SigningHub.com

25 key questions to ask

Here are some questions you should be asking your digital signature service provider before signing up with them

1. Is the system also available for in-house installation?

   Using a public cloud service with sensitive, commercial or personal documents makes some organisations nervous. It's important the full solution capability can be deployed internally on the organisation's own systems.

2. Does the system support an open architecture where anyone can verify signatures without referring back to the service provider?

   This will be true if standard PDF signatures (ISO 32000-1) are used which are verifiable in Adobe® Reader. Check also if ISO 19005 PDF/A format for long-term archiving is also supported if your documents need to verifiable in many years to come.

3. Are unique digital signature keys used for each person so that advanced electronic signatures can be created?

   This is important for non-repudiation regardless of whether the signing happens on the server or locally on the client-side.

4. Can the system support client-side smartcards, secure USB tokens, or soft-tokens?

   Signing on the server is usually easy, but true EU Qualified Digital Signatures currently require a Secure Signature Creation Device (SSCD) to be under the sole control of the signer. The solution must be able to use certified SSCD devices.

5. Can standard long-term signatures be created?

   These are digital signatures with a cryptographic timestamp and signer certificate status embedded inside (using OCSP or CRLs), and do not expire once the signer's certificate is no longer valid. Standard ETSI PAdES format should be used for interoperability with PDF Reader.

6. Are standard Adobe® CDS signatures supported (using server or locally-held keys) to 'certify and lock' documents against unauthorised change?

   This ensures an automatic trust when the documents are verified in standard Adobe Reader with default factory settings.

7. Is the document presented in a "flattened" view so that the user knows exactly what they are signing?

   This avoids the possibility of signing potentially fraudulent intelligent documents that do not reveal all the data during signing.

8. Can the document owner control access rights on the document?

   For example, including whether the document can be saved locally, document open passwords and date embargos.

9. Does the system support templates?

These templates define who the signers/reviewers are, in which order they must sign, where the signatures must be placed on the document, each user's access rights, notification email contents etc. This is essential to making the life of the user easier so that these rules are not defined manually every time a document is sent out.

10. Is there detailed document history and status tracking?

This allows the owner to determine when the document was opened, reviewed and signed etc. Also intermediate versions of the document should be available if required.

11. Is PDF form filling allowed?

Essential in many use cases where people are required to fill, sign and then return the form.

12. Is it possible for anyone from a group of users (e.g. accounts department) to sign a document?

This is important as typically you don't care who signs the document as long as they are the right role holder.

13. Is it possible to set-up a delegated signer to sign on your behalf whilst you are away?

It's inevitable that people will be on leave when an important document needs to be signed, the workflow rules must be able to handle this!

14. Is it possible to decline a signature and add a comment?

In the real world it's not always the case that you must sign every document that is presented to you. You must be allowed to decline and then the workflow rules must define what happens next in the approval process.

15. Does the system guide users on whether they must sign and prevent them from signing in the wrong place?

This is essential for busy, non-technical, users who don't have the time to read everything in advance.

16. If using locally held certificates does the system allow the administrator to configure certificate filters to ensure users do not accidently select a wrong certificate from their local store?

Again non-technical users do not understand different types of certificates and cannot easily choose the correct one by themselves. The solution must automate the selection of the correct certificate.

17. As an administrator, is it possible to create users accounts in advance, or identify which type of users can register, or to approve users who self-register?

Effective enterprise management control is essential for smooth deployment and to prevent unnecessary internal support calls.

18. Can the system work with existing PKIs? Also can it work with multiple PKIs thus acting as an interoperability bridge between these?

Many large organisations and regulated industries have their own existing PKIs; it will be necessary that these existing credentials can be used within the document signing system.

19. Can advanced digital signature algorithms be supported, e.g. large RSA key sizes, SHA-2, and even ECDSA?

Signature algorithms are continually being enhanced for security reasons, so it's essential the latest crypto techniques are supported.

20. Are multiple user authentication options supported?

Typically different user communities will have different requirements on how users are authenticated before signing can take place. It's important the architecture allows multiple options, e.g. username/password, OTP, SMS, certificates, grid authentication, etc.

21. Can attachments be added to a document?

This is useful where attachments of any format can be added to the PDF cover document and then the whole package is signed using standard PDF signatures.

22. Are initials fields supported?

Essential if you want users to acknowledge they have read a particular statement, or even to initial every page as proof they have not missed anything.

23. Is a simple web services API provided?

Often business applications need to push documents into the signing solution and get them signed off. The API should allow full document signature management, and include document status tracking and user account handling also.

24. Is the solution usable on mobile devices?

iPad, iPhone and Android mobile devices are very common tools now, and either a native app or browser based capability should be provided.

25. Is the solution cost-effective?

There must be a clear ROI, it should be more cost effective than traditional paper-based approval.

OK there is still one more question…

26. Can the solution be branded? Also translated into local languages?

Of course it is essential that the system can support multiple brands and languages depending on the user's local context.