Protecting Invoices and other Financial Documents from Fraud

Almost every organisation needs to issue invoices. For medium to large businesses there are substantial benefits in eliminating all the costs associated with paper production, handling and postage that can exceed €1 per invoice. Electronic invoicing systems can provide a fast ROI against these costs and make the business more efficient. The main financial data is usually held electronically and invoices can be archived in their digital form (usually PDF, sometimes XML) to avoid the storage costs and retrieval issues when using paper.

It is clear therefore that 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 archived information is today's business imperative.

The Security Issues

With any digital document it is easy to modify the content or copy the images and create realistic but fraudulent documents. Unprotected PDF, XML or other electronic documents provide a recipient with no way of determining if a document is genuine, who the originator was, whether they are authorised to release it or whether it has been modified since its creation. There is a good solution to these issues – it is very easy to digitally sign and optionally timestamp these documents in such a way that locks the data against change and provides proof of sign-off & approval. This signed solution sheet provides such an example. Another well-known fraud is to send an invoice recipient a letter notifying them of a change of banking details. It is easy to replicate header paper and make this believable however it is mathematically infeasible to forge a trusted digital signature. VAT and payment frauds can be made much less likely for your business if you sign everything with a trusted digital signature.

Regulatory Requirements

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 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 key issue for any business.

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 sender with the data content in a way that clearly shows if the document has changed. Digital signatures deliver trust services that are effective both immediately and for many years of archive storage. Authenticity and integrity are assured and the time of approval is also bound into the document. The use of PDF/A (ISO 19005) format documents guarantees that anyone can display and print the document both now and for many years to come.

Digital signatures provide an effective way of mapping wet-ink paper signatures to the electronic world. 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 invoice enables a recipient:

- To confirm who sent the invoice, 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 send it – it is not a draft unsigned document and that the originator cannot deny approving and sending 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 the EU VAT Directive and where required using Qualified Electronic Signatures to ensure signature acceptability within the EU

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

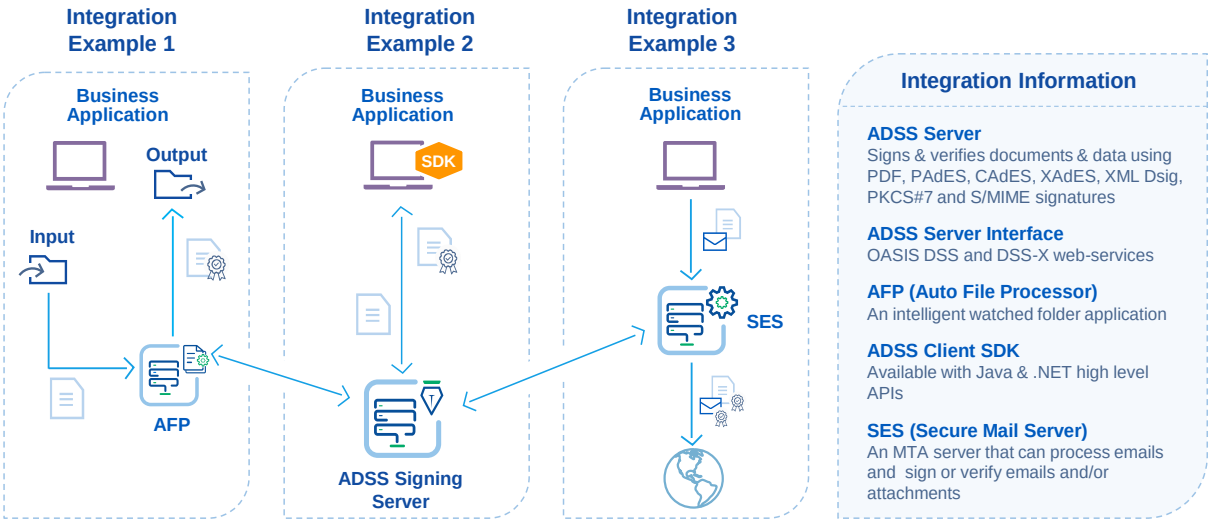
Ascertia's Products and Solutions

The Ascertia ADSS Server has 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 invoices is just one example of where digital signatures bring value. Other documents such as orders, quotations, proposals, tenders and receipts all benefit from using trust services to provide evidence of formal sign-off and release. 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, XML and other forms of data can all be signed.

ADSS Server is of value to organisations because it provides:

- 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 using watched folder processing, email or high level APIs
- An immediate way of complying with the EU directive and applicable local legislation

Digital signatures can be applied to documents as they are output by the business application as shown below. A separate solution sheet deals with workflow sign-off and approval and multi-user signed requests to authorise the use of a corporate signing key.



Example 1 offers a very easy to implement approach using ADSS AFP (Auto File Processor) a watched folder application to read, digitally sign and output signed documents. Multiple folders can be used to identify different document types and signing keys if required. AFP can

also create PDFs from other document types and also insert blank signature fields as part of the preparation process. No integration effort is required for this.

Example 2 shows the use of the ADSS Client SDK high level Java and .NET APIs to enable easy access to web-service based signing features (direct XML/SOAP interface is also available).

Example 3 shows email integration using Secure Email Server (SES) to process outbound email and sign either the email or more likely the attached documents as they are sent to the recipients. No integration effort is required for this – emails with a PDF, XML or other attachment simply need to be routed via the Secure Email Server for the automated filters to identify the email and its attachment document and sign using defined signing keys and appearances.

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
- The security management controls that regulate the digital signature creation process and the way in which access to this can be authorised and 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)

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 ADSS Server offers comprehensive services and handles this in two easy ways:

- Creating long-term signatures that include (a) a trusted timestamp of the authenticated time of signing and (b) a signed response from a trusted validation authority confirming that the signers certificate was good at the time of signing;
- Using historic validation services to ensure that the signer's certificate was valid at the time of signing by checking old CRLs (Certificate Revocation Lists).

Either of these are good standards-based approaches.

Historic verification requires a more sophisticated checking system whereas long-term signatures include all the information to enable an application to verify the signature. To implement either approach ADSS Server has been designed to make it easy for applications to sign and verify documents using the approaches shown above and several others. The trust services offered are suitable for all important business documents including:

- e-Invoices and other financial documents as well as archived 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

For long-term archiving of documents you should review the long-term evidence archiving solution sheet.

Need more information?

Ask us for further information on how we can deliver trust services that protect your business documents and workflow processes info@ascertia.com