



Authorising Corporate Signatures

Often it is necessary to digitally sign a document on behalf of an organisation rather than an individual, in this paper we refer to such signatures as “corporate signatures”. Typically a corporate digital signature is created using a special corporate signing key. This is typically held centrally and is controlled by the relevant business application. Within an organisation, there may be a need for several corporate signing keys, serving different purposes including signing invoices from different legal entities, signing purchase orders or receipts or approving documents for multiple external purposes.

The Problem

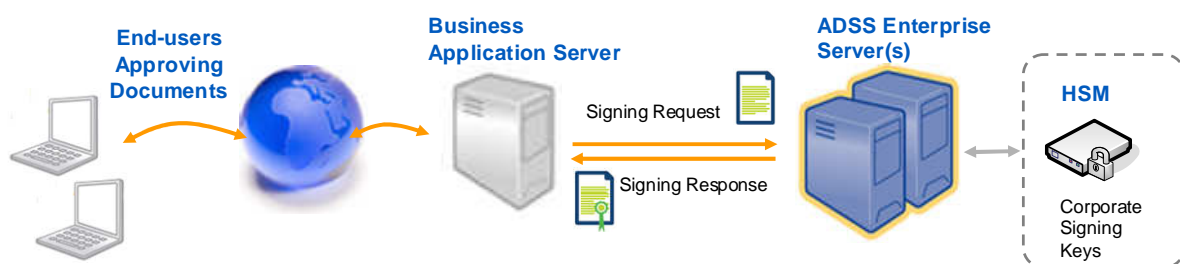
The challenge of using corporate signatures is to ensure that fine grained controls can be applied to enforce security policies that protect access to the signing profiles and the associated signing key and certificate use. Audit teams also require strong evidence so that the effectiveness of such internal controls can be assessed. Ascertia believes that more sophisticated usage scenarios will require one or more individual role-holders within an organisation to sign and approve the use of such corporate signatures. Their role-based rights need to be assessed and their intent to sign must be properly recorded, otherwise uncertainty and doubt can be placed in the minds of people that may assess such evidence later on. Some recent high-profile banking cases have similar parallels.

Solution Approaches

There are a few ways to address the need of how to authorise and track the access to such corporate signing keys, to ensure only authorised role-holders can request signatures as part of their official duties. Ascertia’s ADSS Enterprise Server has been designed to make such tasks easy whilst providing a range of high-level, easy-to-use trust services including the ability to control the application of corporate signatures on a wide variety of document formats.

Business Application Control

In the following approach business users interact with a business application, which is responsible for requesting corporate signatures once the criteria for signing are met, e.g. the monthly invoice run commences:



ADSS Enterprise Server authenticates the requests from the business application and then applies the relevant digital signature using the signing profiles (policies) that have been defined by security administrators. It controls all security administrators, all signing profiles, signing keys and log records thus simplifying things for the business application. Application-level authentication options are:

- ❖ SSL/TLS client certificates used by the business application to secure the session
- ❖ XML Request signing certificates used by the application to sign the requests
- ❖ Other network specific controls (e.g. firewalls) to limit access to the ADSS Servers

It is thus the role of the front-end business application to determine that a wilful action to sign the data with a corporate signing key has been taken before proceeding to request corporate signatures from the ADSS Server. This architecture ensures that the ADSS Server acts as e-Trust service provider and is independent of the business specific logic or workflow.

User Authentication Techniques

In some cases business applications wish to authenticate that one or more end-users have approved the request for a corporate digital signature to be created. There are a number of techniques that could be used, such as:

- ❖ Basic username/password authentication
- ❖ One time password or two-factor authentication (using tokens, mobile phones etc.)
- ❖ Digital signature techniques

Ascertia recommends the use of digital signatures and in particular the use of ADSS GoSign applet. This provided user authentication and long-term evidence that the user approved the signing of a particular document or transaction. It also enables multiple users to counter-sign and approve such a request.

It is conceivable to get the end-user to digitally sign using (a) a random challenge, (b) a transactional summary or (c) the request message sent to the ADSS Enterprise Server instead of the document which requires a corporate signature, but these alternatives need synchronisation or other extra work to provide strong evidence. PDF documents lend themselves very usefully to such workflows simply because users can clearly see what they are being asked to sign.

A typical workflow with ADSS GoSign-based user approvals is:

1. The web application presents the document to the user and requests the user to sign it using a locally held signing key (either in browser or in smartcard/USB token)
2. The web application uses the ADSS Server to verify and trust the user's signature on the document. The business application may perform other business specific checks (role, signing levels etc.) and it should record the signed document for future reference
3. If the user's signature is trusted then the web application requests a corporate signature

As mentioned before multiple approvals can be made within such a business application workflow to ensure that key documents such as financial summary statements, project reports, tender submissions are approved prior to final corporate signing and submission.

ADSS GoSign can also be used in its .NET and Java variants to have desktop applications authorise documents or transactions.

Summary

ADSS Server provide high-level security services that enable multiples business applications to have controlled access to corporate signing keys in a way that enables them to maximise their use of strong e-trust techniques (i.e. digital signatures), whilst retaining the option to use internal controls such as HR databases to account for changing roles and approval authorities.

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***