ADSS Server v8.4.0 –

Gateway Services Guide

ASCERTIA LTD

FEBRUARY 2026

Document Version- 1.0.0

CONTENTS

FIGURES

1 Introduction

1.1 Scope

This document explains the role of Gateway Services in ADSS Server. It describes how different gateways, such as OCSP, Verification, Signing, RAS, and CSP, work as secure entry points for client applications. Each gateway checks requests for correct format, required information, and client authorization before passing them to the back-end service. This helps protect the back-end services, ensures standards compliance, and allows only trusted requests to be processed.

1.2 Intended Readership

This document is for system administrators, security officers, integrators, and application developers who use ADSS Server Gateway Services. It will help readers understand how the gateways work, the type of checks they perform, and how they protect and optimize the back-end services.

1.3 Conventions

The following typographical conventions are used in this guide to help locate and identify information:

- Bold text identifies menu names, menu options, items you can click on the screen, file names, folder names, and keyboard keys.
- `Courier New` font identifies code and text that appears on the command line.
- **`Bold Courier New`** identifies commands that you are required to type in.

1.4 Technical Support

If Technical Support is required, Ascertia has a dedicated support team. Ascertia Support can be reached/accessed in the following ways:

Website	https://www.ascertia.com
Email	support@ascertia.com
Knowledge Base	Ascertia Community Portal

In addition to the free support services detailed above, Ascertia provides formal support agreements with all product sales. Please contact sales@ascertia.com for more details.

When sending support queries to Ascertia Support team send ADSS Trust Monitor logs. Use the Ascertia's trace log export utility to collect logs for last two days or from the date the problem arose. It will help the support team to diagnose the issue faster. Follow the instructions on how to run the trace log export utility.

2 Application Gateways

An application layer gateway (ALG) is a type of security software or device that acts on behalf of the application servers on a network, protecting the servers and applications from traffic that might be malicious. The application gateway accepts incoming traffic on one or more listeners. Here, a listener is a logical entity that checks for connection requests. It is configured with a frontend IP address, protocol, and port number for connections from clients to the application gateway.

ADSS Server provides gateways for its service modules that will be discussed in this document.

3 Gateway Services in ADSS Server

Gateway Services in ADSS Server are designed to protect back-end services by preventing them from being directly exposed to the internet. This ensures that all services operate in a secure and controlled way

ADSS Server provides gateway options for the following modules:

- OCSP
- Verification
- Signing
- RAS
- CSP

This document gives an overview of how each gateway works and the role it plays in securing requests before they reach the back-end service. All gateway features are controlled through the ADSS Server license.

When the gateway sub-module is enabled, the server instance can only function as a gateway, and other configuration options will not be available. If the gateway sub-module is not included in the license, only the standard service option will appear in the Service Manager.

For a gateway-enabled module, at least one back-end server address must be configured in the Service Manager. During installation with a gateway license, sample data is not installed. In the case of an upgrade, the system will continue using any server addresses that were already configured in the existing gateway sub-module.

4 OCSP Gateway

The ADSS Server OCSP Service is a powerful implementation of the Online Certificate Status Protocol (OCSP). It provides up-to-date certificate revocation information using either CRLs or real-time data. The service follows the IETF standards RFC 6960 and RFC 8954, and partly RFC 5019, and can handle certificates issued by multiple CAs defined in the Trust Manager.

In **Gateway mode**, the OCSP Gateway checks that each incoming request is a valid OCSP request based on these standards. It makes sure all required fields are present, the request format is correct, and the client is properly authenticated. Only valid requests are forwarded to the back-end OCSP Server, while invalid ones are blocked

4.1 Implementation of OCSP Gateway

The OCSP Gateway operates in the OCSP Service by following the below-mentioned two modes:

- **Service**
  In the Service mode, the OCSP Service will receive the revocation status requests, process the requests and return the results.

- **Gateway**
  In Gateway mode, the OCSP Service operates as an intermediary. Instead of processing requests directly, the gateway verifies the request structure and authenticates the client through the client manager. If the validation is successful, the request is forwarded to the back-end OCSP Server according to the configurations described below. If the validation fails, an error message is sent back to the requesting application. In this setup, the operator is responsible for configuring the address and other settings for the back-end service.

4.2 Configuration of OCSP Gateway in ADSS Server

When enabled, this OCSP Service instance will function as a gateway for the back-end OCSP Server. The OCSP Service will verify the request structure and validate the client. If successful, it will relay the request to the back-end OCSP Server using the specified configurations.

Follow the instructions below:

1. Launch the ADSS Server Console
2. Navigate to OCSP Service → Service Manager

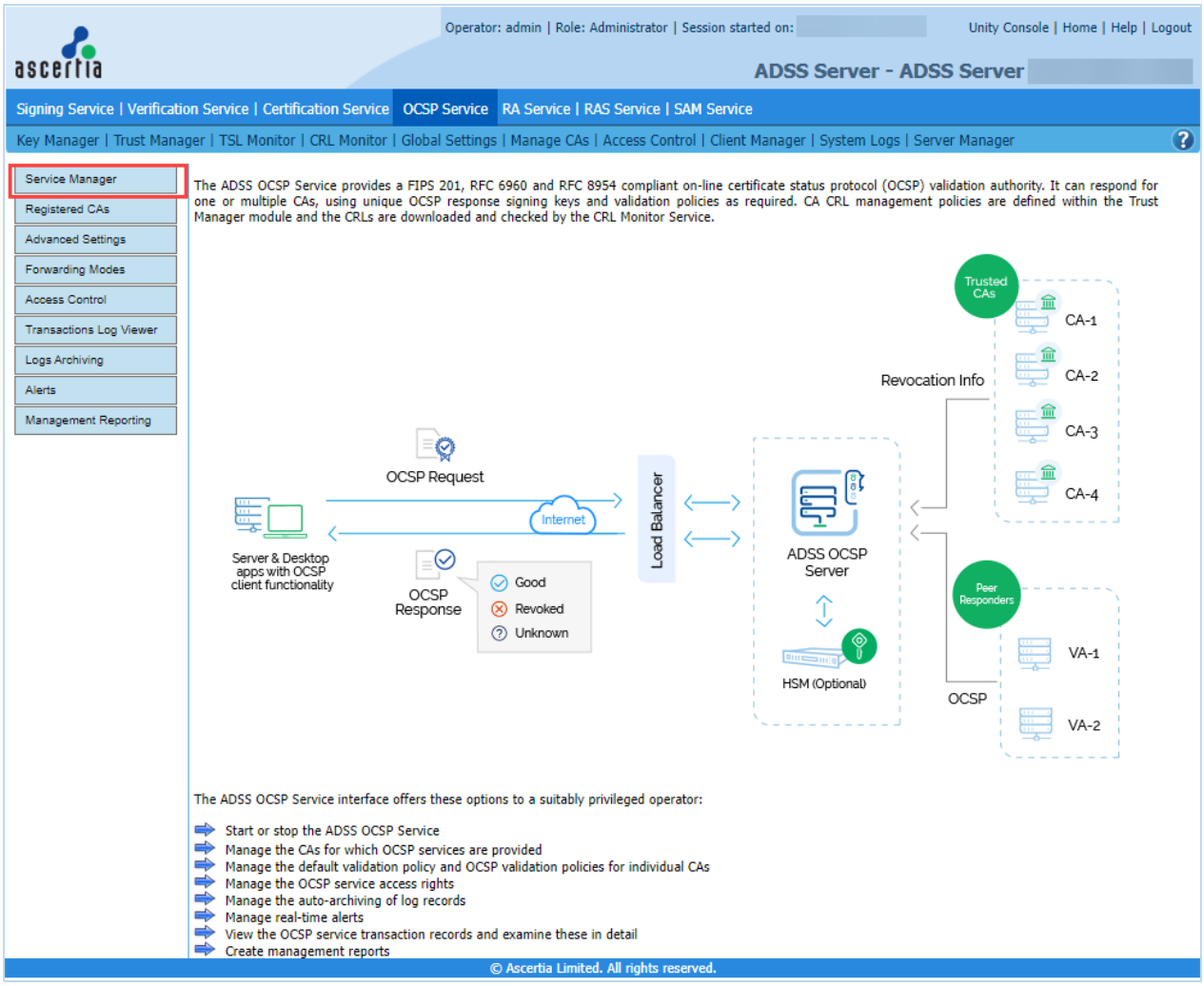

Figure 1 – OCSP Service – Home

3. Mark the ‘Enable Gateway Mode’ radio button , it will display the following screen:

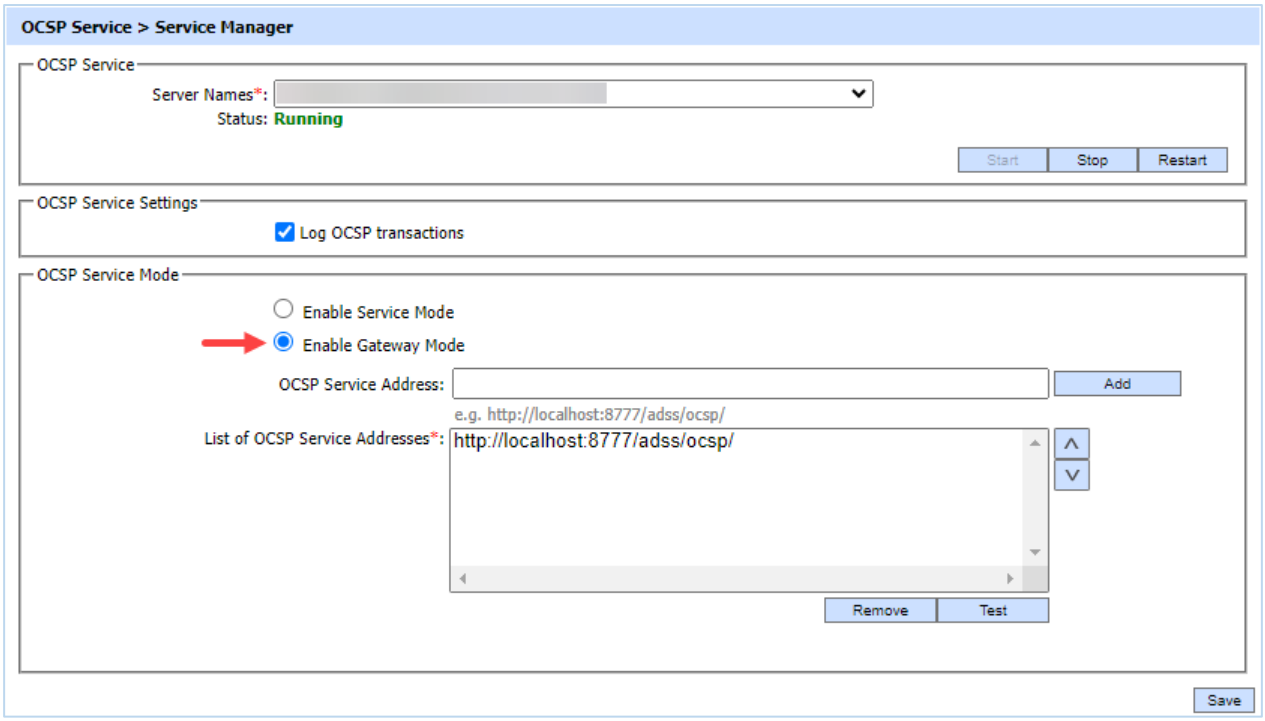

Figure 2 – OCSP Service – Service Manager

4. Once the radio button is enabled, its relevant fields will start displaying on the screen. The list of fields that becomes available are:

    a. **OCSP Service Address:** This field displays the OCSP Service Address(es) used to forward requests to the back-end OCSP Server. You can add multiple service addresses. The Test button allows you to check if the service is available, and the Remove button lets you delete a configured service address.

    b. **Remove:** the Remove button lets you delete a configured service address.

    c. **Test:** The Test button allows you to check if the service is available.

5 Verification Service Gateway

The ADSS Server Verification Gateway is the main entry point for verification requests from client applications. It ensures that only correct and safe requests reach the back-end Verification Service.

In **Gateway mode**, the service checks each request against the DSS/Verification schema. It confirms that the request is properly structured, includes all required information, and is free from harmful content. The client is also authenticated through the Client Manager. If everything is valid, the request is forwarded to the back-end service; otherwise, an error is returned

5.1 Implementation Modes of Verification Gateway

The Verification Gateway operates in the Verification Service by following the below-mentioned two modes:

- **Service**
  In the Service mode, the Verification Service will receive the verification requests, process the requests and return the results.

- **Gateway**
  In Gateway mode, the Verification Service operates as an intermediary. Instead of processing requests directly, the gateway verifies the request structure and authenticates the client through the client manager. If the validation is successful, the request is forwarded to the back-end Verification Server according to the configurations described below. If the validation fails, an error message is sent back to the requesting application. In this setup, the operator is responsible for configuring the address and other settings for the back-end service.

5.2 Configuration of Verification Gateway in ADSS Server

The Verification Gateway will be configured in ADSS Server by enabling the 'Enable Gateway Mode' option. If this option is enabled, the current instance of the Verification Service will function as a Gateway for the back-end Verification Server.

Follow the instructions below:

1. Launch the ADSS Server Console
2. Navigate to Verification Service → Service Manager

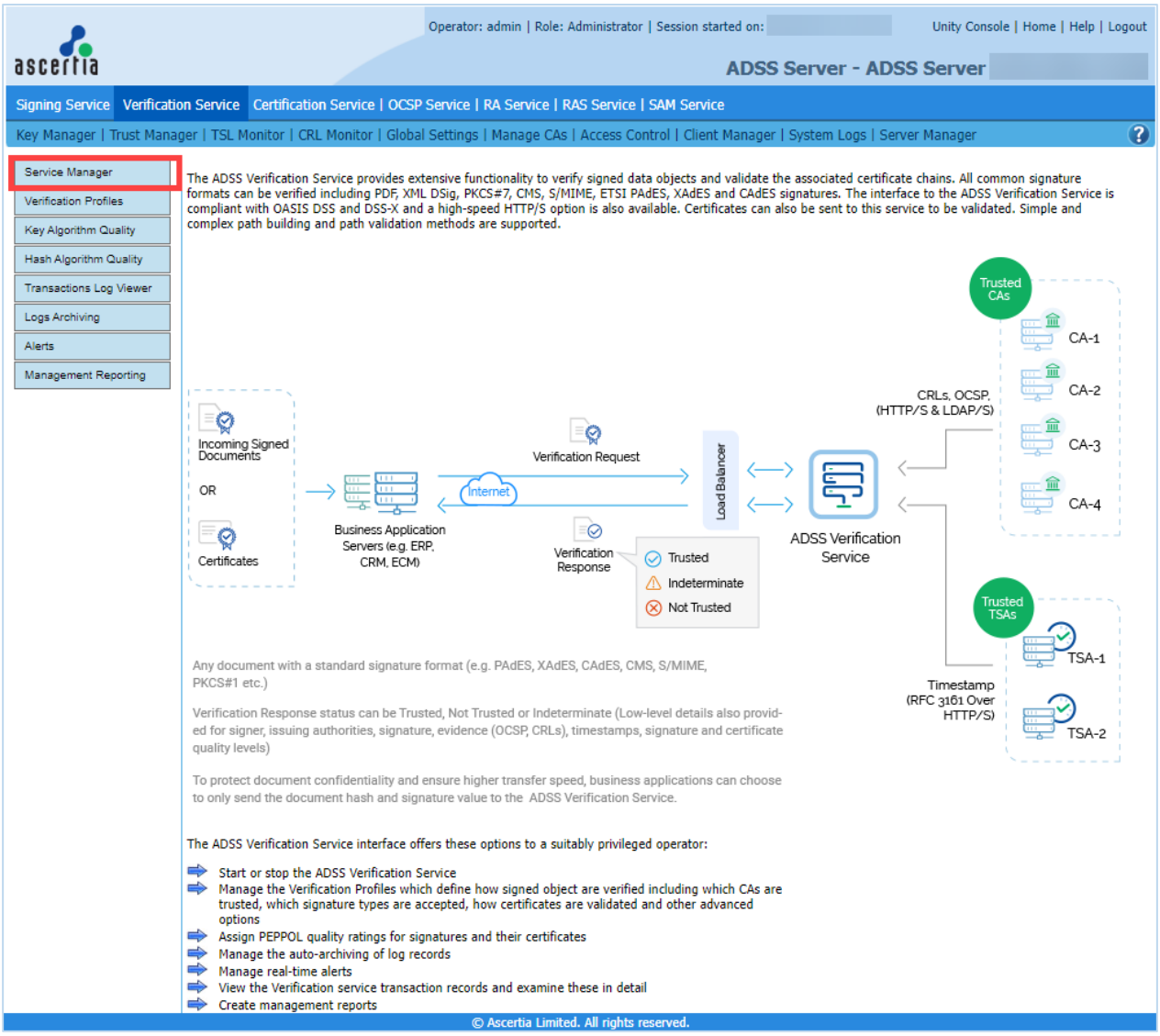

Figure 3 – Verification Service – Home

3. Mark the 'Enable Gateway Mode' radio button , it will display the following screen:

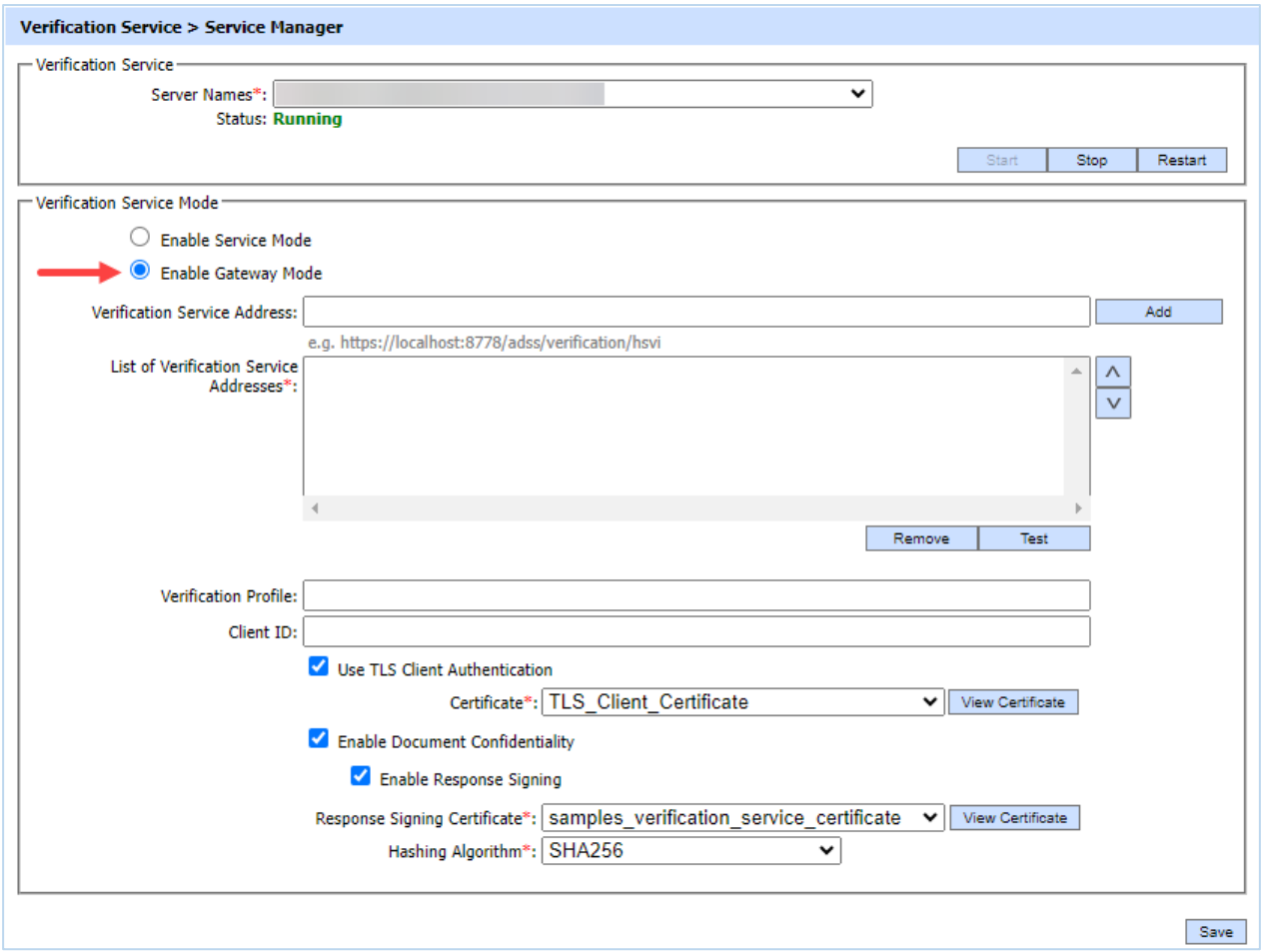

Figure 4 - Verification Service – Service Manager

4. Once the radio button is enabled, its relevant fields will start displaying on the screen. The list of fields that becomes available are:

    a. **Verification Service Address:** The Verification Service Address displays the location of the back-end Verification Service to which all requests will be sent through the gateway. You can input multiple addresses for the verification service, and arrange them in a preferred order. If the gateway encounters issues with the first address, it will attempt to connect using the subsequent addresses in the designated sequence.

    b. **Verification Profile:** This is a profile set up within the back-end service, which the gateway includes in every request it sends. If a profile is included in the request, the gateway will disregard the profile configured in this field and use the one received in the request instead. Note that if the operator hasn't configured any profile here, and the client application also doesn't include any profile in the request, the back-end service will utilize the default Verification Profile to handle the request.

    c. **Client ID:** The gateway functions as a client for the back-end service, requiring prior registration in the Client Manager of the back-end service using a unique Client ID. This same Client ID must be configured on this screen and will be included in every request sent by the gateway to the back-end service.

    d. **Use TLS Client Authentication:** If communication between the gateway and back-end service necessitates TLS Client Authentication, you must select this option. Once selected, a drop-down menu will appear below this checkbox, listing TLS Client Authentication Certificates for you to choose from.

e. **TLS Client Authentication Certificate:** This TLS Client Authentication Certificate is used by the gateway to authenticate itself with the back-end service over TLS. If the 'Use TLS Client Authentication' checkbox is checked, you must select a certificate from the list provided.

5.2.1 Enable Document Confidentiality

It's important to prevent the document from being sent to the back-end service for signature verification in order to maintain the document confidentiality. When the document confidentiality checkbox is enabled, only the signatures and hash data will be sent to the back-end Verification Service, rather than the entire document. This applies even when a single document contains multiple signatures.

To use this feature, enable the checkbox is mentioned in the screen below:

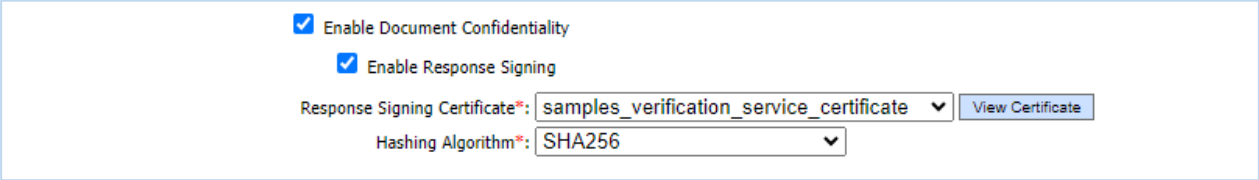

Figure 5 - Verification Service – Enable Document Confidentiality

The configuration items are explained below:

a. **Enable Response Signing:** This checkbox is accessible to the operator when the 'Enable Document Confidentiality' option is turned on. When enabled, it allows the response received from the Verification Service to be signed on the DSS interface before being sent back to the client.

b. **Response Signing Certificate:** In the case of the Document Confidentiality feature, verification response messages are signed to ensure trust in the ADSS Verification Service's responses. To designate the signing certificate (and private key), select from the options in the drop-down menu labelled Response Signing Certificate.

c. **Hashing Algorithm:** The selected hashing algorithm is used to sign the generated Verification responses. The available options are SHA1, SHA224, SHA256, SHA384, SHA512, SHA3-224, SHA3-256, SHA3-384, SHA3-512, and RipeMD160.

6 Signing Service Gateway

The ADSS Server Signing Service allows client applications to sign data and documents in many formats, such as PDF, Word, ETSI standards (PAdES, CAdES, XAdES), PKCS#1, PKCS#7, CMS, and S/MIME.

In **Gateway mode**, the Signing Service checks that the signing request is correctly structured and includes the necessary details, like the signer's certificate. It also verifies the client's identity through the Client Manager. Valid requests are then forwarded to the back-end Signing Server for processing, while invalid or incomplete requests are rejected

6.1 Working of Signing Service Gateway

Currently, the Signing Profile has the following option to enable remote signing:

6.1.1 Forward signing request to a remote ADSS Signing Server

If this option is selected, the Signing Service functions as a gateway, forwarding the request to a back-end Signing Service to compute the PKCS#1 signature. In this gateway mode, the Signing Service does not have access to the Certification database. Therefore, business applications must include the signer certificate in the request. This setup causes the ADSS Server to act as a proxy server. The proxy ADSS Server will hold the document locally and only send the signature structure to the Signing Server for signing, operating in synchronous mode. Additionally, the signing gateway will verify with the client manager to ensure the requesting client is authorized to use the service.

Follow the instructions below:

1. Launch the ADSS Server Console
2. Navigate to Signing Service → Signing Profiles

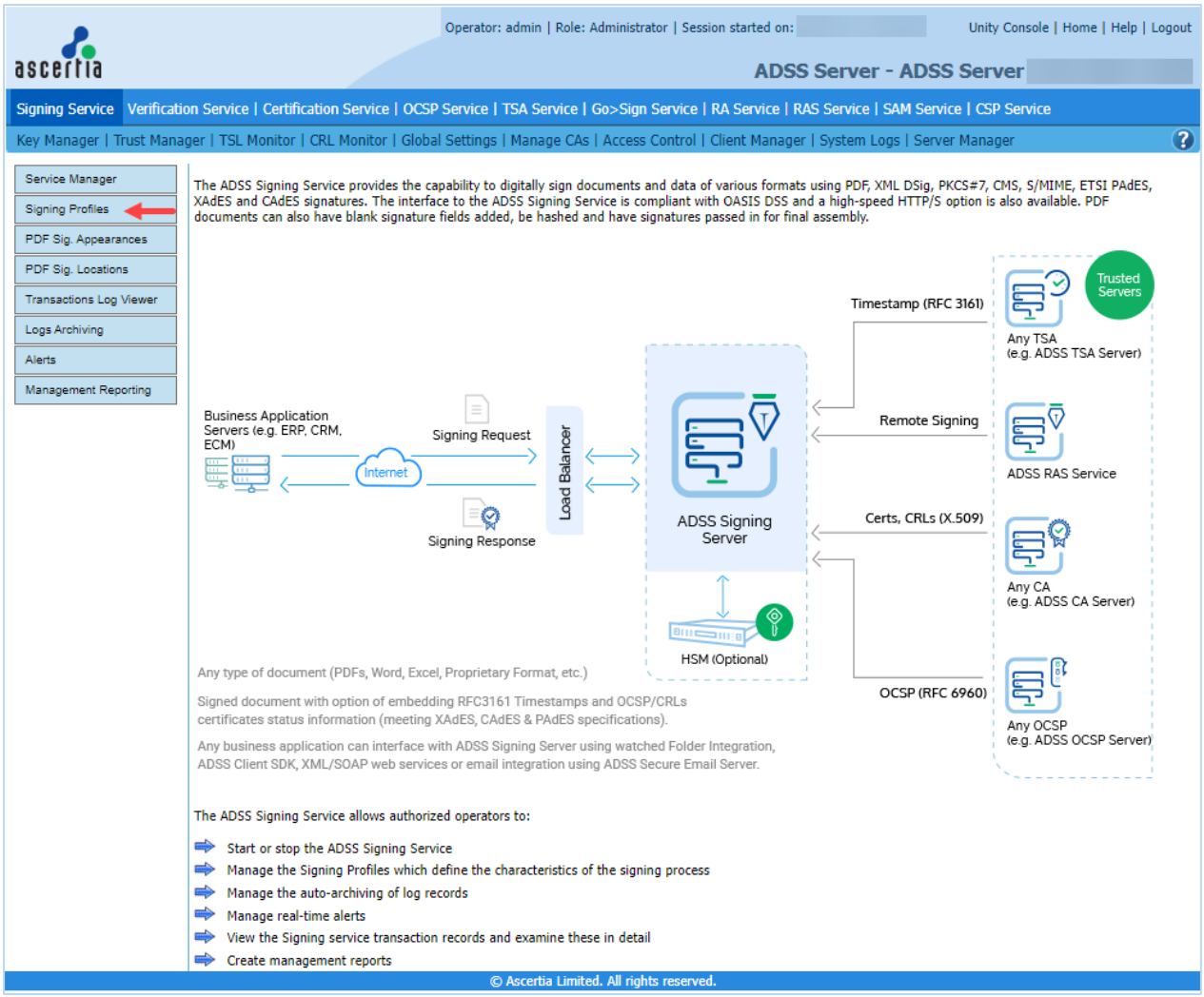

Figure 6 – Signing Service – Home

3. The Signing Profiles page will display, click on the New button as indicated below:

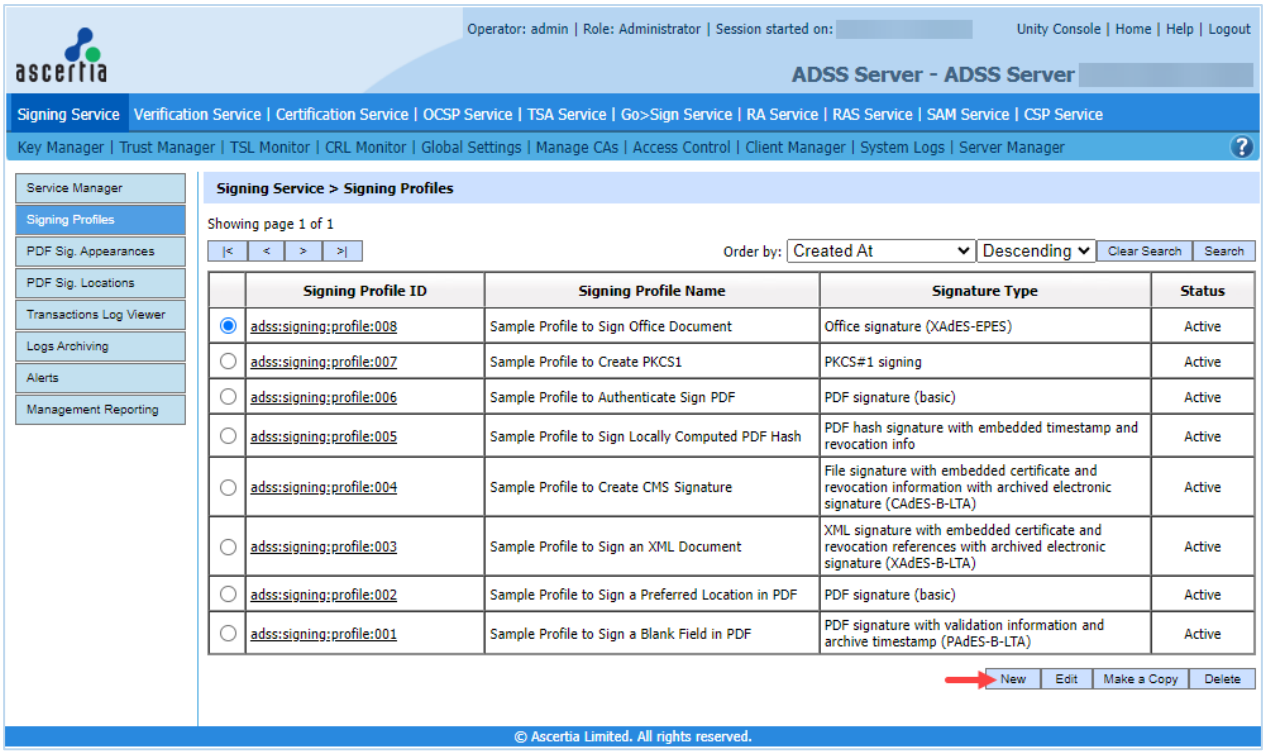

Figure 7 – Signing Service – Signing Profiles

4. Under Signature Types, select 'PKCS#1' as shown in the screen below:

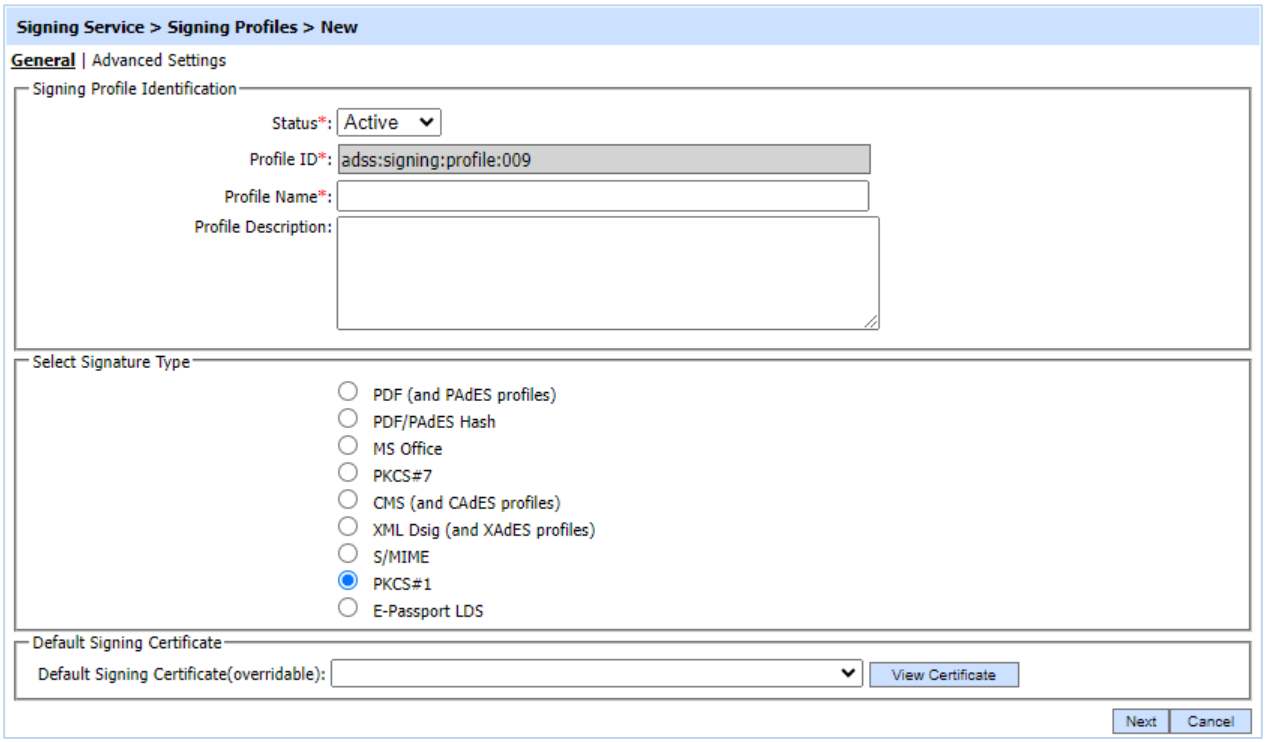

Figure 8 – Signing Service – Signature Type

5. Once the configurations are complete, navigate to the 'Advance Settings' tab.
6. Mark the 'Enable remote signing' checkbox and then enable the 'Forward signing request to a remote ADSS Signing Server' radio button, it will display the following screen:

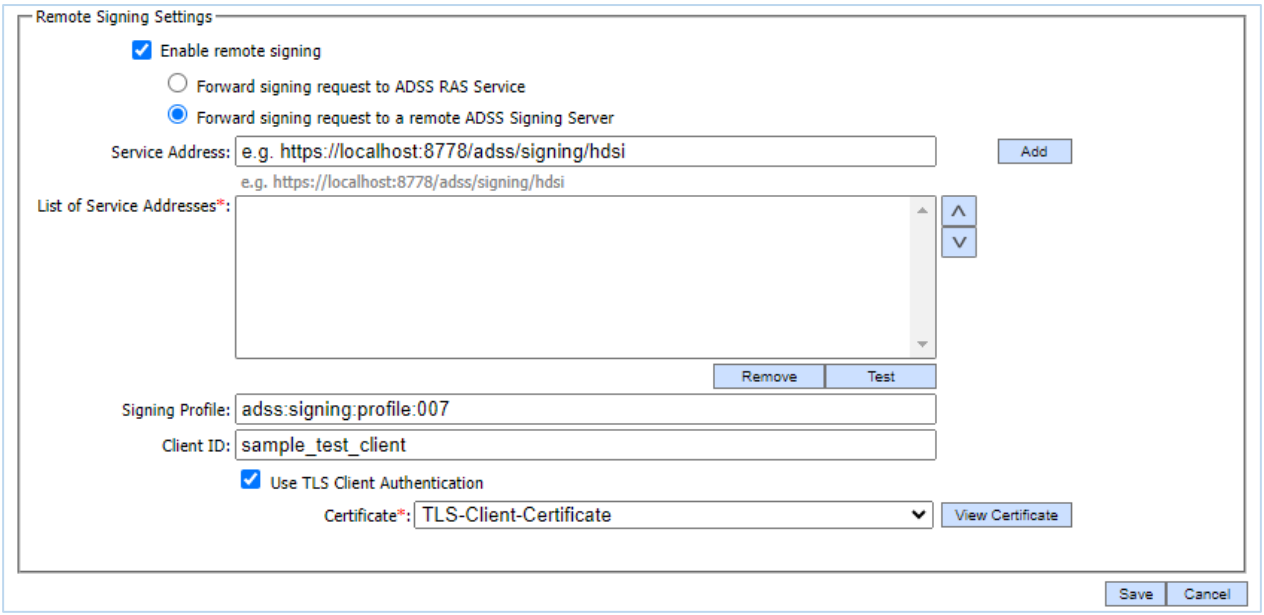

Figure 9 – Signing Service – Enable remote signing

7. Once the radio button is enabled, its relevant fields will start displaying on the screen. The list of fields that becomes available are:

    a. **Service Address:** This field displays the Signing Service Address(es) used to forward requests to the back-end Signing Server. You can add multiple service addresses. The Test button allows you to check if the service is available, and the Remove button lets you delete a configured service address.

    b. **Signing Profile:** Select the signing profile configured with PKCS#1 signature type as mentioned before.

    c. **Client ID:** The gateway functions as a client for the back-end service, requiring prior registration in the Client Manager of the back-end service using a unique Client ID. This same Client ID must be configured on this screen and will be included in every request sent by the gateway to the back-end service.

    d. **Use TLS Client Authentication:** If communication between the gateway and back-end service necessitates TLS Client Authentication, you must select this option. Once selected, a drop-down menu will appear below this checkbox, listing TLS Client Authentication Certificates for you to choose from.

    e. **TLS Client Authentication Certificate:** This TLS Client Authentication Certificate is used by the gateway to authenticate itself with the back-end service over TLS. If the 'Use TLS Client Authentication' checkbox is checked, you must select a certificate from the list provided.

7 RAS Service Gateway

The ADSS Server RAS Gateway acts as the first point of contact for end-user requests, protecting the back-end RAS Service.

In **Gateway mode**, the service checks that each request follows the correct RAS format and includes all required fields. It also verifies the client's credentials with the Client Manager. Once validated, the request is forwarded to the back-end RAS Server. If the request is invalid or unauthorized, it is blocked to keep the back-end safe

7.1 Working of RAS Gateway

The process starts when the end user or business application sends requests to the RAS Gateway. The RAS Gateway independently verifies the client via Client Manger, and checks the necessary request parameters. Once validated, it forwards the request for the backend RAS service, using the client settings configured in its service manager, and forwards it accordingly. Additionally, the Profile ID can be modified in the RAS Gateway service manager; if provided by the client, it takes precedence; otherwise, it uses the setting from the service. Finally, the ADSS RAS Gateway responds to the client based on the received response from the RAS service.

7.2 Implementation Modes of RAS Gateway

The RAS Gateway operates in the ADSS RAS Service by following the below-mentioned two modes:

- **Service**
  In the Service mode, the RAS Service will receive the requests directly from end users or business application, process the requests and return the results.

- **Gateway**
  In the Gateway mode, the requests are received by the RAS Gateway. It verifies the client and checks the necessary request parameters. Once the credentials are validated, it forwards the request to the backend RAS service.

7.3 Configuration of RAS Gateway in ADSS Server

When this radio button is selected, the RAS Service will run in Gateway Mode to communicate with a remote RAS Server.

Follow the instructions below:

1. Launch the ADSS Server Console
2. Navigate to RAS Service → Service Manager

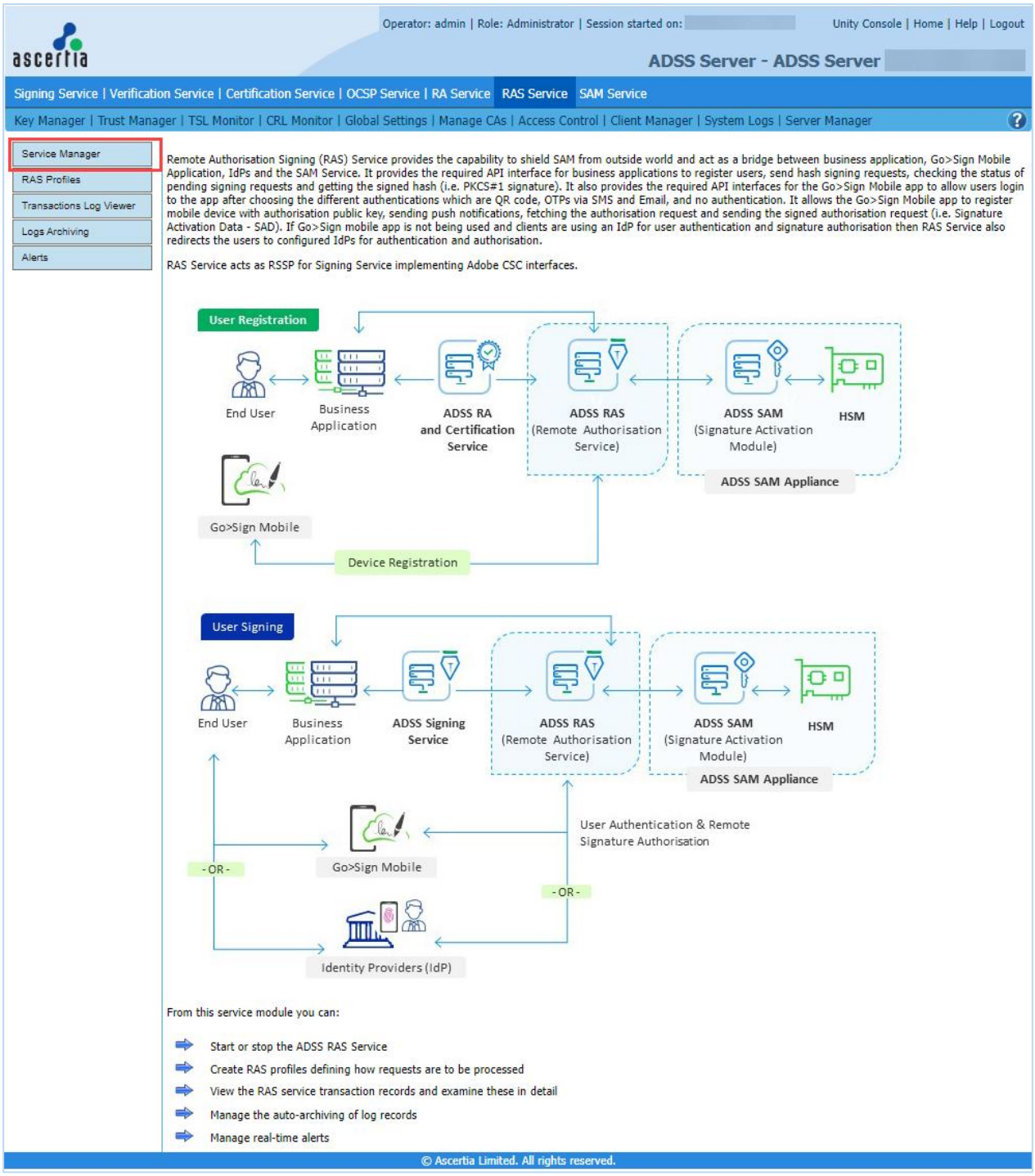

Figure 10 – RAS Service – Home

3. Mark the 'Enable Gateway Mode' radio button , it will display the following screen:

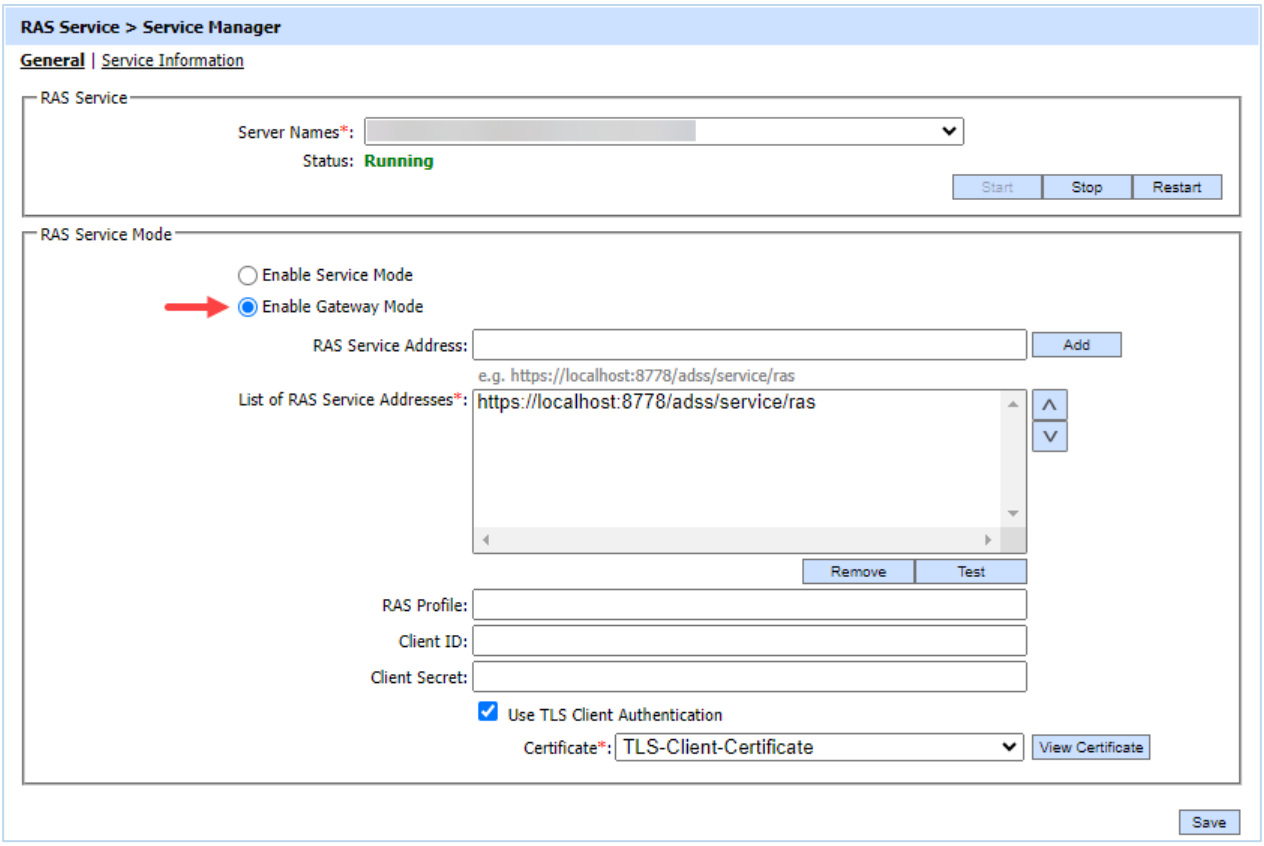

Figure 11 – RAS Service – Service Manger

4. Once the radio button is enabled, its relevant fields will start displaying on the screen. The list of fields that becomes available are:

    a. **RAS Service Address:** The RAS Service Address displays the location of the back-end RAS Service to which all requests will be sent through the gateway. You can input multiple addresses for the RAS service, and arrange them in a preferred order.

    b. **RAS Profile:** This field provides the option to specify the RAS profile for requests sent to the back-end RAS Service. If left unconfigured, requests will be forwarded to the back-end RAS service without a specific RAS profile. In this case, the back-end RAS Server will utilize the default RAS profile set for the Client in the Client Manager.

    c. **Client ID:** The gateway functions as a client for the back-end service, requiring prior registration in the Client Manager of the back-end service using a unique Client ID. This same Client ID must be configured on this screen and will be included in every request sent by the gateway to the back-end service.

    d. **Client Secret:** In this field, the user enters the Client Secret generated during the registration of the configured Client in the back-end RAS Service.

    e. **Use TLS Client Authentication:** If communication between the gateway and back-end service necessitates TLS Client Authentication, you must select this option. Once selected, a drop-down menu will appear below this checkbox, listing TLS Client Authentication Certificates for you to choose from.

    f. **TLS Client Authentication Certificate:** This TLS Client Authentication Certificate is used by the gateway to authenticate itself with the back-end service over TLS. If the 'Use TLS Client Authentication' checkbox is checked, you must select a certificate from the list provided.

8 CSP Service Gateway

The ADSS Server CSP Gateway provides secure access to the Ascertia Virtual Cryptographic Service Provider (VCSP). It acts as the public interface between client applications and the back-end CSP Service, ensuring that all incoming requests are valid and authorized before processing.

The **Gateway** checks that each request follows the correct CSP/VCSP structure, includes all mandatory fields, and complies with any configured CSP profiles (such as allowed algorithms or key usages). It also authenticates the client through the Client Manager and, if enabled, validates TLS client certificates to confirm secure communication. Only after these checks succeed does the Gateway reconstruct and forward the request to the back-end CSP Service. This layered approach not only protects the CSP Service from direct internet exposure but also ensures that only trusted, policy-compliant requests are processed.

8.1 Implementation Modes of CSP Gateway

The CSP Gateway operates in the CSP Service by following the below-mentioned two modes:

- **Service**
  In the Service mode, the CSP Service will receive the requests directly from end users or business application, process the requests and return the results.

- **Gateway**
  When enabled, this CSP Service instance will function as a Gateway for the back-end CSP Server. The CSP gateway validates the request structure and the client. If the validation is successful, it forwards the request to the back-end CSP Server using the configurations specified below. If the validation fails, it returns an error to the calling application, such as Virtual CSP.

8.2 Configuration of CSP Gateway in ADSS Server

When this radio button is selected, the CSP Service will run in Gateway Mode to communicate with a remote CSP Server.

Follow the instructions below:

1. Launch the ADSS Server Console
2. Navigate to CSP Service → Service Manager

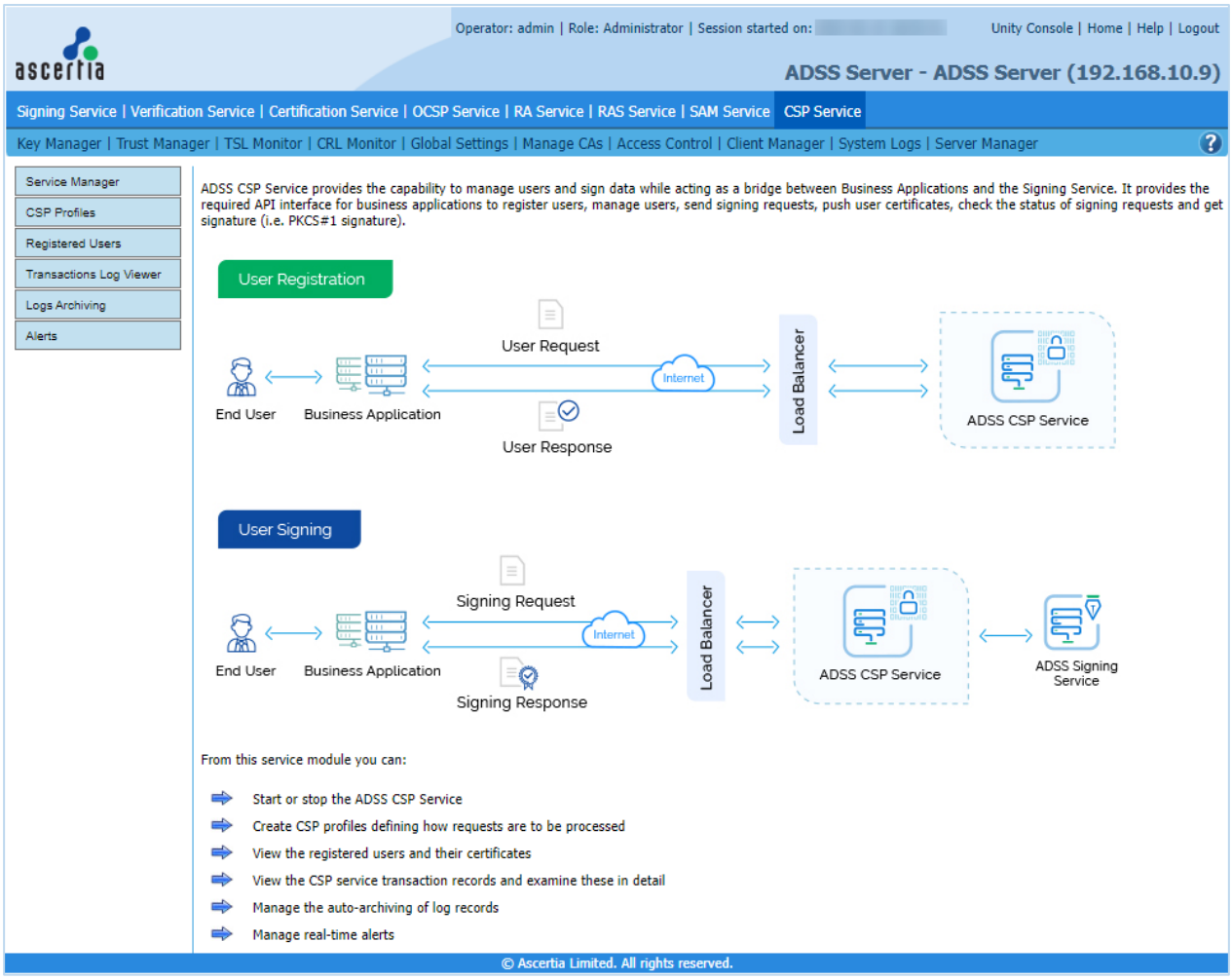

Figure 12 – CSP Service – Home

3. Mark the 'Enable Gateway Mode' radio button , it will display the following screen:

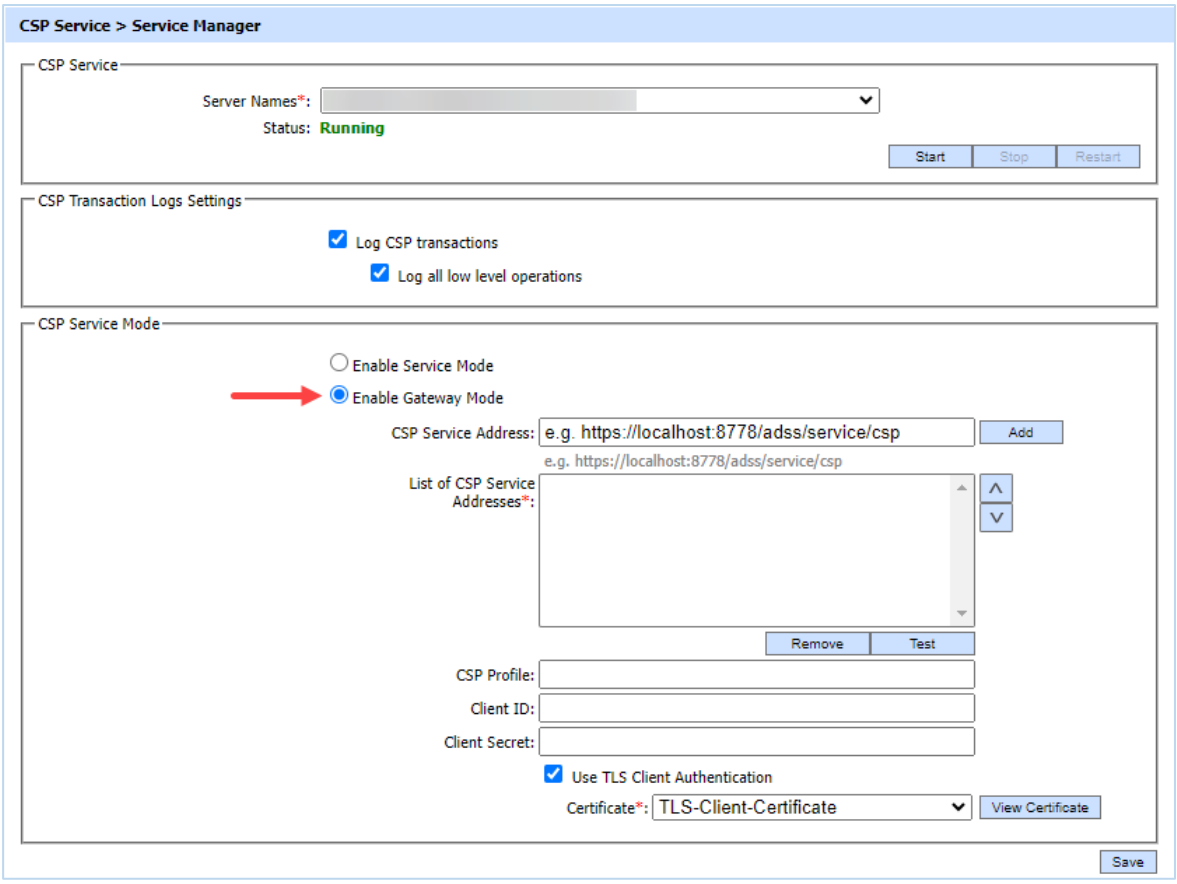

Figure 13 – CSP Service – Service Manager

4. Once the radio button is enabled, its relevant fields will start displaying on the screen. The list of fields that becomes available are:

    a. **CSP Service Address:** The CSP Service Address displays the location of the back-end CSP Service to which all requests will be sent through the gateway. You can input multiple addresses for the CSP service, and arrange them in a preferred order.

    b. **CSP Profile:** This field provides the option to specify the CSP profile for requests sent to the back-end CSP Service.

    c. **Client ID:** The gateway functions as a client for the back-end service, requiring prior registration in the Client Manager of the back-end service using a unique Client ID. This same Client ID must be configured on this screen and will be included in every request sent by the gateway to the back-end service.

    d. **Client Secret:** In this field, the user enters the Client Secret generated during the registration of the configured Client in the back-end CSP Service.

    e. **Use TLS Client Authentication:** If communication between the gateway and back-end service necessitates TLS Client Authentication, you must select this option. Once selected, a drop-down menu will appear below this checkbox, listing TLS Client Authentication Certificates for you to choose from.

    f. **TLS Client Authentication Certificate:** This TLS Client Authentication Certificate is used by the gateway to authenticate itself with the back-end service over TLS. If the 'Use TLS Client Authentication' checkbox is checked, you must select a certificate from the list provided.

******* End of Document *******