Using Trusted Notary Services to Avoid Trust Issues

Traditionally public notaries have provided an important trust service in witnessing the execution of legal and commercial documents. They have verified the identity of the parties, witnessed the signatures and vouch for their later authenticity.

As the business world moves on-line to save substantial costs and to "go green" the same trust services are still required. Similar trust services can now be offered for electronic documents using online trusted notary services that use advanced long-term digital signatures also called digital notary seals.

This paper describes how online trusted notary services can easily be offered for PDF documents. PDF is the most common business document format; however other document formats could be supported by using the same approach within other desktop products.

The Problem

When end-users receive signed PDF documents there is no certainty that they can correctly verify the embedded digital signatures. For example, is their PDF viewer able to use the relevant trust anchors (Root CAs) so that the signer's credentials can be verified? Is revocation checking enabled to determine the current status of the signer's credential? If CRLs are being used, is the CRL a reasonable size to download and check? Can the signature verification process provide information on the quality of the signature and its acceptability for the current business application? Can it historically verify signatures at the time of signing for which the certificates are now expired?

Without the appropriate settings in the PDF viewer and some education of the user a valid signature may be seen as not trusted or an invalid signature may be shown as okay!

The Solution

An independent authority such as a digital notary can attest to the fact that signatures on important documents are trustworthy and the document can be reliably acted upon both now and into the future. The notary service can handle these complex signature verification decisions leaving the end-users and business applications with a simple response on whether the document can be trusted or not. Positive evidence can be provided to the end-user because the response from the notary is signed and timestamped. In some cases the notary may even choose to mark the PDF document with its own digitally signed seal so the notarisation evidence is bound within the document.

Ascertia recommends three approaches to this:

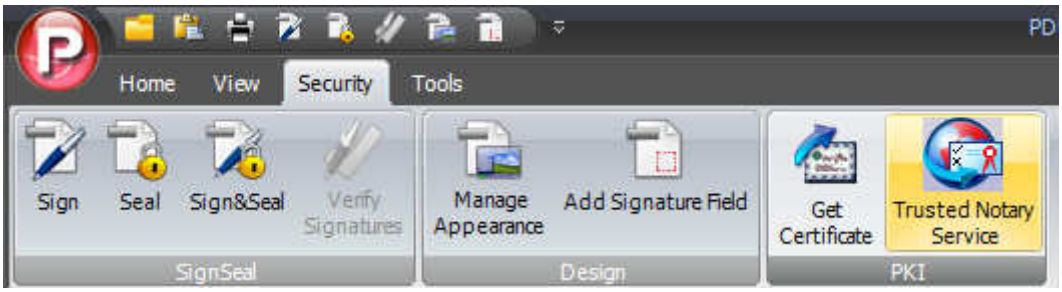
- Using Ascertia PDF Sign&Seal - a stand-alone desktop product that now contains an option to request services from an online notary service provider. Only the signatures are sent for checking so that document confidentiality is maintained.
- Using notary service web-pages that ask the user to upload a document so that the signature(s) can be checked. In this case the service provider must be trusted to handle the document with care.
- Using notary email service that enables a user to send a signed document via email to a service, e.g. notary@globaltrustfinder.com (available for testing from July 1st) so that the signature(s) can be checked. A return email to the sender will provide verification information from the notary.

Of course there will always be subtle requirements to meet specific business requirements, such as keeping copies, signing and timestamping response data, perhaps even PDF receipts confirming the verification and trust status. All this can be readily accommodated within a solution delivery.

Looking at the first of these options – a simple, effective solution can be implemented using:

- PDF Sign&Seal – to review the PDF and send the signatures to the notary
- ADSS Enterprise Server - this advanced signature, timestamp and verification product provides server-based trust services that enable organisations to offer notary services to verify signatures and provide signed and optionally sealed responses to end-users.

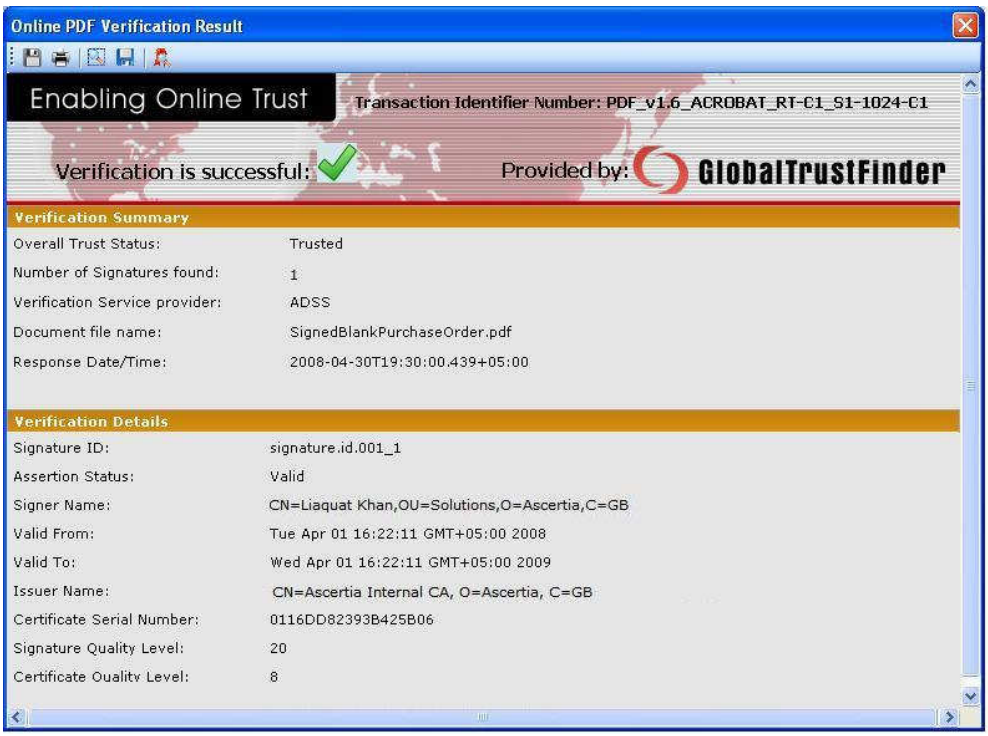
Within the desktop PDF Sign&Seal product the end-user can request the verification of the signatures via a notary service from a toolbar button, as shown highlighted below:



When the button is clicked PDF Sign&Seal extracts the signature(s) from the PDF document and sends these to the configured online notary service to be verified. Note that there is no loss of confidentiality since it is just the signatures that are sent to the notary service. This is all the notary needs to verify the signatures and validate the signer's certificates.

The communication with the notary is real-time and transparent to the user. The signed response message from the notary's verification service is then internally processed by PDF Sign&Seal to ensure it can be trusted and is consistent with the request.

Multiple signatures are handled seamlessly with the response from the notary detailing the verification status of each signature. PDF Sign&Seal displays these in a simple result window for the user:

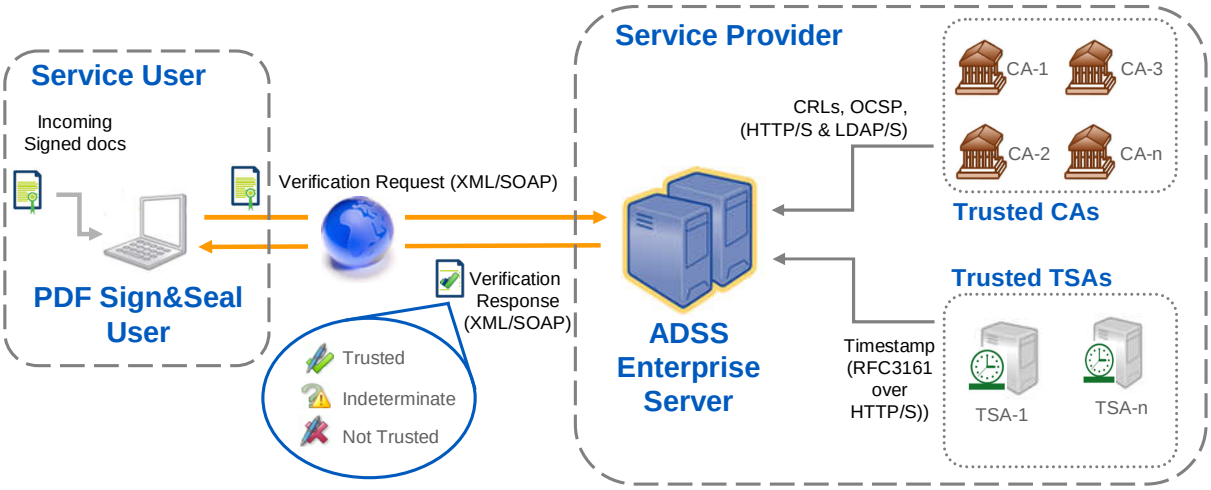


The format of this window is flexible and can be easily adapted by Ascertia if necessary. The user can see who the notary is from the verification summary and the logo (in this case

GlobalTrustFinder / ADSS). The response from the ADSS Server is always signed so that PDF Sign&Seal and other applications can trust it. The Transaction ID in the top banner is a unique reference number managed by the ADSS Server for dispute resolution purposes. The server also maintains a secure log of all request and responses to the verification service. PDF Sign&Seal can also optionally record a log of all transactions made by the user.

Solution Architecture

The following diagram illustrates the notary service architecture (without the ADSS Gateway):



The workflow details are:

- An end-user uses PDF Sign&Seal and clicks the trusted notary button
- PDF Sign&Seal communicates with the ADSS Enterprise Server using a standard web service call (XML/SOAP). Full details of the XML schema are available from Ascertia. A high level API is provided for enabling verification services in your other digital signature applications.
- The ADSS Enterprise Server verification service is responsible for handling all aspects of signature verification. This includes:
  - ➔ Checking the signature is cryptographically verified
  - ➔ Checking the signer's certificate was issued by a trusted issuer CA
  - ➔ Checking the signer's certificate has not been revoked (using CRLs or OCSP calls)
  - ➔ Checking the signer's certificate has not expired
  - ➔ Checking the signature and certificate meet minimum quality levels (i.e. based on certificate policy, asymmetric algorithms, and key lengths). PDF Sign&Seal can request these minimum quality levels based on its configuration files.
- The response from the ADSS Enterprise Server is digitally signed so that it can be trusted by PDF Sign&Seal. It may also contain a secure timestamp from a back-end Time Stamp Authority (TSA) for long-term validity.

Further information is available about the advantages of PDF Sign&Seal, ADSS Enterprise Server and the Secure eMail Server from the Ascertia web-site.

Ask Ascertia or our partners for details of how such trust services can easily be added to your existing documents and workflow systems – email us on ***info@ascertia.com***