ascertia

Authorising Corporate or Qualified Signatures

It is often necessary to digitally sign documents on behalf of an organisation or a role holder (e.g. CFO) using Qualified Certificates or other high-trust certificates. To be available for automated processes such certificates need to be held securely on a server protected by a Hardware Security Modules (HSM) or perhaps a smartcard. In this document we refer to all signatures produced by such keys as “corporate signatures”. In more complex cases multiple keys and certificates may be used to enable different legal entities or role-holders to sign and approve documents for multiple purposes.

The Authorisation Problem

The challenge of using qualified or high trust keys and certificates resident on a server is to ensure that each signing process is properly authorised. Effective internal controls are needed to ensure that access to the signing mechanism (and key) is protected and only available to appropriate staff. Qualified Advanced Electronic Signatures require that signing data is a wilful act performed by the signer. Auditors also require evidence of review and approval to ensure that internal controls are effective.

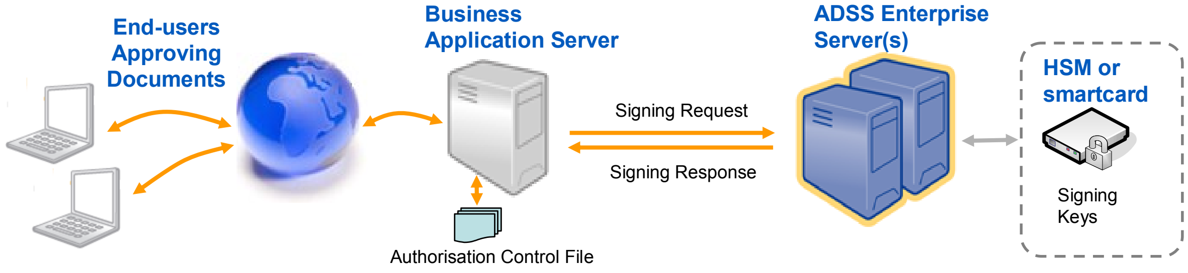
More sophisticated usage scenarios can require multiple role-holders within an organisation to approve the signing request before a server signature is applied. Each approval needs to be checked so that their intent to sign and approve is clear. Some recent high-profile bank fraud cases have similar parallels. Compliance regulations also demand such action.

The Solution

Ascertia’s response to these requirements has been to provide a mechanism that allows requests for server signatures to be suitably authorised by selected staff. The OASIS Digital Signature Services (DSS) specification provides a standard protocol for requesting server-side signatures. Ascertia has extended the OASIS DSS request message to allow it to include authorisation information from one or more users (referred to as “authorisers”).

A typical workflow is: Business users interact with an online web application that shows one or more documents that need server-side signatures to be applied, e.g. corporate reports, invoices, government submissions, etc. The web application creates an Authorisation Control File, which contains the input documents plus the signatures of the authorisers indicating their approval - these signatures are referred to as “authorisation signatures”. The web application sends the Authorisation Control File to the ADSS Server as part of the request message for server-side signing. ADSS Server can verify and accept or reject these authorisation control files. It already provides a wide range of high-level, easy-to-use signing, verification, timestamp, long-term signing and archiving services.

The following diagram summarises how users can interact with a web application to build such an Authorisation Control File that can then be passed to the ADSS Server for processing:


End-users Approving Documents
Business Application Server
Signing Request
Signing Response
Authorisation Control File
ADSS Enterprise Server(s)
HSM or smartcard
Signing Keys

ADSS Enterprise Server authenticates the requests from the business application. It also checks that this application is approved to use the required signing profile. Signing profiles are pre-defined by security administrators and they have an option to select an authorisation profile that must be fully satisfied before the server-side signing process can start.

The authorisation profile defines an M of N check – it contains a list of allowed authoriser certificates (the number within the list is N). The profile is then set to define the minimum number (M) of authoriser signatures that must be presented within the Authorisation Control File in order to approve the use of the signing profile and its signing key. If less than M signatures are present then the request fails. If M or more authorising signatures are seen and fully verified then the request is approved and signing of the file(s) commences.

Enabling Authorisation Signatures

Ascertia provides an intelligent high-level ADSS Client SDK library for .NET and Java environments that enables easy integration of ADSS Server with business applications. For authorised signing this is the typical workflow detail:

1. The web application presents one or more documents to the user and builds an authorisation control file (ACF) using the intelligence within the ADSS Client SDK.
2. The first user reviews the files they are being asked to authorise and then the application requests them to sign it, thereby creating an authorisation signature. ADSS Go>Sign Applet is used to hash and sign using a smartcard, software credentials or roamed credentials. This action is repeated as required for other users, thereby creating multiple authorisation signatures.
3. As each user signs, checks are made to ensure that the input files remain unchanged.
4. When the workflow has completed and all authorisation signatures are gathered by the web application, it embeds the ACF in a request to ADSS Server for server-side signing.
5. ADSS Server authenticates the web application using the defined mechanism (AuthID, SSL and signature), checks its rights to use the selected signing profile and signing key/certificate, verifies the ACF signatures and checks them against the M of N authorisation policy. It also checks that the specified files have not changed. Finally if all these checks are okay then the files are signed and returned to the business application.
6. NOTE: ADSS Server keeps a copy of all request and response messages (optionally including the business documents) in its signing service transaction logs

Separately the web application may wish to check individual’s roles and other attributes such as payment limits. Such items can be easily placed within an LDAP directory and checked in real-time. Since these elements are dynamic it is recommended that these organisation specific attributes are checked by the business application.

Summary

ADSS Server already provides easy to use digital signature creation and verification services that enable business applications to add trust to important business documents and data. All the complexity of signing and verifying documents can be delegated away from business applications and on to the dedicated and secure ADSS Server.

Authorised Signing ensures that an indelible audit trail can be created that binds individual approvals to corporate or automated signing actions. The benefits for the organisation are that it can be easier for individuals to sign and approve a batch of documents – rather than having to arduously sign each one. Later on there can be no denying the intent to sign, no suspicion that the files had changed during or after approval and no doubt that the final documents were approved by a suitable number of authorised parties. This adds valuable trust and evidence to critical business information workflows.

Ask Ascertia or our partners for details of how such techniques can easily be added to your existing documents and workflow systems - ***info@ascertia.com***

Identity Proven, Trust Delivered