ascertia | IDENTITY PROVEN TRUST DELIVERED

Business Needs For Document Approval

The Business Problem

Getting a document approved and signed-off is a crucial part of any business, be it an order, sales contract, claim forms, internal HR documents or any other type of document that needs to be clearly agreed and approved preferably with a clear audit trail.

In today's economic climate the traditional inefficient paper-based approach of manually sending, signing, tracking and storing documents has become a major cost burden for organisations.

Organisations today are also facing a variety of pressures to provide enhanced security of data, better accountability, traceability and auditing capabilities to ensure compliance with local legislation, regional directives and market and shareholder/ stakeholder expectations and requirements.

High-level Requirements

An obvious solution to the problem of paper document approval is to use electronic documents and digital signatures.

Standalone digital signature desktop products have been around for some time, however today organisations require a simple to use, cost effective document approval workflow solution, which can gather signatures from multiple parties, provide document tracking and history details. A fully automated approval process is required so that business professionals can concentrate on the core business tasks rather than chasing paper or emails – and with emails you never quite know if you are dealing with the latest version.

Many document approval solutions are available on the market, which encompass document signing , but typically they have the following serious limitations:

- They require complex user software to be installed, which senior business managers do not find easy to use. Additionally management and maintenance of this software becomes a real burden for administrators.

  Answer: The solution should be server-based (zero footprint), ensuring ease of use by end-users and ease of maintenance and centralised management by administrators

- They use proprietary "closed" signature schemes, such that signed documents cannot be independently verified; instead the relying parties need to feed the document through the service provider's systems in order to verify them.

Answer: The solution must use standard digital signature formats. By far the most popular document format in business is PDF; therefore standard PDF signatures must be supported.

Signatures produced by the solution must be "open" i.e. verifiable in freely available PDF Reader, without having to upload documents to the service provider for verification.

Signed documents must stand on their own, i.e. be verifiable without having access to the service provider's logs.

Document signing solutions are categorised as either "e-signature" or "digital signature" solutions. The difference is that e-signatures can be a simple mouse scribble, scanned signature image or any other mark which indicates the user's consent. On the other hand, digital signatures are based on Public Key Cryptographic and provide both data integrity and strong evidence of who signed the document thereby helping to provide non-repudiation services.

- They do not use unique signing keys under the sole control of the signer. Many solutions use a single server-held signing key that is used for all users, in effect a "proxy" signature. Some approaches do not even use a cryptographic digital signature but rely on hand-drawn ink squiggles with proprietary crypto techniques.

Answer: The solution must use different keys for each signer. This is an essential requirement for European advanced digital signatures.

Electronic hand-signature images can be used to give human recognition for technology acceptability reasons but can be easily copied so the solution must not rely solely on these as a security measure - their use for aiding human recognition and acceptance is welcome.

The solution must protect each user's signing key such that only the authorised owner can knowingly release their key for signing purposes.

- They do not allow the use of locally held signing keys (e.g. on smartcards or secure USB tokens).

Answer: Many countries have issued electronic ID (eID) cards to their citizens. These offer the highest level of identity authentication and signing key protection. If such an eID infrastructure exists then the solution must allow these eID cards to be used for signing purposes.

Qualified signatures within Europe require the signing key to be held on a smartcard or USB token (officially called a Secure Signature Creation Device or SSCD) under the sole control of the signer. The solution must allow the use of such smartcards or tokens.

Within a corporate environment, employees may have already been issued with certificates by the organisation's PKI system. The solution should also allow the use of these certificates.

- Many signed documents are not verifiable in the long-term. Even if the solution uses standard digital signatures with unique signer keys, the signatures are not designed for long-term use. Once the signer's certificate expires then the documents signed with this certificate can be hard to verify. When viewed in Adobe® Reader the trust status is shown as 'unknown'.

Answer: The solution must support long-term signature verification by using ETSI standard enhanced digital signatures that include an embedded timestamp plus the signer's certificate status information at the time of signing.

- There is a lack of "trust" interoperability. Users of one PKI system are not able to trust the signatures from users of another PKI system.

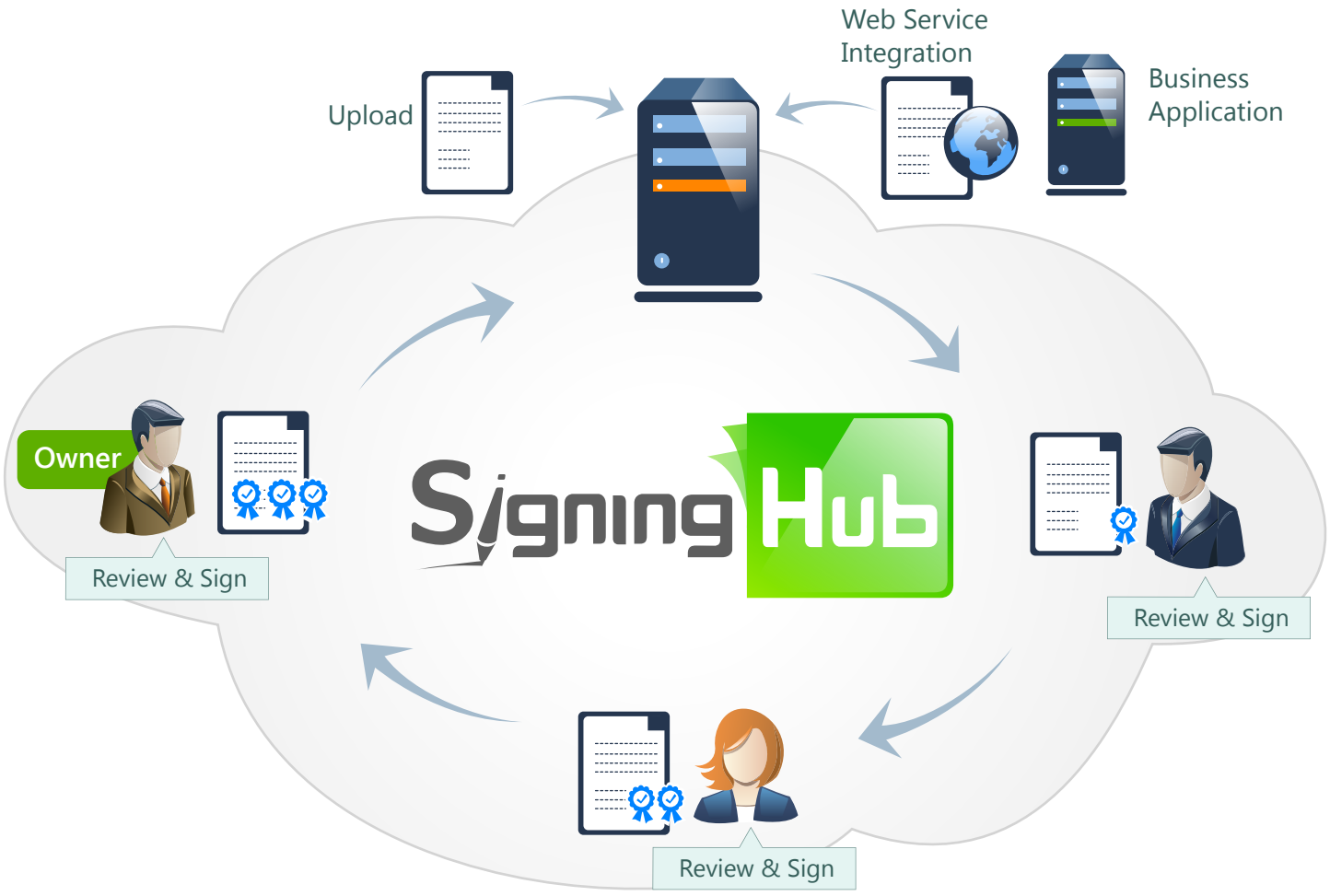
Answer: The solution must allow multiple PKI systems to be used and therefore trusted. There will never be just a single global PKI system that everyone uses. Trust interoperability is especially important for cross-border interactions. The solution must be able to distinguish between the different levels of "quality" offered by the different PKI systems. The solution must allow users to compartmentalise which PKI systems they wish to trust and for which purposes.

In addition to the above, organisations require a solution which reflects real business approval processes, for example the ability for anyone from a typical department or group to sign a document, the ability to control the document such that it can only be signed within a specific area of the page, the ability to define delegated signers in case the primary signer is ill, on holiday or otherwise not available.

SigningHub has been developed to avoid the issues discussed above and use individual signatures with high-security and long-lived trust. Furthermore, SigningHub supports the complexity of real-world business document approval processes so that it can be effective in replacing paper and ink signature processes.

About SigningHub

SigningHub is a cloud-based application that allows users to upload, share, review and securely sign documents as part of an automated document approval workflow process:



The key features and benefits of SigningHub are:

- There is a lack of "trust" interoperability. Users of one PKI system are not able to trust the signatures from users of another PKI system.
- It is a flexible document workflow digital signature approval system with an ability to share documents with both internal and external users in a formal and informal way. Signature fields can be added as required and effective tracking and reminder facilities are provided so that the approval status can be monitored at all times by the document owner.

- Documents can be uploaded and shared by multiple web-based users, and optionally by back-end applications, using a web-services interface, that wish to use SigningHub as a front-end signing solution. Once a workflow is complete, the signed document can be transferred to other systems.

- Document approval uses advanced digital signatures. These signatures are created using unique keys for each registered user – a much better approach than using a centrally held "proxy" signing key and certificate used for everyone. In SigningHub, each user has a unique signature key only accessible under the user's control thus providing strong evidence of the signing action.

- Existing local signing keys and certificates can be used – these are typically held on a smartcard or USB token and certainly this is the case for eID credentials. Another option is to use roamed credentials that are downloaded to the user's machine when a document needs to be digitally signed. The final choice is to use centrally managed keys on the server, held securely for each user. The server then act as a virtual smart card for multiple users.

- Signatures with timestamps or with full long-term validation (LTV) capability can be created so that they can be verified many years into the future. LTV means that both a timestamp and the signer's certificate status information is embedded inside the signature. This is key business requirement and is considered important for all agreements, contracts, invoices and other documents that need to be trusted for a few weeks, months or years into the future. As discussed before, basic signatures will cause trust confusion for future reviewers. EU Qualified Certificates and Adobe CDS certificates can be used to create high-trust signatures.

- PDF (ISO 32000) and PDF/A (ISO 19005) documents and signature formats are supported. Signed documents can be verified by anyone with the freely available Adobe® Reader (or other compatible viewer and signature verifier, or a suitable document verification portal).

- Visible signature appearances can include information about the signer, the signing reason, their location and even their hand-signature images and company logos for a formal and professional looking signature.

- Document owners can control the access rights to a document, for example they can allow or disallow local printing, local saving and open date & time embargos as well as optional document open passwords.

- Sharing profiles are used to remember signature settings and these can be readily re used to quickly assign the same settings and rights to new documents. Many people deal with the same types of documents such as reports, purchase orders, expenses, requisitions, approvals on a repetitive basis and this feature allows each of these to have one (or more) standard share profile(s).

- Supports multiple document formats and internet browsers to offer wide external desktop / browser and key/certificate support.

- Any standards compliant Certificate Authority (CA), Time Stamp Authority (TSA) and smart cards / USB tokens can be used (via Windows CAPI, Apple Keychain or PKCS#11).

- If a user's signing keys are held centrally on the server, a One Time Password (OTP) mechanism using SMS messaging to the user's registered mobile device can be added as an additional authentication for the signing action.

- Local languages are supported and are automatically selected by the user's browser language setting – assuming these language tables exist on the server. Light rebranding of the user GUI can be provided so that partners in various countries can offer a local look and feel with their own language(s).

These and other features are discussed in this document. SigningHub uses digital signature security services provided by the Ascertia ADSS Server and ADSS Go>Sign Applet. ADSS Server can be used to provide CA services, CRL issuance, OCSP Validation Authority (VA), Time Stamp Authority (TSA), and long-term archiving and notary services (LTANS) either in conjunction with SigningHub or separately.

About Ascertia Limited

Over the last ten years, Ascertia has become a successful global provider of advanced digital signature and electronic identity (eID) validation software solutions. Ascertia's products and business solutions focus on enabling trust within e-commerce environments using digital signature and data encryption technologies. Firms can now safely cross the final hurdle of migrating paper-intensive processes to the digital world by using Ascertia's products to sign securely on the desktop or application server.

Ascertia customers include national and regional governments, central banks, global financial institutions, leading telcos, large multinationals and SMEs.