Trust Services that Reduce Fraud, Risk and Costs

It is easier than you think to safeguard your e-business data and create secure, trusted documents that cut risk and costs.

Many businesses are still using paper based agreements and documents and relying on ink signatures. Of course organisations have used these for hundreds of years to formalise agreements with other companies, their employees, government departments and for approving financial instruments.

All formal documents are created to ensure that there is no confusion about what is being offered and what is being accepted. In the electronic world, business documents also need trust services to ensure that each party can have confidence in both the signer's identity and the document's integrity both immediately after signing and well into the future.

Many companies are already using trust services to differentiate themselves. Their processes are easier to deal with, they become faster to respond and they can also reduce their prices by saving their paper, postage and handling costs. However other organisations have moved online and take no special measures to protect their data and place their reputations at real risk. There is no need for this since putting an e-business trust solution in place can have an ROI measured in months, even for small organisations.

The common business issues we see when trust services aren't used include:

- **Unauthorised changes** - to key business documents by employees or external parties
- **Lack of clarity -** around version control and the approved status of documents
- **Corporate identity theft -** using fraudulent documents, data and packaging
- **A lack of evidence -** raising risks and costs in disputes over e-invoices, orders, confirmations, tenders, expenses, reports and existing agreements and subsequent written amendments or clarifications, especially by email

It's Ascertia's view that these issues can be easily resolved by providing:

- **Traceability -** by embedding a clear approval process within business documents to create strong, legally admissible evidence
- **Accountability -** by binding the identity of the approvers to the documents
- **Auditability -** using strong integrity and authentication mechanisms and providing policy based controls and secure event and transactional logs
- **Strong evidence -** using industry standard, legal weight digital signatures that are verifiable by internal systems and staff as well as external organisations

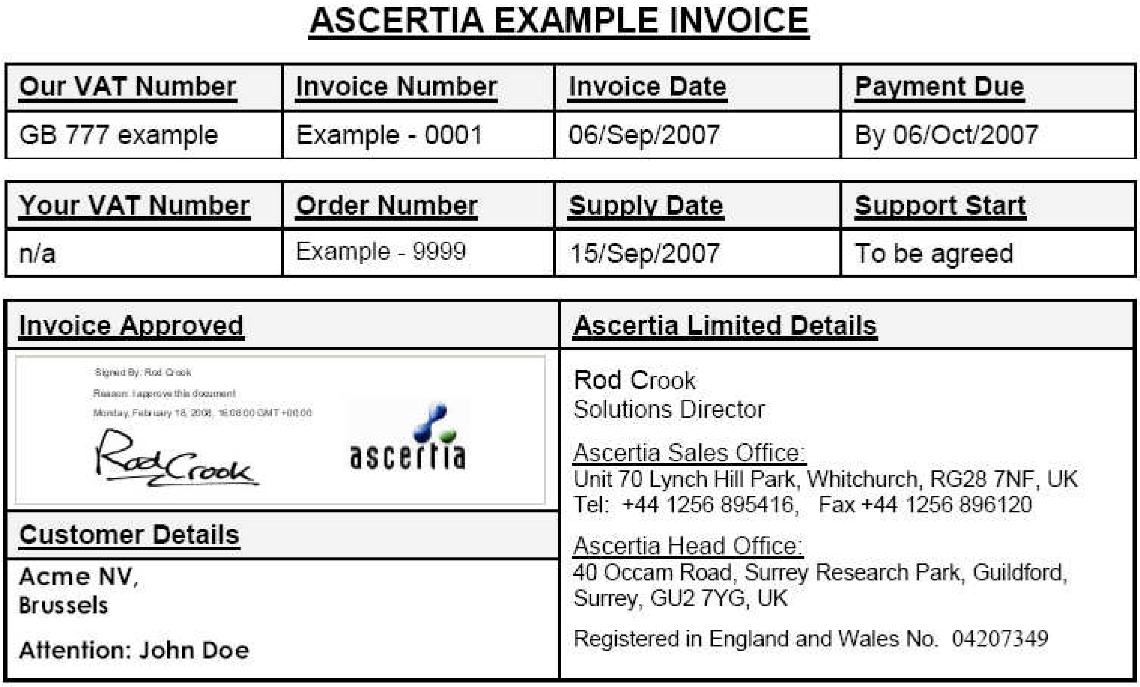
Even today it is still surprising how many businesses still think that their documents and data do not need any special protection, that traceability, accountability, audit and legal weight evidence are all things that aren't really needed. It's likely that these are the same companies that think they are safe using simple username and password approaches to access important systems across the net.

This document looks at what we mean by trust services, why they are valuable, when they should be used and how easily they can be adopted. Common business risks are identified and standards-based solution approaches are proposed to mitigate the risks.

Digital Signature Trust Services

Paper based systems generate substantial costs for businesses in terms of print production, postage and handling. Of course receiving documents in paper form also creates substantial costs including manual handling and re-keying data, secure archiving and disaster recovery. Many firms choose to scan paper into images and then destroy the original, however there is still a question of evidence.

Whilst paper documents typically create good evidence that can be used effectively within dispute resolution procedures, digital signatures provide even stronger evidence for e-business data. They achieve this by binding the signer's identity and time of signing to the original document and by providing integrity checks to ensure that no post-signature changes can be made anywhere in the document. The image below shows a digital signature embedded within an example PDF invoice:



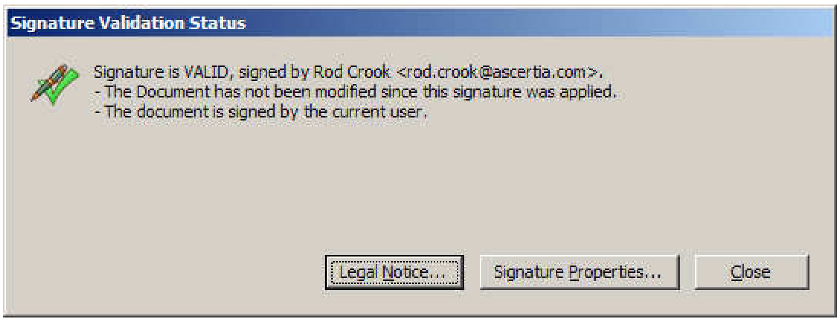
ASCERTIA EXAMPLE INVOICE

Our VAT Number	Invoice Number	Invoice Date	Payment Due
GB 777 example	Example - 0001	06/Sep/2007	By 06/Oct/2007

Your VAT Number	Order Number	Supply Date	Support Start
n/a	Example - 9999	15/Sep/2007	To be agreed

Invoice Approved	Ascertia Limited Details
Signed By: Rod Crook Reason: I approve this document Monday, February 18, 2008, 16:08:00 GMT +00:00 Rod Crook ascertia	Rod Crook Solutions Director Ascertia Sales Office: Unit 70 Lynch Hill Park, Whitchurch, RG28 7NF, UK Tel: +44 1256 895416, Fax +44 1256 896120 Ascertia Head Office: 40 Occam Road, Surrey Research Park, Guildford, Surrey, GU2 7YG, UK Registered in England and Wales No. 04207349
Customer Details	
Acme NV, Brussels Attention: John Doe	

The signature includes some informative text, the time of signing and two useful images – a hand-signature image and a company logo. The hand-signature image is just for convenience – it is a visual cue to the reader – and thus it has no need to be the normal signature appearance and so widespread dissemination on the Internet is not a problem. The key part of this signature is the industry standard, financial strength digital signature cryptography. Clicking on this digital signature block shows further verification information to aid the end-user:



Signature is VALID, signed by Rod Crook <rod.crook@ascertia.com>.
- The Document has not been modified since this signature was applied.
- The document is signed by the current user.

This provides reassurance that independent checks are being made on the document's trust elements.

Why use digital signatures internally?

Unfortunately it is all too easy for draft documents to look like final approved documents, for important information to be changed when it should not be, for documents to be acted on in good faith where no such trust should actually exist. In such cases disputes arise and the cost of such actions can rise substantially if the evidence is weak.

Strong trust services that authenticate the signatories to a document, that confirm the integrity of the data, and the trustworthiness of the identities involved (at the time of signing) all create useful legal evidence. Such evidence enables the swift resolution of any dispute, e.g. for disciplinary procedures you may wish to prove that an individual had signed and approved a particular document in the past. Without the use of digital signatures this can be far from easy if they can allege that someone else has later changed part or the whole document and there is no proof to the contrary.

Documents, emails and even audit logs that are unprotected and easy to change are not that useful – their value and integrity can be easily questioned and their value thrown into doubt. In contrast digital signatures use tried and trusted techniques that have been exposed to public scrutiny for over 30 years. Their use is enshrined in most legal systems and of course contract law can make them applicable and binding on the parties in any circumstance.

Why use digital signatures externally?

For external interactions you need to know that your communications with third parties are trustworthy, that their identity can be trusted and that the data you exchange can be shown to be authentic and unchanged. Establishing such trust enables web-based systems to replace paper-based systems. Processes that used to take many days or weeks can now be operated in just minutes or hours using signed electronic documents. Data entered on-line can be used to form binding on-line agreements and both parties can easily sign and co-sign such documents.

PDF documents dominate in this area mainly because of their global acceptance as a means of displaying information on different systems. They also are fully compatible with digital signatures and have been for several years.

The value of managed services

It may well be appropriate and prudent to carry out additional checks on the authorisation levels of an individual, on their current role or qualifications or indeed the financial standing of the company they represent. External approvers need to know that the signature they see is from a qualified or authorised individual e.g. approved financial advisers, company directors or qualified professionals. This role based data can be attested to and signed by the service provider or the relevant institution.

For documents that have a lifetime of many years (insurance policies, license agreements, guarantees, compliance, financial or health records etc) then long-term signatures can be created that can be immediately verified for many years into the future. Digital signature timestamps provide the proof of when a document was signed, received or accepted.

The human factor

Without these trust services measures, human frailties will guarantee that accidental, fraudulent or malicious changes will be made. Draft documents will inevitably be released into workflow process and business risk will be much higher than it need be. To minimise human errors the trust services should be easy to deploy and easy to use. Senior managers always want to see a minimum of complexity, e.g. 'your signature is required' followed by a SIGN button and a CANCEL button. There should be no complex questions or inputs because the business application should know what signature type is required, where to place it and how to apply it.

Verifying Digital Signatures

The recipient of a digitally signed business document needs to check if the signature can be trusted. This can be done as part of a document management workflow or when reviewing the document in a browser, on the desktop or on a mobile/PDA. To avoid the human factor the former is recommended.

Signature verification ensures that the mathematics behind the signature checks out and of course this should be done in a seamless and invisible way. Various PDF document viewers are able to show the identity and integrity of any signed document as was demonstrated earlier.

The big issue is whether you trust the claimed identity. Governments trust certain digital certificates (e.g. EU qualified certificates), banks trust certain certificates (e.g. their own and those from global banking associations such as IdenTrust), other organisations can either implement such trust services themselves or ask third party providers for help. Outsourced services are now available such as the Validation Authority service from BBS (www.bbs.no). BBS offers to verify signatures and give organisations a quality rating on the signatures that they check, furthermore they offer liability on this service, thus ensuring relying parties can accept signatures with confidence. Other national service providers are busy implementing local trust services for various markets.

Trusted Archiving

Important documents need to be kept for several months or years and must be shown to be unchanged during the archive period. Once again, digital signatures can easily ensure that documents are protected and have not changed. Without such trust services it is quite possible to inject false information into an archive or perhaps more seriously delete information in the archive and the evidence of such deletion. Timestamps are particularly useful in proving original archive time and thus also showing that document and data retention policies are enforced

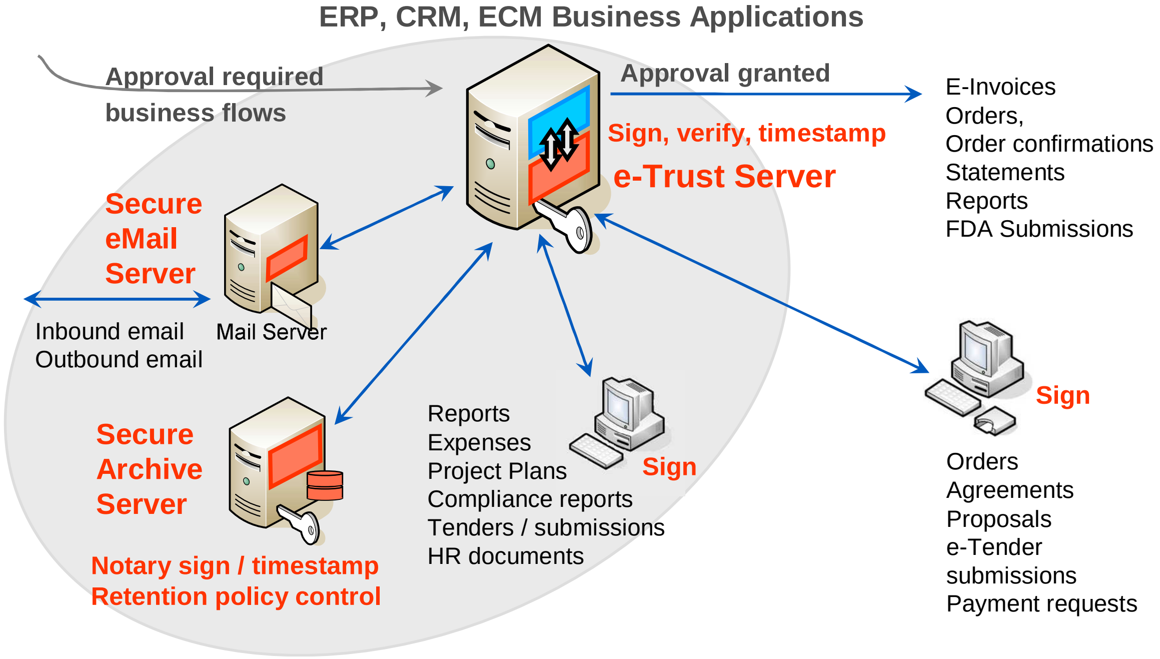
There have been concerns about how documents can be opened and viewed in the future. ISO 19005:2005 defines a format of the PDF standard, known as PDF/A that ensures that documents can be rendered (i.e. viewed or printed) many years hence. Thus the display of the document is "guaranteed" into the reasonable future and digital signatures can ensure that its integrity and authenticity is also provable.

User Registration, Authentication, User Authorisation

Identity Management is a widely used term that encompasses corporate identity, role management, multi-system single-sign on and password synchronisation. Within this broad arena there much debate about how best to authenticate users and also authorise actions they request within business applications. There are many authentication options and interestingly the same techniques can be successfully used to authorise transactions and document approvals. By linking such authentication services to a trust server, the use of server-held user keys and certificates can be authorised. Important requests or actions can now be signed by the individual even when they are roaming on different devices, Windows, MAC, Linux and mobile devices.

Workflow Approval

All of the options discussed above can be enabled within existing workflows, e.g. SAP and other ERP invoices can be signed. Web-applications can issue signed receipts, e-portal systems can easily ask users to sign and confirm their order or request. Importantly no new software needs to be installed on the third party or end-user systems. Multiple business applications, systems and users can use the same trust services options in ways illustrated below.



Using such approaches your business can easily create trusted documents that provide legal weight evidence. This will result in reduced process time, reduced errors and thus improved customer satisfaction, as well as reduced costs. It is definitely time to consider the e-business trust issues and how they can be used to secure and differentiate your business.

Summary

Using trust solutions such as those described above enables all organisations to remove the high costs of paper processes and to benefit from the use of protected documents that provide legal weight evidence. It has never been more important than now to evaluate your business processes and see how they can be made more efficient, effective, how trust solutions can and should be used to protect your data and reputation and to differentiate your business.

Ask Ascertia or its partners how we can help to safeguard your corporate information before someone else demonstrates why this form of insurance is necessary.