Digital Signature Verification using Historic Data

Digital signatures are now relatively common; however historic verification of digitally signed data is not so widely understood. As more data is held in electronic form and as important documents need to be referred to over a period of time this area will become increasingly important and relevant to businesses, governments and individuals. For example legal agreements, government and financial documents need to be referred to and validated at various points during their lifetime. Sometimes this can be many years after the document was originally created, for example old tax records, patent data, land ownership. To support these needs various digital signature techniques can be used.

This paper discusses how the advanced digital signature features of Ascertia's ADSS Server can be used to fully address these requirements for long term signatures and historic validation.

Digital Signatures today

Digital signatures are in daily use for protecting data and proving the existence, origin and authenticity of documents. The concepts of this technology are well understood.

For example, a business sends a digitally signed contract to a business partner, the digital signature is verified, the contract is digitally countersigned and sent back and filed for future reference.

Some time later however the contract may need to be referred to, possibly as a result of a legal dispute or company audit. This may occur a few days or weeks after the original signatures or even some years later. As long as the document's digital signatures are able to be verified then the document can still be considered valid.

Digital Certificate Expiry and/or Revocation

In theory the digital signatures present in the document can be verified at any time and can show that the document hasn't been altered since the signature was applied and also that the digital signatures are still valid.

However, what happens if by the time the document is re-opened the digital certificate has expired or has been revoked by the issuing Certificate Authority? Also, what happens if some of the certificate data needed for the verification is not readily available?

Under these circumstances, the digital signature will be shown to be invalid and then it is up to the person viewing the document to understand and interpret why this should be.

There is clearly a need to provide a digital signature verification service that can make use of historic validation data. It would then be able to report that the digital signature was indeed valid at the time the document was signed.

Ascertia's ADSS Server and Historic Verification

The Ascertia ADSS Server has been designed to address these needs for historic signature verification and certificate validation. As long as ADSS Server has access to the necessary historic data, digital signatures can be verified at any specified date and time.

ADSS Server automatically downloads and stores Certificate Revocation Lists (CRLs) as they are issued by CAs and it can be manually pre-loaded with even older CRLs if required and use these during the validation process. All validation data (e.g. Trust Anchors, CRLs etc.) are maintained in the system database for future reference and use.

ADSS Server stores current CRLs in expanded form inside a database table so that it can provide real time responses quickly (instead of having to parse the CRLs at run time). Older CRLs are held in their original compact form within the database. The relevant historic CRL is then parsed at run time.

In summary ADSS Server can check historic digital signatures at any time in the past when it has access to the relevant trust data.

Handling of Grace Periods

ADSS Server offers considerable flexibility in establishing allowable validation policies. An example is around the handling of 'Grace Periods'. Some national regulations require that digital signatures are only considered valid after a grace period has elapsed. This allows for the possibility that a document is signed just before or just after the associated digital certificate has been revoked, but before the issuing Certification Authority has been able to report the revocation. If the digital signature is verified successfully once the Grace Period has elapsed, the recipient can be sure that the certificate was valid at the time of signing and certain legislations demand that grace periods are used for legal acceptance. ADSS Server supports such configurable grace period handling for signature creation and signature verification profiles.

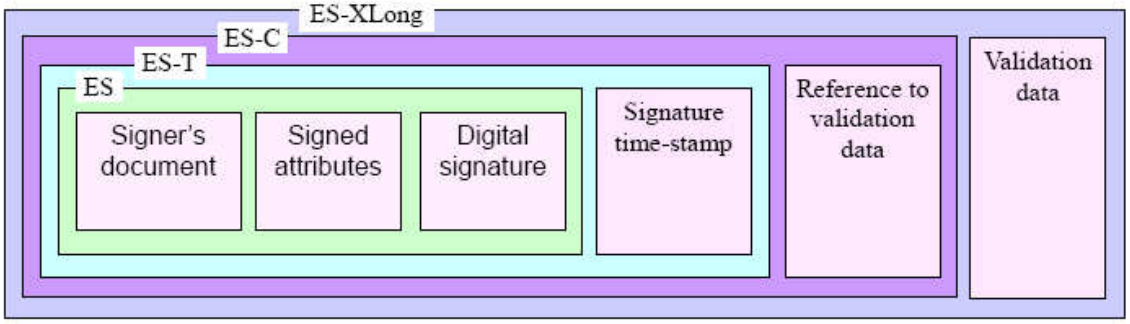
Long Term Digital Signatures

The historic validation of basic digital signatures requires a server based verification capability that has access to archive of historic trust data such as CRLs and ADSS Server is a class leading product for this. However a better approach to address long term signature verification is to include any necessary validation data along with the basic digital signature. This approach removes the need to load historic validation data.

ADSS Server also supports the creation and verification of these long term digital signatures.

ETSI Long Term Digital Signatures

ETSI has defined a number of signature formats that allow for the addition of timestamps and certificate validation data into a digital signature. These signatures are in effect wrappers around the basic digital signature. In the diagram below, the basic signature is referred to as ES. By adding a timestamp from a trusted time stamp authority (TSA) it then becomes an enhanced ES-T signature. Validation data can then also be added to form the long term signature (either ES-C or ES-XLong).



Depending upon the type of data and signature, the resulting long term signature is referred to as XAdES-X-L for XML signatures, CAdES-X-L for PKCS#7/CMS signatures and PAdES for PDF signatures.

The validation data that forms part of the long term signature can either be individual certificate status responses (OCSP) or complete Certificate Revocation Lists (CRL). Both must relate to the time when the document was signed and additionally the validation data must be for the full certificate chain and not just the signer's end-entity certificate.

ADSS Server provides support for creating these 'long term' signatures both at the time the document is signed and at a later date by enhancing an existing signature.

OASIS DSS/DSS-X Support

Ascertia follows the important industry standards and ADSS Server supports the OASIS DSS and DSS-X protocols. Using these protocols, ADSS Server is able to historically verify documents containing single and multiple signatures and to provide detailed Verification Reports as part of the protocol response. The OASIS DSS protocol can also be used for creation of long term signatures.

As an aid to business application development, Ascertia also provides an SDK so that developers can build simple signature creation and verification requests without the need to understand the underlying OASIS DSS/DSS-X, XML/SOAP request and response protocols. Versions of the ADSS Client SDK are available for different platforms (refer to the ADSS Client SDK datasheet for details).

Long Term Validation

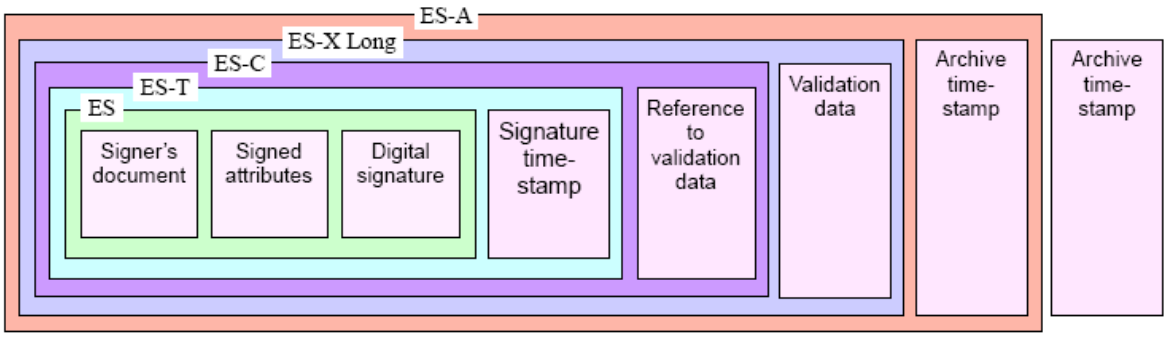
For documents that were digitally signed a long time in the past (say 10 or more years) the validity of the document's digital signatures and associated certificates may be open to challenge. The cryptographic algorithms used to sign the documents may now have become too weak to be relied upon and the digital certificates themselves may have long since expired (most only have a lifetime of a couple of years). Further, the stated time of the signature(s) may be questioned especially if the digital signature has not been officially timestamped or the timestamp authority's certificate itself has expired. The issuing Certificate Authority may also no longer be operational. To overcome these issues two different approaches may be employed:

- The first is to periodically add 'Archive Timestamps' to the long term ETSI signatures to create "AdES-A" signatures
- The second is to create Evidence Records for any archived documents.

These two approaches are discussed below.

Archive Timestamping

Over time digital signatures can become weaker due to advances in computing power and/or crypto-analysis techniques. To overcome this, ETSI long term digital signatures can be periodically archive timestamped with stronger algorithms. The timestamp protects the signature it envelops and the cryptographic strength is dependent purely that of the latest timestamp.

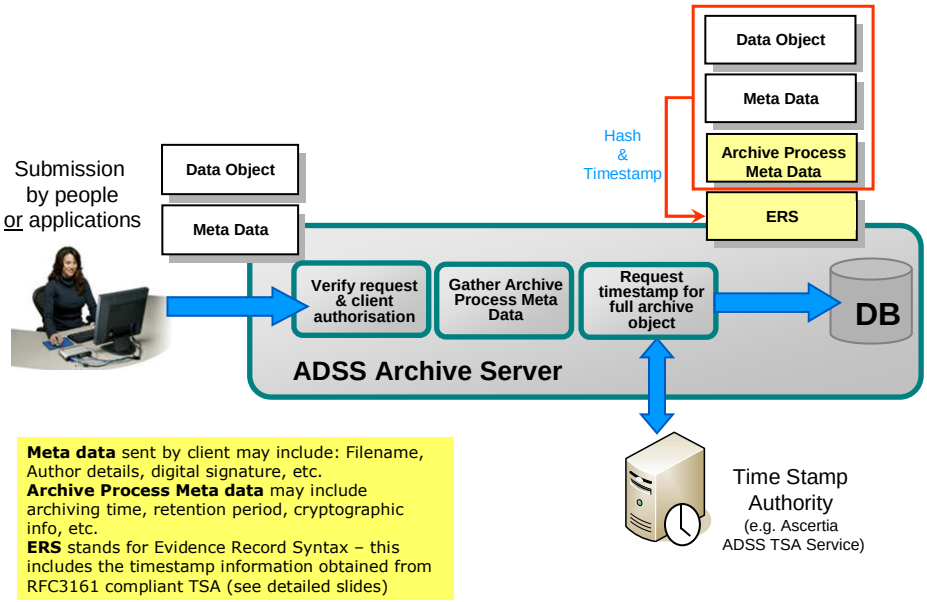


The resulting archive signature is referred to as XAdES-A for XML signatures and CAdES-A for PKCS#7/CMS signatures. ADSS Server supports the creation and verification of these archive timestamp signatures.

IETF Long Term Archive and Notary Services (LTANS)

LTANS based long term archiving provides an alternative to periodic re-timestamping of long term signatures. It can also be applied where ETSI signatures have not been used and so can be used to archive any data whether it is already signed or unsigned. It can even be used with encrypted data, i.e. the archiving component does not need to parse the data being archived in order to protect it.

In this case, signed archive evidence records (called Evidence Record Syntax, ERS) are created which wrap the archive data objects together with Meta Data, Archive Process Meta Data and a timestamp from a trusted Timestamp Authority (TSA).



Meta data may include items such as file names, author details, detached digital signatures etc. Archive Process Meta data may include archiving time, retention period, cryptographic information etc.

ADSS Archive Server provides full support for long term archiving i.e. the creation, renewal and verification of evidence records (ERS) and is compliant with the draft IETF LTANS standard. LTANS defines two encoding formats for the ERS one in ASN.1 format and one in XML, ADSS Server supports the XML format referred to as XMLERS. The LTANS interface for access the archiving authority is also XML/SOAP web services and referred to as Long Term Archive Protocol (LTAP).

The additional advantage of LTANS over the ETSI archive timestamp approach is that the Evidence Records can be automatically refreshed based upon a defined policy so that the business application doesn't need to be involved in trying to re-timestamp.

Re-evidencing can be based upon the use of lifetime timestamp authority certificates with a periodic assessment of algorithm strengths, or alternatively just on policy (e.g. automatically re-evidencing every couple of years).

Historic Certificate Validation

In addition to the OASIS DSS and DSS-X protocol standards, ADSS Server also supports other protocol standards such as XKMS and SCVP. These protocols for example allow for the historic validation of certificates and certificate chains if this is all that is required by the business application as compared to historical verification of full signatures.

Ascertia ADSS Client SDK also supports these protocols so that business applications can implement the required client-side functionality with just a few high-level API calls.

Signature and Certificate Quality Assessment

Another important aspect of signature verification is that of signature and certificate quality. The motive behind this is that in a large cross-border environment it becomes difficult to determine to what degree to trust certificates (and thus digital signatures) which are from foreign CAs.

This issue is recognised within the European Commission, and as a result the new PEPPOL (Pan-European Public Procurement On-Line) project aims to standardise quality criteria for all electronic signatures between enterprises and EU government institutions for all procurement processes. PEPPOL proposes the use of signature policies to define the acceptance criteria for e-signature and the provision of Validation Authority (VA) services based on the OASIS DSS Verify protocol and W3C XKMS Validate protocol. These and other protocols are already supported by ADSS Server.

The purpose of the quality ratings is to enable business applications to more easily decide if sufficient trust and assurance exists in signatures and certificates to allow transactions to be accepted. The way this works is that ADSS Server is configured to respond with rating values for certificate quality (from 0 to 6), independent CA assurance (from 0 to 7), and hash and public key qualities (0-5). The business application can now make its decisions based not only that the certificate is valid but also that it meets the required quality levels. The Ascertia solution paper Creating PEPPOL solutions for eProcurement projects discusses this area in further detail – shown as a PDF document on the Ascertia website.

ADSS Server – Future Development

As can be seen from the above, ADSS Server is at the forefront of digital signature technology and is Ascertia's core strategic product and thus subject to continuous R&D investment; so you can be assured that Ascertia will support your business needs long into the future. A list of satisfied major client references is available on the Ascertia web-site.