10 Things to Negotiate When Buying a Digital eSignature Tool

A Digital Signature Tool (DST) provides the ability to capture a signature in a secure manner using cryptography. Depending on your location, these digital signatures can be legally binding, as long as both parties have given consent. These solutions can speed up the process of signing contracts and documents and help you track progress; they also ensure the authenticity of the Signer.

Many people ask the difference between a digital signature and an electronic eSignature. A digital signature is a type of eSignature, that is more secure, and is encoded with encrypted data that is permanently embedded into the document as changes are made, this prevents any tampering.

We recommend that you compare at least three products. Here are our top ten things we think you need to add to your requirements list:

1 – Top 10 Features – Firstly the features, here are some core features you should expect/ ask for:

- **Identity Authentication** – signers should be required to provide validation to prove who they are to ensure the right person is signing. This ensures the signing person cannot deny signing the contract, and it is not possible to claim someone signed the contract when they did not.
- **Task progress and changes tracking** – this will give you the ability to track where all contracts are in the process at any time, be able to cancel a contract from being signed mid process and enables you to replace a Signer.
- **Data Integrity** – provides data integrity by being able to prove that the contract has not been modified since signing.
- **Document Storage** – gives you the ability to collect, upload, store and share documents in a central location.
- **Mobile Signature Capture** – ability for you and your employees to use on all devices including mobile. You should expect a seamless experience on IOS, Android or web.

10 Things to Negotiate When Buying a Digital eSignature Tool

- **Audit Trail / Document Analytics** – allows you to collect data on the entire signing process from the signers email address, device IP to document fingerprint and timestamp. The tool should track each transaction, documenting evidence of the entire transaction, this could be critical for legal evidence.
- **Customizable templates and branding** – customise the document workflow i.e., with your logo.
- **Reminders** – the DST will send you reminders and instant notifications.
- **Ease of use** – if the DST product is intuitive and easy to use, the adoption rate in your team is likely to be higher.
- **Multiple Users** - allow multi party signing – sharing documents with multiple users and collect multiple signatures in a chosen order or simultaneously.

2 – Scalability – The tool needs to be scalable and cost effective as you grow., if not then it must be easy to cancel the contract so you can move on.

3 – Ongoing Support – Ask for ongoing support for your tool and configuration. You should be able to access support either via email, phone, or live chat. If the tool is hosted, they should have an availability SLA. Ensure that the vendor does not require you to have an ongoing contract to validate signatures.

4 – Security – Ensuring the security of yours, and your client's contracts and data, is of the utmost importance from hacking or security breaches – ensure all sensitive data is encrypted competently or password protected – losing sensitive information will mean losing the trust of your customer. Also look for Single Sign On capability (SSO), and multi factor authentication.

5 – Cloud vs On Premise – You will need to decide which suits you best. With a cloud version you don't need a server or technical expertise on your side – all the info will reside on the vendors server – with on premise (server resides on your site) you own the software and it is physically hosted by you on your hardware – you have direct access to the servers and the contracts and documents are stored on your storage, and no recurring subscription charges, however this will include a higher upfront cost.

6 – Integration - Ensure the tool integrates with your existing tools, or has an API (Application Programming Interface) solution for integration to your other tools and systems.

7 – Vendor Assessment – It is important to do your due diligence on the company. Ask about the company stability and reputation, ensure you get references, and understand the adoption rate. Request a demo and test drive a free trial.

8 - Total cost of ownership – Weigh up the cost of the tool and associated costs to your business, including, implementation, time required to update and maintain. Setup should be fast and simple, no extensive training. Watch out for expensive plans, or lock in contracts Also best to try and get a free trial or a free plan to get started.

9 – Ownership of Data – If the software and data is being hosted in a cloud environment the ownership of data becomes more important, you should own the data. Ask the vendor if they will have access to your customers data, and what happens when you leave the subscription, who will retain data.

10 Things to Negotiate When Buying a Digital eSignature Tool

10 – Legal Compliance – Obtain users consent before using digital signatures, this will be a legal requirement in the event of a dispute, also ensure the product meets other local laws including data privacy. Ask the supplier for the GDPR clause. The customers data and where it is stored and who can access it is very important. Evaluate the use case for your documents and confirm that a digital signature would be legally acceptable.