ascertia | IDENTITY PROVEN TRUST DELIVERED

- > DOCUMENT SIGNING
- > eID VALIDATION
- > SIGNATURE VERIFICATION
- > TIMESTAMPING & ARCHIVING
- > APPROVAL WORKFLOW

Why Document Management Systems Need Digital Signatures

Online information systems allow organisations to improve their efficiency, substantially reduce their costs, enhance their green credentials and comply with regulatory requirements. Having timely and reliable access to accurate, final, approved and even archived information is today's business imperative. A good document management system is often thought of as all that is required – but further protective measures are required to ensure that valuable corporate data cannot be faked or have fraudulent or other unauthorised changes applied after approval.

The Security Issues

Document management systems generally offer good security and control access to document and the ability to change documents. However when a document leaves this secure environment it is exposed to potential changes. With any digital document it is easy to modify the content or copy the images and create realistic but fake and fraudulent documents. Unprotected PDF, XML, Office and electronic documents provide a recipient with no way of determining if a document is genuine, who the originator and approvers were, whether they are authorised to release it or whether it has been modified since its release. A simple embedded squiggle signature image does nothing to protect the document against future change.

In general people understand the concept of digital signatures, however most don't know what makes it valid or what level of security is required for their use case. The vast majority of people are familiar with e-signing on tablet devices to accept deliveries, however high value or high risk agreements internally or with third parties need approval with signatures that can be confirmed as authentic and that ensure that nothing can be later modified without the signature breaking.

Fortunately cloud based business services make it easy to create digital signatures and verify these at any later time. Digital signatures provide strong evidence of sign-off and approval (non-repudiation) plus document authentication (integrity) and they lock the document against unauthorised change. Long-term signatures ensure that this evidence remains valid for many years into the future and embeds the trusted time of signing in the form of a time stamp within the document. This document has such a long-term signature on the last page that is verifiable by the ubiquitous Adobe Reader product. Secure audit logs and other accountability features also provide strong evidence of user's signing actions.

Regulatory Requirements

In the USA the Food and Drug Administration also require digital signatures on high trust documents including drug approvals and controlled substances prescriptions, why? Because they are the only form of signature that protects the data. In Europe the Digital Signature directive defines both Qualified and Advanced Digital Signatures as means of producing legal weight evidence that is an electronic equivalent of an ink signature. Qualified Signatures provide the gold standard of trust because end-users must go through a strict Known Your Customer registration process. Advanced Signatures are also acceptable for many business applications but generally have a less formal registration process.

Within Europe the EU VAT Directive aims to prevent VAT fraud by mitigating the risks of changed or fictitious documents. The Directive requires that: "Invoices sent by electronic means shall be accepted by Member States provided that the authenticity of the origin and integrity of the contents are guaranteed". The only standard and interoperable way of doing this is to use digital signatures and the EU recommends that a qualified electronic signature is used to confirm the identity of the originator.

The Directive also requires that "The authenticity of the origin and integrity of the content of the invoices, as well as their readability, must be guaranteed throughout the storage period". This is probably the most important aspect since documents must be kept for many years and being able to show they are unchanged and original is a pretty hard ask for any business - unless of course you protect your invoices with long-term digital signatures. Ascertia has provided a wide variety of organisations with invoice signing solutions, payment protection solutions, data or document signing and document workflow approval solutions.

Digital Signatures and Business Benefits

The most effective way of meeting these requirements is to use industry standard digital signatures. These bind the identity of the signer with the document content in a way that clearly shows that the document is authentic and that the document is unchanged. Digital signatures deliver trust services that can remain effective for many years, enough for all financial documents (special options exist for proof beyond 20+ years). An advanced electronic signature provides authenticity and integrity and generally the trusted time of approval is also bound into the document. Couple these signatures with PDF/A (ISO 19005) format documents and you can now guarantee that the document can be displayed correctly with no content or layout changes and that the signature(s) are still valid for many years into the future.

Visible digital signatures provide an effective way of mapping wet-ink paper signatures to the electronic world. Invisible signatures are by their nature less obvious and yet they prevent any unauthorised change. The protection offered by the cryptographic processes is extremely robust and uses multiple international standards for widespread interoperability. Without this form of protection important business data is open to abuse, manipulation, fraud, denial and theft. A digitally signed document enables a recipient:

- To confirm who signed the document, when they signed it and their current trust status (by checking and validating the signers digital certificate)
- To confirm the document has not been changed either now or later, be it weeks, months or even years (by verifying the digital signature)
- To confirm the originator meant to approve it – it is not a draft unsigned document and that the originator cannot deny approving it (by verifying the signature)
- To save time and substantial monthly costs in invoice printing, paper, postage and archive/storage (by enabling paperless workflows)
- To meet the needs of various legislative and regulatory regimes

National laws can also be met see http://en.wikipedia.org/wiki/Digital_signatures_and_law for a useful set of reference data.

Ascertia's Products and Solutions

Ascertia's ADSS Server product and SigningHub Cloud service have been designed to make it easy to add (or retro-fit) effective and flexible document signing services to a range of business applications. Adding trust to NDAs, license terms and conditions, quotes, orders, invoices, statements are just some examples of where digital signatures bring substantial value. Final, released documents can now be seen to be approved on behalf of the legal entity and the data within them cannot be changed. PDF, PDF/A, Office docs, XML and other forms of data can all be signed. SigningHub and ADSS Server provide substantial value because they deliver:

- An effective way of safeguarding organisational identity and its financial documents
- An effective way of confirming the accuracy and integrity of documents to third parties
- An effective way of minimizing fraud committed using fake corporate identities
- Multiple easy ways of adding security to existing business applications
- An immediate way of complying with EU, USA other legislation and regulatory requirements
- A secure audit trail that provides clear accountability of who, what, when, how, where.

Creating Trust

Trust for document digital signatures is derived using a number of elements:

- The trustworthiness of the certificate issuer and the quality of their policies and procedures when dealing with user registration and identity proofs (i.e. Qualified Certificate Signatures versus Advanced Digital Signatures)

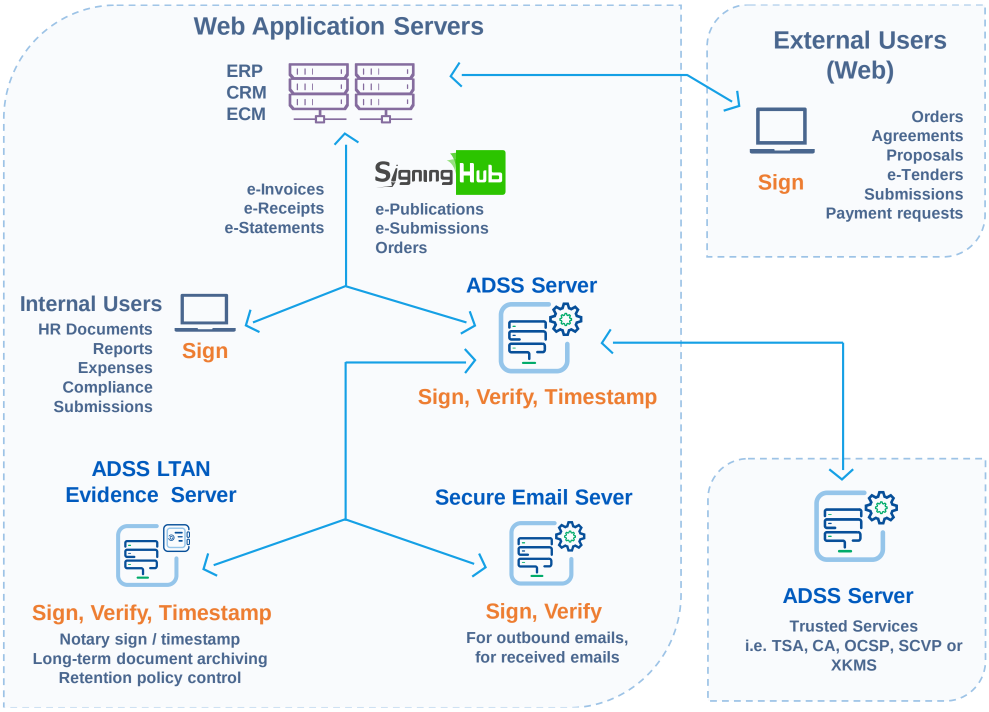
- The security management controls that regulate the digital signature creation process and the way in which access to this can be authorised and event and transaction logs audited
- The way in which the digital signature can be reviewed and verified by independent third party software (e.g. PDF reader products) as well as service providers
- The use of trusted third parties to provide timestamp, signing or verification services to independently assert trust (often offering liability for these services)

Ascertia Delivers

- User authentication
- Trusted identities
- Traceability
- Accountability
- Certainty
- Integrity
- Archiving

For

- PDF documents
- XML data
- Word, Excel and other file types
- Web forms
- Emails



Even when digital signatures are added to a document, “trusting” a digitally signed document can still become a business issue within a very short timeframe. Some systems will fail to verify documents as soon as the signer’s digital certificate expires. Ascertia’s products offer comprehensive trust services and support, and indeed recommend, the use of long-term digital signatures. These include a timestamp that shows the trusted date/time for each individual user signature plus a signed response from a trusted validation authority confirming that the signer’s certificate was valid at the time of signing. Very few companies match this high bar of security, not because they don’t want to, but because it is technically very advanced to deliver this. It is similar to car door locks – all cars have them but very few offer the highest levels of security.

SigningHub and ADSS Server have been carefully designed to make it easy for applications to sign and verify documents using the approaches discussed above as well as many other use cases. The technical complexities are hidden from view and add to the security by enabling users and developers to access advanced trust services whilst security operators define what these are and how they will be provided. The trust services offered are suitable for all important business documents including:

- Those placed within Document Management Systems
- All e-Invoices and all other issued and archived financial documents
- Regulatory submissions in the financial or pharmaceutical and other markets
- Financial instruments, insurance policy documents, loan agreements
- Central and local government documents, health records, library systems
- Engineering, architecture, planning, R&D drawings
- Policies, procedures, internal controls and compliance documents
- ERP, CRM, HR and other document management systems

Why Choose Ascertia

Ascertia offers world-class products that deliver functionally rich, easy to deploy security solutions. Our focus is delivering PKI infrastructure trust services and making it easy to digitally sign business documents and data. Signatures deliver the essential trust services needed by governments, financials, telco, healthcare and other organisations to conduct electronic business. Digital signatures deliver the assured authenticity and data integrity needed to meet internal controls requirements, traceability, accountability and audit services to meet legislative and regulatory requirements. Fraud often involves fake information or unauthorised changes and these trust services help protect organisational brands and data.

Ascertia's senior management team has decades of experience in working with security for Government and Financial systems both in Europe and North America. We are trusted by an impressive set of clients and work with some of the leading IT security vendors and managed security service providers.

Need more information?

For further information on how we can deliver these trust services that protect your business documents and workflow processes visit the Ascertia web-site or the SigningHub web-site www.SigningHub.com or ask the Ascertia team via info@ascertia.com