The Business Need for Long-Term Evidence Archiving

How can your business ensure that archived data and transactions remain in their unchanged original form in 10, 20 or even 50 year's time? To meet compliance and other requirements most organisations must keep authentic electronic records for at least seven years, whilst some contracts, insurance documentation, financial agreements, medical data and library materials needs to be accurately preserved for perhaps 100 years or more. Without effective trust these records are open to unauthorised changes, which will create substantial business risks and unforeseen claims.

Creating Trust

Trust can be provided for e-business documents by using digital signature and timestamping services within standard products. The problem is that even if 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, however there are two options to deal with this:

- Create long-term signatures that include a timestamp of the authenticated time of signing and also a signed response form a validation authority confirming that the signers certificate was good at the time of signing;
- Use historic validation services to check the Certificate Revocation List (CRL) that was current at the time of signing to determine if the signer's certificate was valid at the time of signing.

Either of these are good standards-based approaches and the latter has less dependence on enhanced security capability in end-user applications.

It is clearly better if the dependency on being able to trust a document is also passed to a specialist long-term trust solution that has been designed to offer archive creation and verification services. Ordinary applications will be unable to handle such advanced features for some years to come and so deploying a separate service as part of the business workflow process makes a lot of sense.

Archiving Services

For information that only needs to be kept for up to 7 years a simple digital signature with a timestamp is generally considered good enough. The digital signature will identify the author or approver of the document, or it might identify the organisation – particularly in the case where it is archiving and evidencing the unprotected data it received. Such notarisation can be done immediately by the web-application that receives the data, writing it to the evidence archive system and then passing the data into existing ERP, CRM or other business systems. Either a separate detached signature can be used and archived or an embedded PDF or XML signature could be applied – depending on the business needs. Such an archive system can be operated internally or an external service could be used. In either case the evidence data is produced immediately that the data is received.

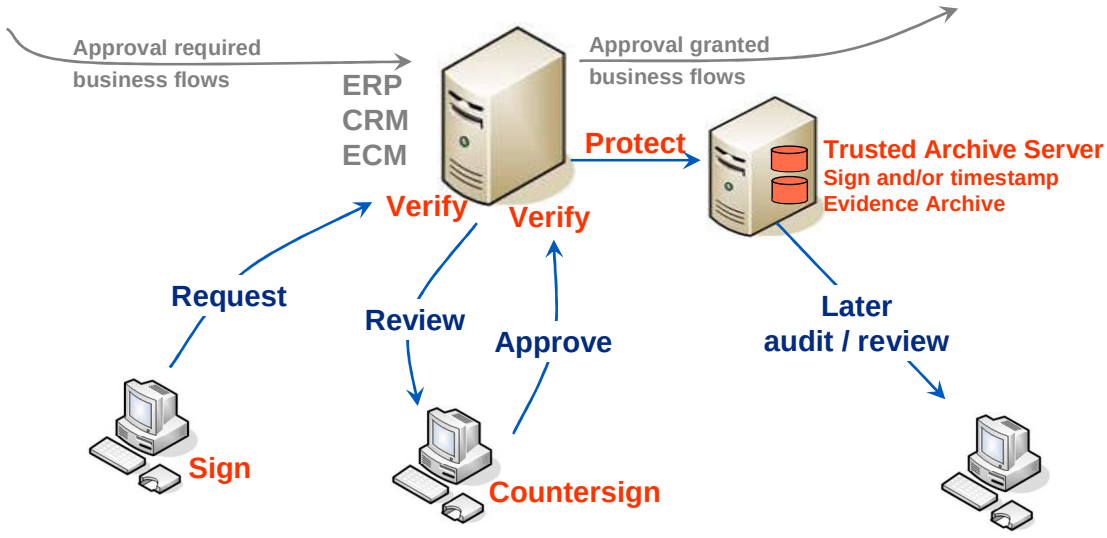
Currently businesses, even Governments and major banks, use algorithms and keys lengths that have a lifetime of just 10 to 15 years. Ultimately these signatures fail their purpose when it becomes too easy to forge any change to the trusted data. A simple archive service should therefore at least re-protect the data using high strength algorithms, for example the new German legal requirement for a permissible archive is to use RSA keys of 2048-bits and SHA-512 algorithms. This is expected to protect data for roughly 25 to 30 years.

Long term security

To archive and preserve data for the very long-term, that is beyond 30 years alternative approaches are required. Long-term evidence archive files are needed that can attest to the accuracy of a specific document or data file when they were first processed. These evidence archive files are best implemented as separate documents that have a self-describing XML structure designed to allow for multiple layers of digital signature and timestamp evidence to be wrapped around a hash of the original data. The draft IETF LTANS standard includes such as capability within its Evidence Records Syntax. This technique ensures that even as current security algorithms weaken and are perhaps even broken, new techniques can be applied to protect the original data and all previous evidence layers. Clearly careful thought needs to be given to the way in which such long-term evidence archive solutions are to be described, created, managed and used. Ascertia has considerable expertise in this area from delivering such a solution to a major national library.

Today the Ascertia Advanced Digital Signature Server (ADSS) Server delivers services that allow archive services to be readily implemented. Ascertia is currently working on an LTANS compliant Trusted Archive Server product. It is able to verify all signatures that are associated with the data being archived, as well as archiving unsigned or encrypted data.

Business Workflow Example



How can archived data be independently checked?

Using a self-describing archive allows the protected document type, the algorithms, the key lengths and the trust scheme to be identified and described. Thus the archived data can be accessed and the contents verified. Since the evidence archive is independent of the original document then verification can be achieved simply by being able to hash the data, verify the signatures and timestamp tokens.

Why is this necessary?

Without such protection it is quite easy to retrospectively change electronic documents especially if they are ever used outside of an internal Document Management System. However even within such a system they may be subject to changes by suitably privileged employees or contractors. Over the course of time it can be very difficult to prove that nothing has changed unless strong cryptographic techniques are used to secure the data.

Within a few years current cryptographic algorithms and key lengths will weaken as computers become faster and cheaper thus enabling brute force attacks to be contemplated. The other certainty is that user signing credentials will expire and sometimes may be revoked for various reasons even during their validity timeframe. The trust and assurance provided by a long-term evidence archive solution is a crucially important aspect of any notary service. Its applicability is not restricted to any vertical market – any business that keeps important data for any period of time (short, medium, long or indefinite) may need to show that the data is unchanged since it was approved or archived (or both) using clear proofs that stand up to independent examination by expert witnesses. Such results may themselves need to be signed to prove that the archive system is providing trustworthy information.

The bottom line is that any data that needs to be kept for longer than 10-15 years requires advanced and/or future-proofed protection.

Where would this approach make sense?

The archiving of business documents can apply anywhere that legislation, regulation or business risk requires it. The integration of such a service is not difficult to achieve.

- 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 ECM or document management systems

Need more information?

Ask Ascertia or its partners for details of how this can easily be added to your existing documents and workflow systems. Send emails to ***info@ascertia.com***