Strong Legal Electronic Evidence

Signhost complies to the international requirements for advanced electronic signatures of amongst others the European EC/1999/93 directive for Electronic Signatures (ETSI 102 042 – advanced digital signatures) and the EU eIDAS Regulations (2014). These regulations and local e-signature law around the globe give electronic signatures the same legal weight as traditional ink signatures.

Contract and evidentiary rules apply to electronic records in the same way they do with paper. If a dispute goes to court, judgement will be rendered based on the evidence admitted. With paper processes and electronic ones.

The advantage is that electronic processes can render more evidence than is possible with paper.

Evidence is constructed in two ways: document and process evidence.

Signhost delivers both:

1. Each document is digital signed with an independent time stamp and sealed with PKI encryption;
2. Signhost creates an audit trail and transaction receipt of every signed PDF with prove of the process.

Signhost creates a signed document and signed audit trail for every transaction. For Strong Evidence all signers receive a copy of the signed document and signed audit trail. No dependencies are created to contact Signhost in a later stage.

The following describes in detail how Signhost provides strong evidence.

Requirement	**Details**
Capture as much document-related data as possible	During the signing process a digital signature is captured: timestamp, authentication details, hash, process steps and other details.
Secure the document and signature(s) so they cannot be altered	Signhost generates a tamper proof signed document and audit trail using a PKI signature (PADES). The signed document and audit trail are generated in Human Readable format to eliminate the “what you see is what you sign dispute”.
Capture as much process-related data as possible	All process data is captured in the audit trail: viewed, opened, signed, downloaded including a timestamp. Besides authentication is captured and document metadata like Document name, Hash, #pages.
Go beyond log files	There is no dependency of any log file of Signhost. All process steps are logged in the audit trail.
Plan for long-term archiving & accessibility	Signhost uses the ISO PDF standard and signs with a PADES signature. As with paper end users are in control of their documents and can archive their own evidence without a vendor lock.

Requirement	Details
Ensure the electronic evidence can be easily retrieved	Both the signed document and signed audit trail are presented in a readable PDF format. We do not combine both the signed document and the audit trail. A unique link is created, but due to potential privacy issues and changing the document as minimum as possible these to documents are separate.
Verify that the evidence is portable	Signhost evidence is portable by means of PDF format. Potentially can be accessed using a printable QR code or link.
Ensure there are tools to access the evidence	PDF reader is able to verify and access the evidence. In addition authentication mechanisms like SMS or country specific authentication are also accessible to proof authentication process.
Ensure that there is flexibility in process design	Signhost provides flexibility in authentication level, number of signers, pre-seal document, email or web, download.

Signhost uses PKI encryption and (PDF) document signing in accordance with the international PAdES standard.

PAdES stands for “PDF Advanced Electronic Signatures” and is a set of standards published by ETSI (TS 102 778 parts 1 to 5) to support international requirements for electronic signatures. The purpose is specifically for creation of long-term signatures that are verifiable for years or even decades.

Signhost ensures our customers to have all the necessary proof at their own control. Evidos and her e-signature experts are of course there to assist customers, but no extra dependency is needed with Signhost to verify the authenticity and integrity of the signed documents. In case of a dispute the digitally signed documents and the transaction audit trail deliver an internationally binding proof.