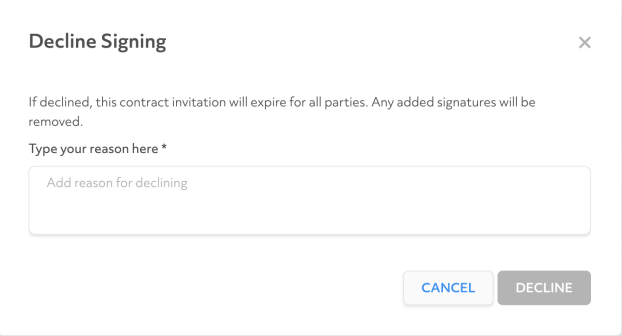
Figure 1 - Signature Modal



2. **Option to Decline to Sign** - As part of signing the document, users can also choose to Decline to Sign. Relevant product screenshots are below.

Figure 2 - Option to Decline

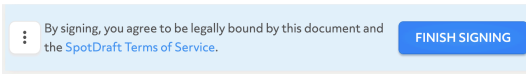
Figure 3 - Decline to Sign Modal



3. **Terms of Service Confirmation** -

   To finish signing the documents, users must agree to the SpotDraft Terms of Service, as shown below:

Figure 4: Terms of Service Confirmation



4. **Cryptographic Encryption** -

After a contract is executed on SpotDraft, we encrypt it using a Digital Signature Certificate (DSC) from an industry-leading provider known as Entrust.

As part of the list of AATL vendors, Entrust allows users to use Adobe Acrobat to verify if the document has been tampered with after execution. Relevant screenshots are below:

Figure 5: Signature Validation in Adobe

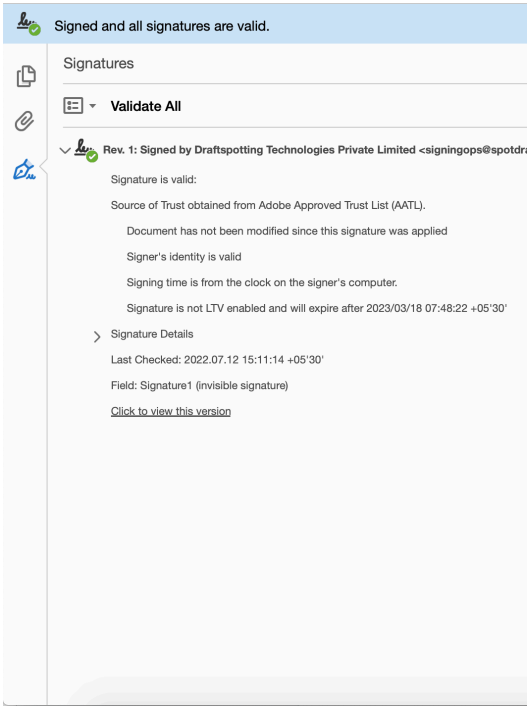


Figure 6: Signature Properties

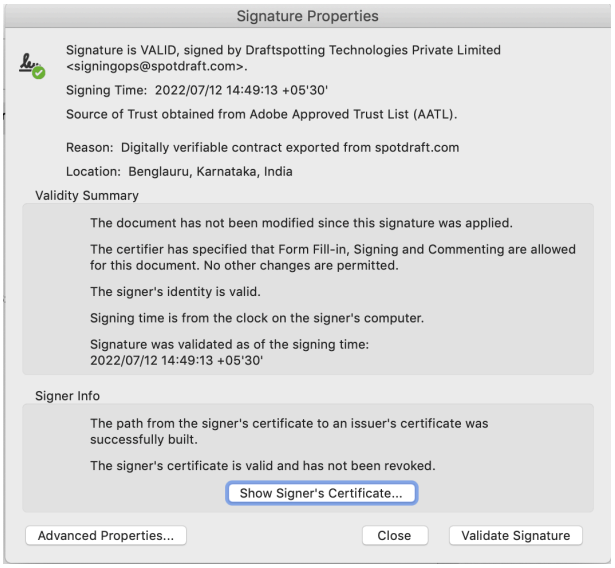
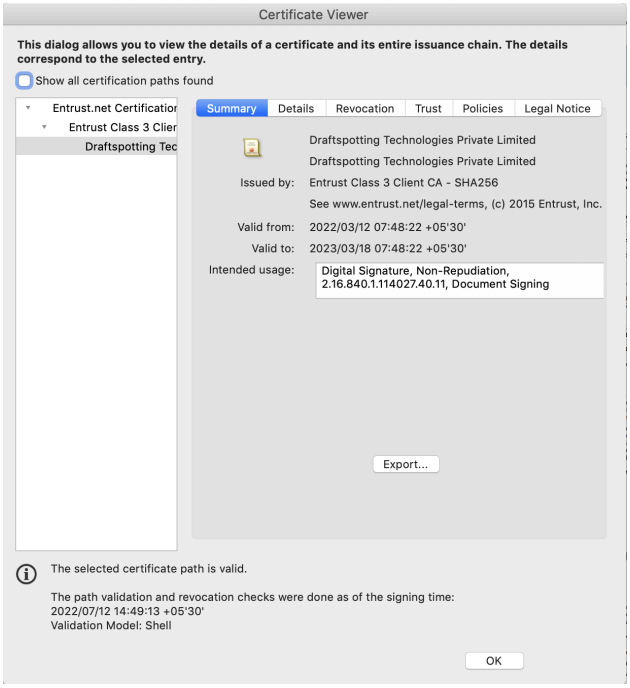


Figure 7: Validation from Entrust

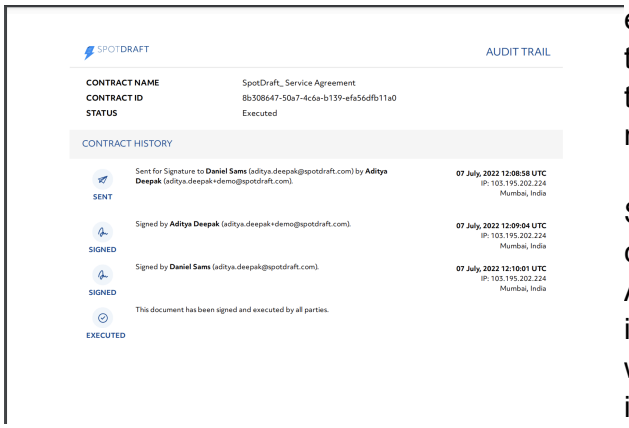


5. **Audit Trail** - During the signing, we include key actions on the platform that tracks key events as part of the signing workflow.

After a contract is executed, we also include a detailed Audit Trail that's

appended to the contract that tracks key information regarding the signing workflow. Please see below for an example:

Figure 8: Example Audit Trail


SPOTDRAFT

AUDIT TRAIL

CONTRACT NAME	SpotDraft_ Service Agreement
CONTRACT ID	8b308647-50a7-4c6a-b139-efa56dfb11a0
STATUS	Executed

CONTRACT HISTORY

SENT — Sent for Signature to **Daniel Sams** (aditya.deepak@spotdraft.com) by **Aditya Deepak** (aditya.deepak+demo@spotdraft.com). — **07 July, 2022 12:08:58 UTC** IP: 103.195.202.224 Mumbai, India

SIGNED — Signed by **Aditya Deepak** (aditya.deepak+demo@spotdraft.com). — **07 July, 2022 12:09:04 UTC** IP: 103.195.202.224 Mumbai, India

SIGNED — Signed by **Daniel Sams** (aditya.deepak@spotdraft.com). — **07 July, 2022 12:10:01 UTC** IP: 103.195.202.224 Mumbai, India

EXECUTED — This document has been signed and executed by all parties.

Conclusion

SpotDraft is a SaaS-based contract automation platform that provides and handles all aspects of the electronic signature process, from providing user validation options to sealing the document with a tamper evident certificate.

SpotDraft's native e-signature supports verification of identity through use of specific identifiers. For SpotDraft customers, all users have login credentials, while for external users, authentication is achieved by sending an email with unique links that contain tokens for a particular signatory. Since most signatories would have access to one email account, this is enough to authenticate and validate signatories.

The link sent to signatories have unique identifiers that are only pertaining to a specific transaction. After clicking on the link, signatories can choose to sign the agreement using different options (Draw, Type, or Upload).

After all signatories have completed signing, SpotDraft certifies and ensures that if there are any changes to the document, they can be easily traced and identified. This is achieved through document certification and it ensures that signatures on SpotDraft are non-repudiable.

SpotDraft allows step-by-step audit logs for complete visibility into the signature process. Along with this, SpotDraft collects signatory information like IP address, geolocation, along with the name and email address of users. This is captured in a secured audit trail that provides enough evidence of all signatures. Once a document is signed by all parties involved and agreement is marked 'Executed', the audit trail is appended to the document and shared with all parties involved.

SpotDraft is ISO27001 certified and is currently undergoing SOC2 compliance checks. Furthermore, SpotDraft's platform is hosted on Google Cloud Platform (GCP), therefore, data security and data integrity is at the highest level.

From a legal perspective, it can be concluded with confidence that SpotDraft is a trustworthy and secure platform for end-to-end contract automation, providing the ability to produce legally enforceable electronic signatures, as defined by nations globally.