The Business Need for Long-Term Evidence Archiving

Many organisations need to ensure that important archived data and documents remain in their unchanged original form in 10, 20 or even 50+ years' 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, identity ownership and library data needs to be accurately preserved for perhaps 100 years or more.

The Security Issues

With any digital document it is easy to modify the content or copy the logos and create realistic but fraudulent documents. Unprotected PDF, XML or other electronic documents provide a future reviewer with no way of determining if a document is genuine or whether it has been modified since its creation. There is a solution to these needs – it is very easy to digitally sign and timestamp such data in a way that uniquely fingerprints the data and cryptographically preserves this mathematical proof of integrity.

Without effective trust these records are open to unauthorised changes, which will create substantial business risks and unforeseen claims if they are not addressed.

Creating Trust

Trust can be provided for e-business documents by digitally signing and timestamping them using standard products or services. One 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. A timestamp should also have an adequate certificate lifetime.

Some systems will fail to verify documents as soon as the signer's or timestamp authority 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 from 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 decision on whether to trust a document is passed to a well-designed and robust trust solution, designed to offer archive creation and verification. Service providers can also be used and can offer such services via web-pages or web services. Standard business applications are expected to 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. The original data can still be processed by the application but the trustworthiness can be first checked.

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

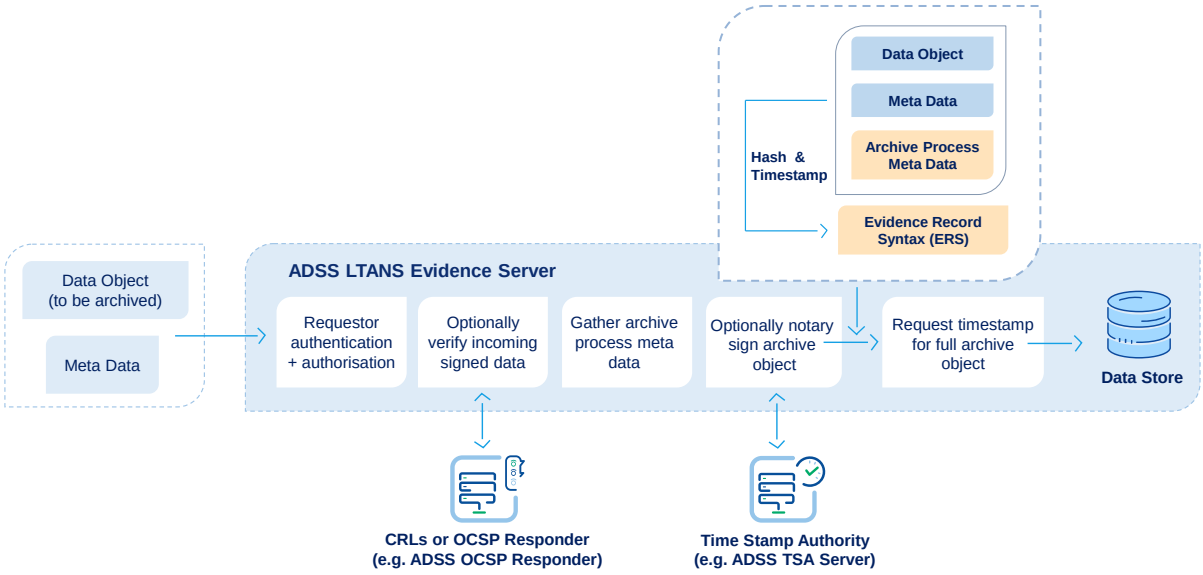
be done immediately by the web-application that receives the data, writing it to the evidence archive system and then passing the data into existing ERP, CRM or other business systems. Either a separate detached signature can be used and archived or an embedded PDF or XML signature could be applied – depending on the business needs. Such an archive system can be operated internally or an external managed service could be used. In either case the evidence record is produced immediately that the data is received.

Currently many organisations including Governments and major financial organisations, use algorithms and keys lengths that have a lifetime of just 5 to 15 years. Ultimately hash and signature key lengths and algorithms fail their purpose when it becomes too easy to forge a meaningful change to trusted data. An effective archive service should at a minimum be able to re-protect the data using current high strength algorithms. As an example the 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 20 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 Record Syntax data. 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 ADSS LTANS Evidence Archive Server delivers services that enables and effective archive service to be quickly and easily implemented. The ADSS Server is able to verify all signatures that are associated with the data being archived. Importantly it can also archive unsigned or encrypted data or data of any type.



How can archived data be independently checked?

Using a self-describing RFC 4998 ERS evidence records allow the protected document, the algorithms, the key lengths, the trust scheme and various other metadata items 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 and verify the timestamp signatures.

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 may be impossible 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.

- Financial instruments, insurance policy documents, loan agreements
- Central and local government documents, land registries
- Archive and library systems, education and professional qualification records
- Justice records, health records, births, deaths, marriages, licenses
- Engineering, architecture, planning, R&D drawings
- Test and trials data required for independent assessment and approvals
- Regulatory submissions in the financial or pharmaceutical and other markets
- e-Invoices, and other financial documents and records
- Policies, procedures, internal controls and compliance documents
- ERP, CRM, HR and ECM or document management systems

Further information on ETSI PAdES Part 4 LTV, XAdES-A and CAdES-A archive signatures can be provided on request

Need more information?

Ask Ascertia or its partners for details of how ADSS Archive Server can easily be integrated to protect your existing documents and workflow systems.

For further details see the Ascertia website www.ascertia.com or email info@ascertia.com.