



ADSS Server CDS Edition **Using CDS Certificates to Sign PDF and PDF/A documents**

In these days of sophisticated fraud attempts, using techniques such as phishing and document forgery, organisations must ensure that they provide trust in their internally or external issued documents.

Both end-users and business systems need to know that the document they have received is:

- ❖ Actually from the person/entity that it is claiming to be from
- ❖ A formal final copy that someone is taking responsibility for
- ❖ That the content is original and unchanged

To meet compliance and other requirements most organisations must keep authentic electronic records for several years, whilst some contracts, insurance documentation, financial agreements, medical data and library materials may need to be accurately preserved for perhaps 10 years or more. Without effective trust these records are open to unauthorised changes, which will create substantial business risks and unforeseen claims.

Creating Long-Term 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 solutions approaches:

- ❖ Create special long-term signatures that include a trusted timestamp proving the time of signing and also a signed response from a validation authority confirming that the signer’s certificate was valid 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.

Ascertia can offer both solutions, however this document focuses on the first solution.

Using Adobe Rooted CDS Certificates

Everyone in the connected world is able to read PDF documents. Most people use Adobe Reader 7, 8 and 9 although more people are also using Ascertia PDF Sign&Seal. By default Adobe Reader only trusts the Adobe Root Certificate Authority and so only Adobe CDS certificates are immediately considered as trustworthy. Of course other trusted CAs can be added but this requires end-user intervention.

When signing with such a certificate the end-user is given clear information about its trust:

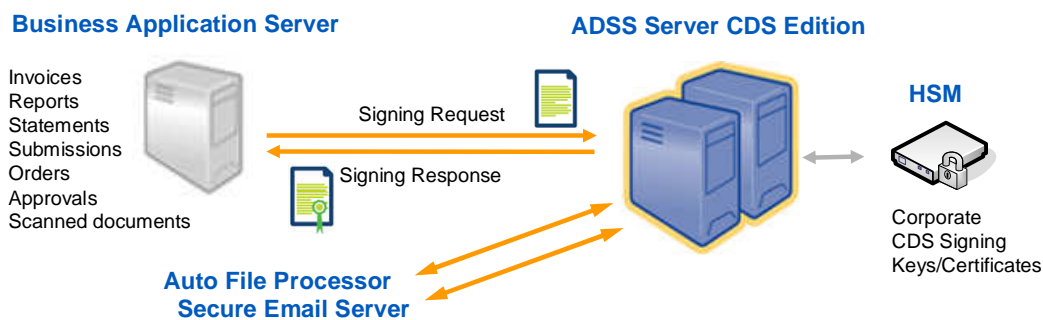


The special CDS certificates are available from a number of service providers. Included within the certificate cost is access to a timestamp authority service. The embedding of a timestamp token and the signer’s certificate validation information enables long-term trust.

The Ascertia Solution

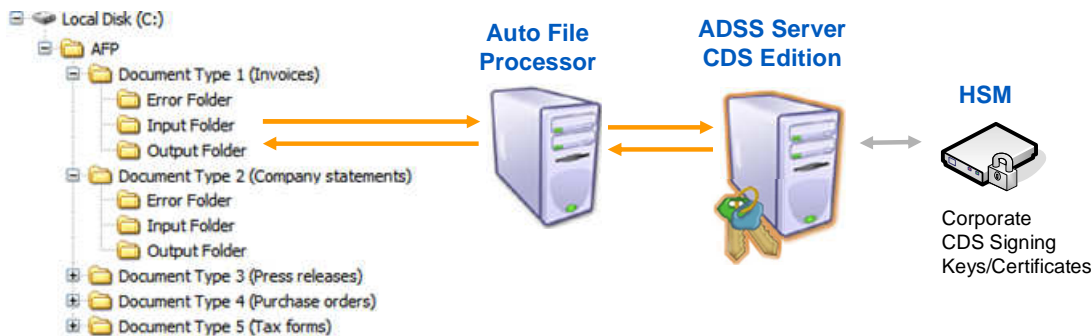
There are very few competent solutions that provide an effective and secure environment to (a) manage the CDS certificate, (b) authenticate the requests to sign, (c) securely audit the transaction, (d) provide management reports on the number of operations (this is often needed to comply with CDS certificate use licenses), (e) provide flexible signature features including multiple options for signature placement, signature appearance and document certification, (f) optionally enforce internal approval (authorisation) of requests to sign with a corporate CDS certificate held on the server, (g) provide high-level client APIs to ensure easy integration, and (h) provide high availability solutions using two or more security servers.

Ascertia has used its knowledge and expertise in this specialist area to create a world-class product called ADSS Server CDS Edition. This delivers all these features in a simple solution. It can be used by integrating it with existing applications using very high-level APIs, or using Ascertia's watched folder application (Auto File Processor), or by using the Ascertia Secure Email Server.



The ADSS Server makes it particularly easy for business applications to sign PDFs. The ADSS Client SDK provides a high-level API that can make calls to the server using as few as 5 lines of code. ISO 19005 PDF/A documents are signed and stay PDF/A compliant

Auto File Processor is a popular approach because there is no integration work. If files are available in an input folder then they can be picked up using Auto File Processor, an intelligent application that then makes requests to ADSS Server to sign using a defined signature profile.



Further Information

Separate solution sheets explain how the Ascertia Secure Email Server and PDF Sign&Seal desktop products work. All Ascertia datasheets and solution sheets are signed with a CDS certificate using long-term certifying signatures.

Create Corporate Trust today! Access Ascertia evaluation software from the main website www.ascertia.com - ask Ascertia or our partners for further details of how our products easily be easily added to your existing documents and workflow systems - info@ascertia.com