ADSS Server – Using Signing & Verification Profiles

ADSS Server is a multi-function server providing digital signature creation and verification web services, as well as supporting infrastructure services like Time Stamp Authority (TSA) services, OCSP validation services and certification services.

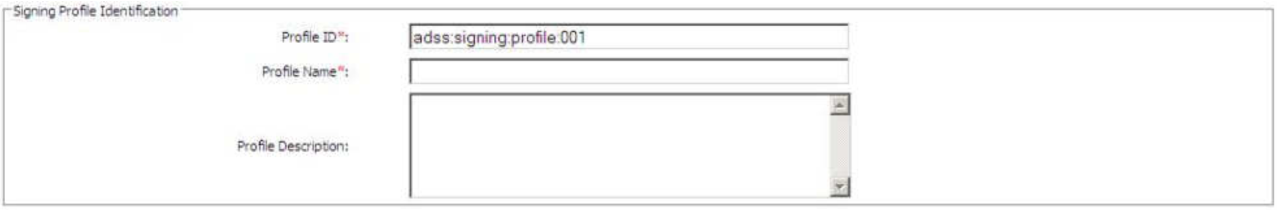
This solution sheet discusses the different profiles (i.e. sets of configurations) which can be created on the ADSS Server. Specifically it describes the attributes of signing and verification profiles and how these can be associated with the business applications that make requests to the ADSS Server. This approach ensures that access to specific trust profiles and associated parameters, like digital signature keys, are only available to authorised business applications.

Signing Profiles

The purpose of signing profiles within the ADSS Server is to configure the digital signature attributes and appearances that are to be produced. Once a signing profile is configured by suitably privileged ADSS Server administrator, then business applications can reference this signing profile in the web services request message. This removes all the configuration management overhead from the applications. Any number of signing profiles can be configured to suit different application needs. The main attributes that can be configured in a signing profile are:

The Signing Profile Identifier:

Signing profiles are uniquely identified within the ADSS Server via a system defined Profile ID:



Signing Profile Identification

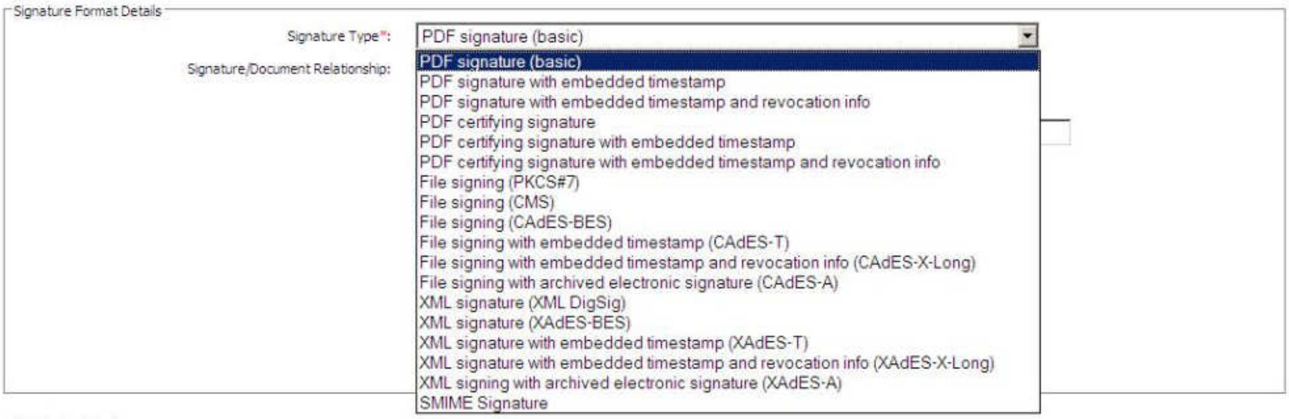
Profile ID*: adss:signing:profile:001

Profile Name*:

Profile Description:

The Signature Type:

One of the main elements of a signing profile is the type of signature to be generated, in ADSS Server v3.4 it is possible to configure a signature type from a full set of signature standards:



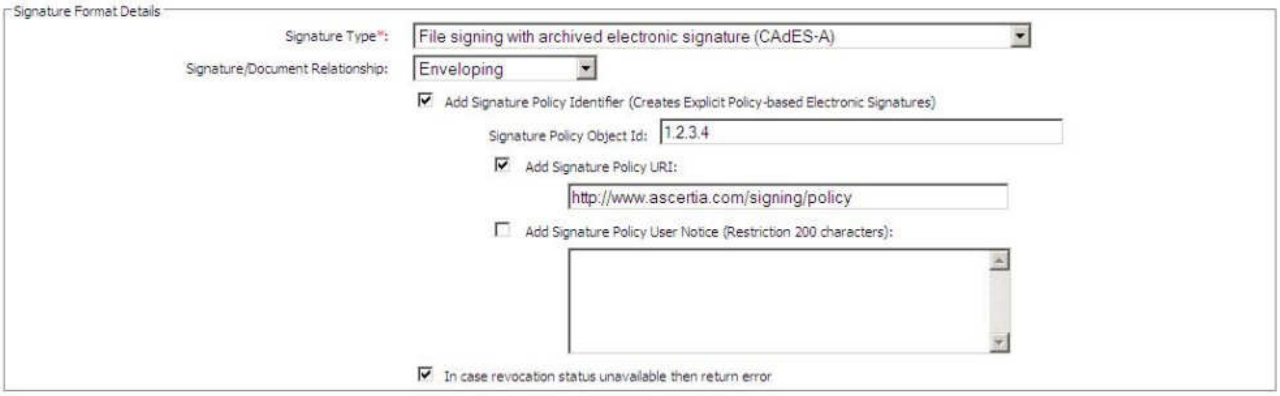
Signature Format Details

Signature Type*: PDF signature (basic)

Signature/Document Relationship:

PDF signature (basic)
PDF signature with embedded timestamp
PDF signature with embedded timestamp and revocation info
PDF certifying signature
PDF certifying signature with embedded timestamp
PDF certifying signature with embedded timestamp and revocation info
File signing (PKCS#7)
File signing (CMS)
File signing (CAdES-BES)
File signing with embedded timestamp (CAdES-T)
File signing with embedded timestamp and revocation info (CAdES-X-Long)
File signing with archived electronic signature (CAdES-A)
XML signature (XML DigSig)
XML signature (XAdES-BES)
XML signature with embedded timestamp (XAdES-T)
XML signature with embedded timestamp and revocation info (XAdES-X-Long)
XML signing with archived electronic signature (XAdES-A)
SMIME Signature

Explicit Policy-based Electronic Signatures (ES-EPES) are supported in ADSS Server v3.4 onwards. These are configured separately from this drop-down menu because many of these advanced signatures could also have ES-EPES elements embedded within them. The settings for ES-EPES profiles are:



Signature Format Details

Signature Type*: File signing with archived electronic signature (CAdES-A)

Signature/Document Relationship: Enveloping

☑ Add Signature Policy Identifier (Creates Explicit Policy-based Electronic Signatures)

Signature Policy Object Id: 1.2.3.4

☑ Add Signature Policy URI:

http://www.ascertia.com/signing/policy

□ Add Signature Policy User Notice (Restriction 200 characters):

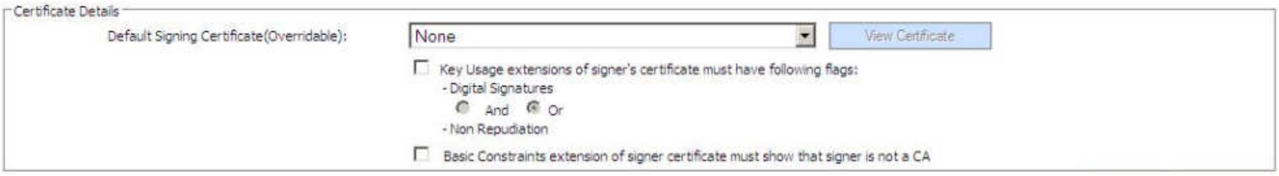
☑ In case revocation status unavailable then return error

This enables administrators to define the Signature Policy OID to be used when creating signatures under this signing profile. A Signature Policy URI and user notice can also be configured to be embedded within the signature produced.

As shown above, the signature format allows the signature / document relationship to be defined, “Enveloping” means the signature wraps around the document, “Enveloped” means the signature is embedded within the document, and “Detached” means the signature is provided as a separate object to the original document.

The Signing Certificate:

It is possible to configure a default certificate to be used with this signing profile. This certificate can be overridden in the request thus allowing business applications to use one signing profile with the range of certificates that are available to it – see later.



Certificate Details

Default Signing Certificate(Overridable): None

□ Key Usage extensions of signer's certificate must have following flags:
- Digital Signatures
○ And ● Or
- Non Repudiation

□ Basic Constraints extension of signer certificate must show that signer is not a CA

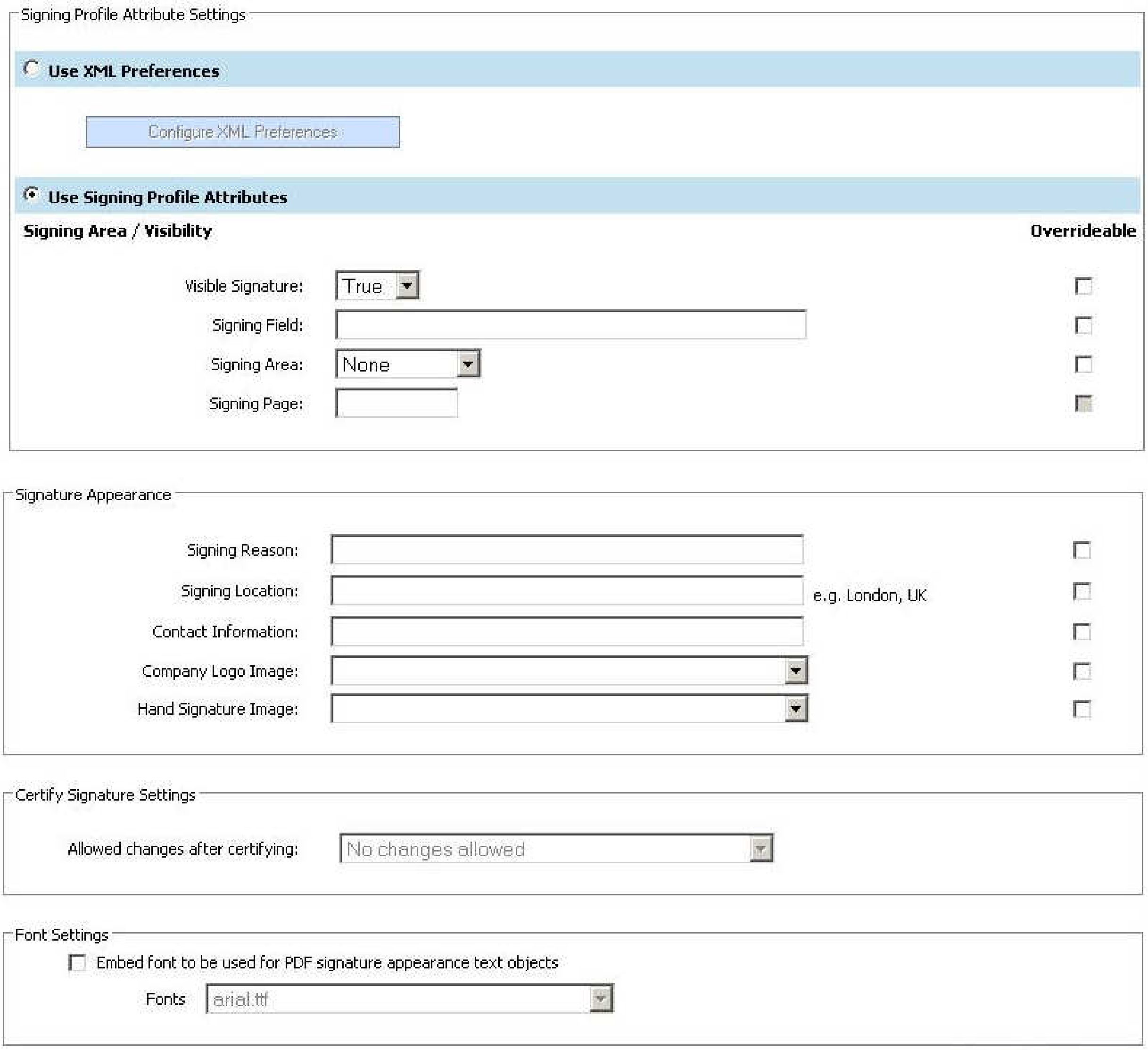
This is also where you can define the type of certificate that is acceptable for signing purposes under this signing profile. In many cases a Key Usage of “non-repudiation” is desirable or even mandatory.

Signature Appearance Details:

PDF documents have the ability to show a digital signature appearance within the document. Ascertia ADSS Server has sophisticated set of controls to determine how signature appearances should display. These options include the dimensions of the signature, where it should be placed on the PDF document, whether labels are to be used, whether reason for signing, location, date and time and contact details are shown or not. Hand-signature and company logos can be applied and even engineering seals are possible.

ADSS Server can sign existing blank signature fields and create signatures on multiple pages and also identify the ‘last’ page – a useful feature when dealing with variable length documents.

The following screenshot shows the signing profile settings GUI:



Signing Profile Attribute Settings

○ **Use XML Preferences**

Configure XML Preferences

● **Use Signing Profile Attributes**

Signing Area / Visibility		**Overrideable**
Visible Signature:	True	□
Signing Field:		□
Signing Area:	None	□
Signing Page:		□

Signature Appearance

Signing Reason:		□
Signing Location:	e.g. London, UK	□
Contact Information:		□
Company Logo Image:		□
Hand Signature Image:		□

Certify Signature Settings

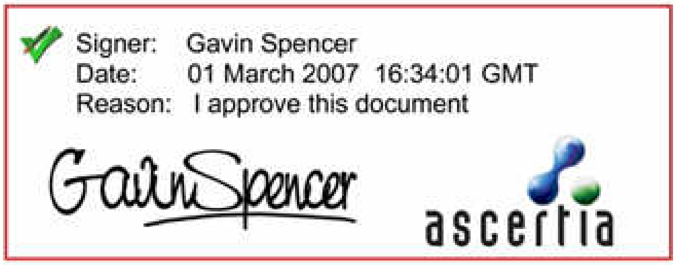
Allowed changes after certifying: No changes allowed

Font Settings

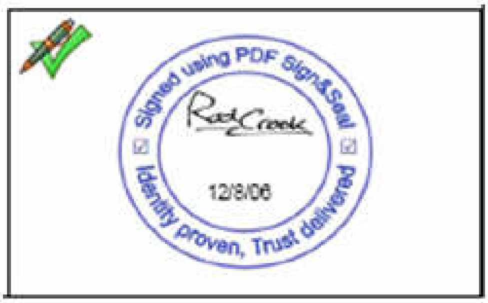
□ Embed font to be used for PDF signature appearance text objects

Fonts arial.ttf

If the overrideable flag is ticked by the ADSS Server Administrator, this enables a business application to provide override information for the specified parameter when using this profile within a specific request message. XML preferences can be used to modify the signature appearance to create various signature styles, e.g.:



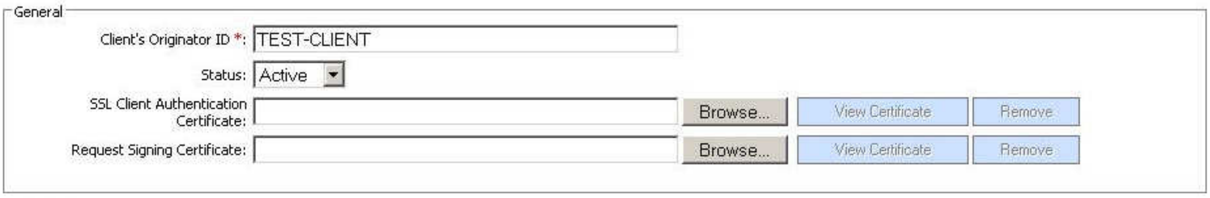
Signer: Gavin Spencer
Date: 01 March 2007 16:34:01 GMT
Reason: I approve this document



Authenticating Business Applications

Business applications are clients to the ADSS Server. They can be authenticated using any of the following three techniques depending on the level of security desired:

- Registering a business application within the ADSS Client Manager and assigning it an “Originator ID”. The business application must then use this “Originator ID” in its service request messages in order for it to be authenticated successfully by ADSS Server.
- The service request messages can be sent over an SSL connection with client authentication enabled. The business application’s SSL client certificate must be registered within ADSS Server and the certificate’s Subject Common Name value must match the “Originator ID”.
- The business application can sign the service request message using a request signing certificate. This certificate must be registered within the ADSS Server. The signature format is XML DSig.



General

Client's Originator ID *: TEST-CLIENT

Status: Active

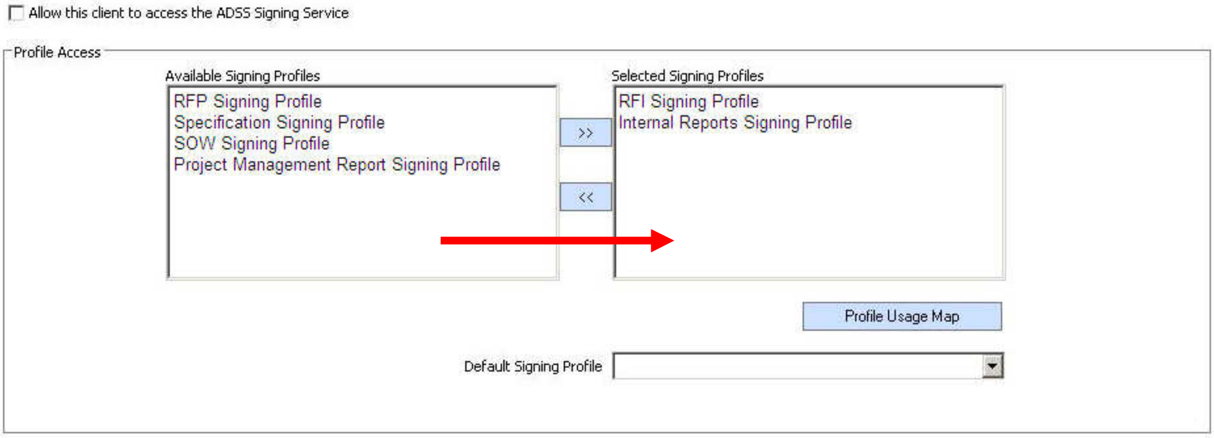
SSL Client Authentication Certificate:

Request Signing Certificate:

All three levels of security can be used together.

Authorising business applications for specific profiles

When registering business applications on the ADSS Server it is possible to configure which of the existing signing profiles (as discussed above) are to be made available for this business client as shown below. The first checkbox within the Client Manager defines whether the business application can make signing service requests:



☐ Allow this client to access the ADSS Signing Service

Profile Access

Available Signing Profiles

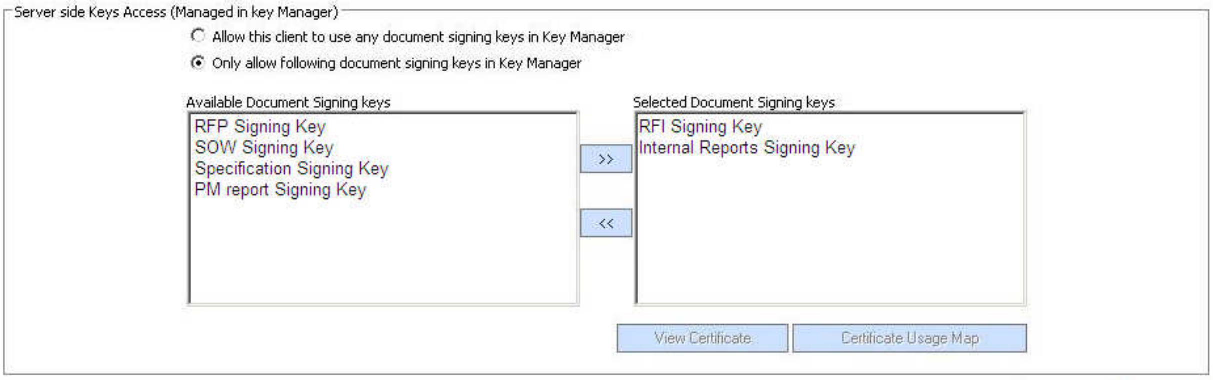
RFP Signing Profile
Specification Signing Profile
SOW Signing Profile
Project Management Report Signing Profile

Selected Signing Profiles

RFI Signing Profile
Internal Reports Signing Profile

Default Signing Profile:

Authorised administrators can simply select an available profile and move it across to the selected list by clicking on the ‘>>’ button. This updates the profiles assigned to this business application. In a similar way administrators can also control which set of server held keys and certificates are available to this business application for use with the signing profile:



Server side Keys Access (Managed in key Manager)

○ Allow this client to use any document signing keys in Key Manager

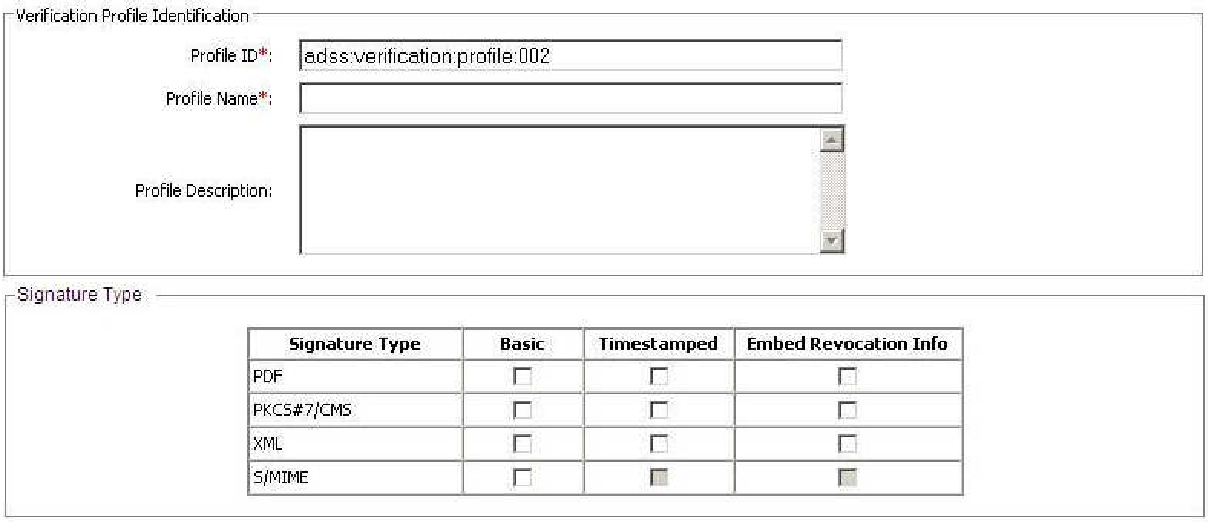
● Only allow following document signing keys in Key Manager

Available Document Signing keys	Selected Document Signing keys
RFP Signing Key SOW Signing Key Specification Signing Key PM report Signing Key	RFI Signing Key Internal Reports Signing Key

In summary it is possible to restrict which business applications can make signature creation service requests, which signing profiles they can reference, which document signing keys they can use, the format of the signatures to be applied, where and how these will appear.

Verification Profiles

In a similar way to signing profiles, the ADSS Server supports the concept of Verification Profiles. These define the type of signatures that can be verified:



Verification Profile Identification

Profile ID*: adss:verification:profile:002

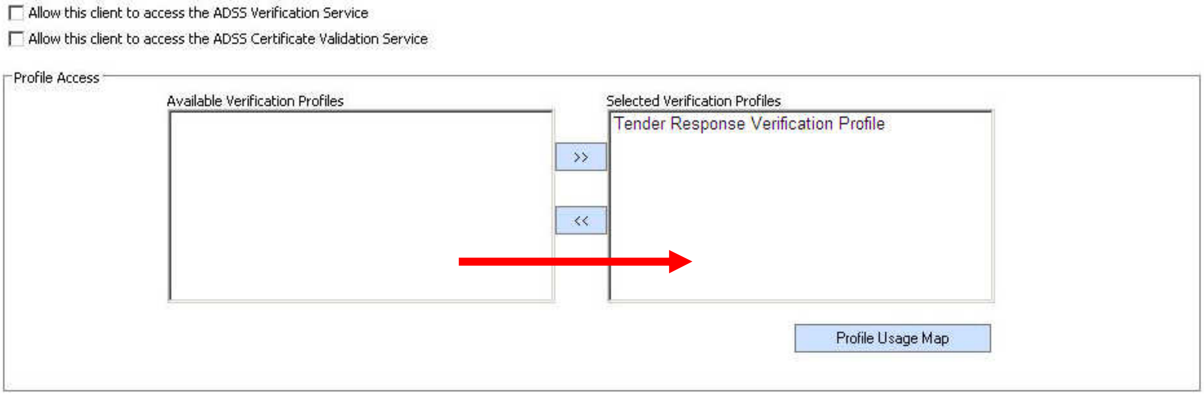
Profile Name*:

Profile Description:

Signature Type

Signature Type	Basic	Timestamped	Embed Revocation Info
PDF	□	□	□
PKCS#7/CMS	□	□	□
XML	□	□	□
S/MIME	□	▨	▨

The configured verification profiles can then also be assigned to specific business applications. :



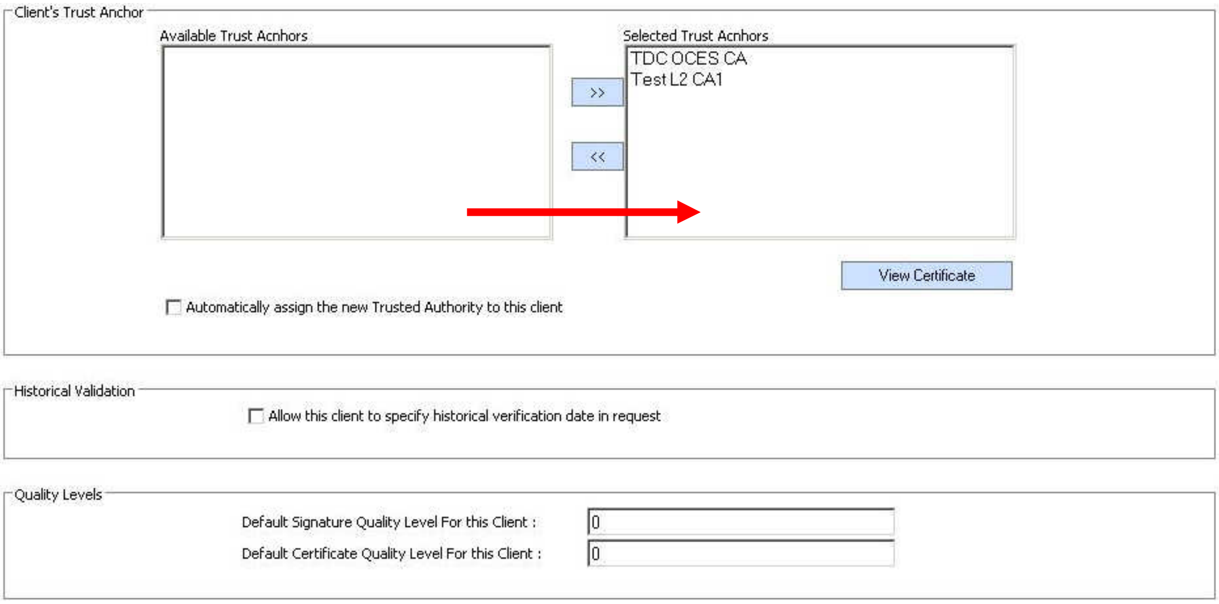
□ Allow this client to access the ADSS Verification Service

□ Allow this client to access the ADSS Certificate Validation Service

Profile Access

Available Verification Profiles	Selected Verification Profiles
	Tender Response Verification Profile

Importantly it is also possible to assign specific sub-set of trust anchors to business applications so that there is no need to trust all CAs that are registered on the ADSS Server for other clients:



Client's Trust Anchor

Available Trust Acnhors

Selected Trust Acnhors
TDC OCES CA
Test L2 CA1

□ Automatically assign the new Trusted Authority to this client

Historical Validation

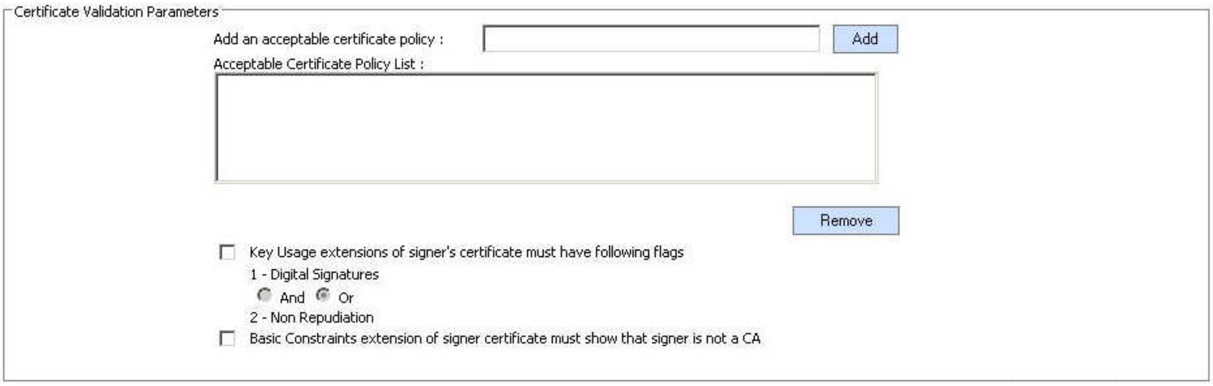
□ Allow this client to specify historical verification date in request

Quality Levels

Default Signature Quality Level For this Client : 0
Default Certificate Quality Level For this Client : 0

Minimum signature and certificate quality levels can be configured per business application to enable application to reject signatures that for example are not qualified signatures, or do not use a smart-token to protect the private key, or use acceptable algorithms.

The administrator can also configure the list of acceptable certificate policies which are required by the business application and the low-level certificate checks which must be performed on the signer’s certificate:



Certificate Validation Parameters

Add an acceptable certificate policy :

Acceptable Certificate Policy List :

□ Key Usage extensions of signer's certificate must have following flags
1 - Digital Signatures
○ And ● Or
2 - Non Repudiation
□ Basic Constraints extension of signer certificate must show that signer is not a CA

ADSS Server v3.5 will provide fine-grained signature policy control per business application.

Summary

The ADSS Server provides a rich set of features for supporting different signature types, configuring different signing and verification profiles and linking these to business applications. Strong authentication, authorisation and role based controls together with secure logging of operator actions and application request/responses ensure the highest levels of security.