A Solution for Signing SAP and other ERP e-Invoices

Almost every reasonable scale organisation needs to issue invoices. For medium to large businesses there are substantial benefits in eliminating paper and the associated handling and postage costs, typically estimated at about €1.50 per letter. Typically core financial data is held electronically and invoices are archived in digital form to avoid the costs and retrieval issues when using paper-based archiving. 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.

Regulatory Requirements

With any digital document it is easy to create realistic but fraudulent documents. Unprotected electronic documents make it extremely hard for recipients to determine if the document is genuine, who the originator is, whether they are authorised to release it or whether it has been modified since its creation.

Within Europe the EU VAT Directive aims to prevent VAT fraud by mitigating such risks. 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 in general EU member states require that a qualified electronic signature is used to confirm the identity of the originator. EDI systems can be used however VAT authorities can still insist on paper summaries being provided for EDI.

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".

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 everyone 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

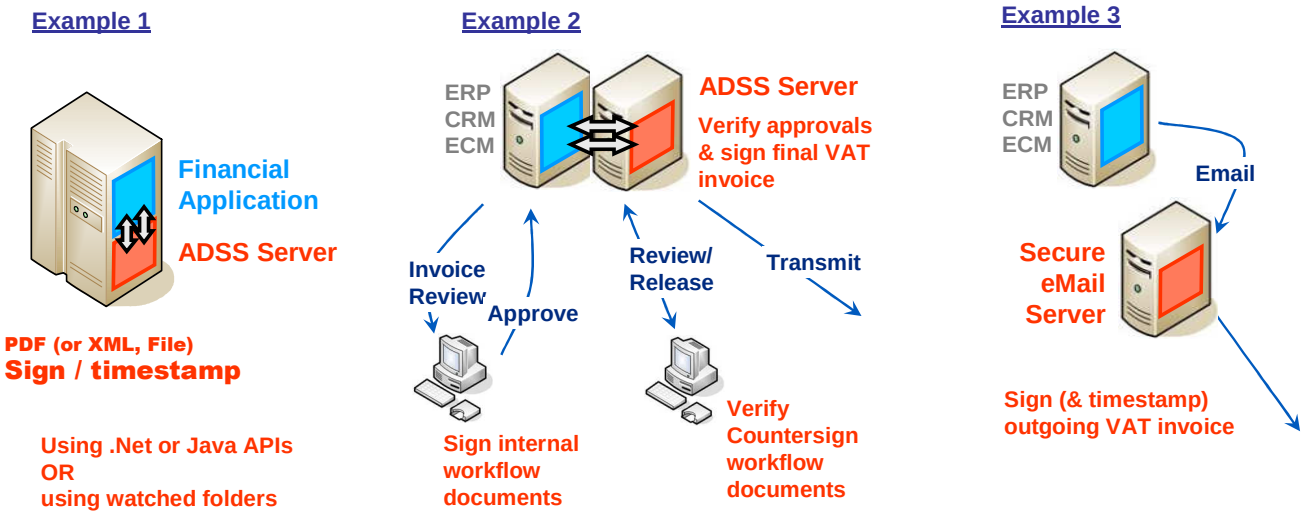
The Ascertia ADSS Server has been designed to make it easy to add (or retro-fit) effective and flexible document signing services to a range of business applications. Adding trust to invoices is just one example of where digital signatures bring value. Other documents such as orders, quotations, proposals, 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.

ADSS Server makes it very easy to implement effective trust solutions to meet the relevant legal, security, audit and compliance requirements for multiple countries. For most business documents Ascertia recommends the use of PDF/A files as a globally interoperable standard that is readable by both people and systems.

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 invoices to a third party
- 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

The digital signatures can either be applied to documents as they are output by the business application (see example 1 and 3 below), or they can be used to authorise and release internal workflows and approve access to corporate signatures as shown in example 2:



Example 1 also offers a simple approach using Watch Folder mode to accept, digitally sign and output invoice PDFs. Multiple folders can be used to identify different document types and signers if required. High level APIs enable easy access to web-service based signing features. The ADSS Client SDK provides .NET and Java APIs and example code to minimise integration effort. Using these APIs the workflow approval approach shown in example 2 can be readily implemented to provide internal traceability and accountability. Far too often it is impossible to prove that key documents were in fact reviewed, approved and released by key staff members. Increasingly legislation and regulation is driving businesses to implement such measures to strengthen their internal controls. Example 3 is the easiest to implement using Ascertia's new Secure eMail Server to sign PDF attachments as they are sent to the recipients. No integration effort is required for this – emails with PDF attachments

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 within digital signatures is derived from a number of aspects:

- 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 has less dependence on the need for enhanced security to create long-term signatures within end-user applications. For long-term trust it is clearly better if documents are passed to a specialist long-term trust solution such as ADSS Server that has been designed to offer both verification and notary archive services. Ordinary applications will be unable to handle such advanced features for some years to come and so deploying a separate product as part of the business workflow process makes a lot of sense. ADSS Server has been designed to meet these needs and offer trust for important business documents including:

- e-Invoices and other financial documents and records
- 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
- Test and trials data required for independent assessment and approvals
- Policies, procedures, internal controls and compliance documents
- ERP, CRM, HR and other document management systems

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

Identity Proven, Trust Delivered