

Secure Email Server™

- A complete server-based drop-in solution
- Works with existing email infrastructures
- Signs / verifies email attachments
- Signs / verifies the email body
- Uses filters to select the emails to act upon



Email is used extensively within every organisation as a vital communication tool. There is an increasing threat from people falsely trusting emails simply because they see a friendly “from:” email address. Email body text can be changed with ease and attachments can be amended.

Ascertia’s Secure Email Server (SES) overcomes these threats by applying digital signatures to emails and their attachments. When such an email is received the same server process can verify the email and its attachments and confirm the identity of its authors, reviewers and/or approvers and allow the email to pass; or route it for audit or security review.

Secure Email Server Architecture

The Ascertia Secure Email Server is a full MTA email server that supports both SMTP and POP3 protocols. It is built using the open source Apache James, a well-regarded platform-independent Java mail server. Apache James provides a mail application platform with two standard extension mechanisms called Matchers and Maillets.

Matchers: These provide message selection services and are written specifically to filter and identify those emails that need processing by passing them to the Maillet.

Maillets: These provide message processing services and are written specifically to process the filtered email. Within Secure Email Server the Maillet calls ADSS Server to digitally sign or verify the email or its attachment.

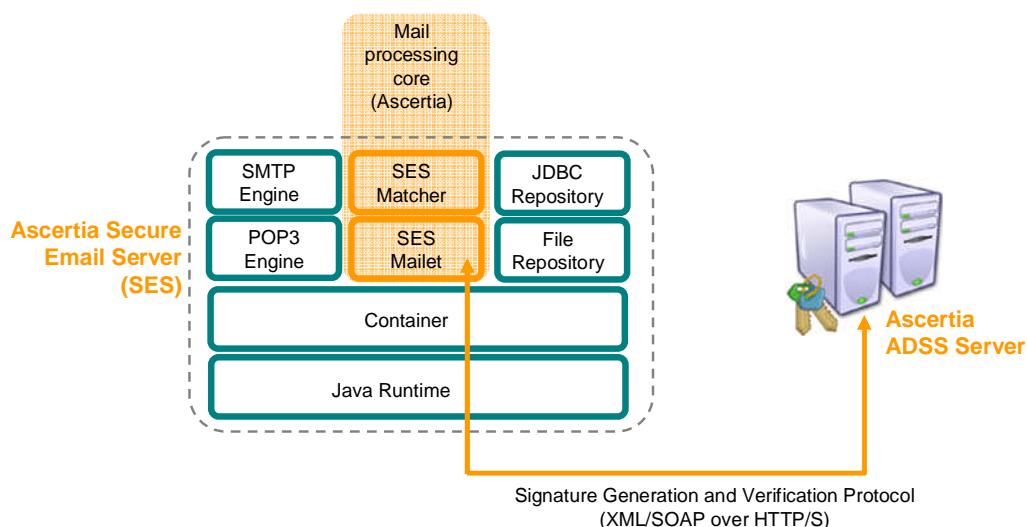
The high-level architecture of Secure Email Server is shown below. The green boxes show the standard Apache James modules including the SMTP and POP3 engines that handle inbound and outbound email messages.

The Ascertia core mail processing engine is shown by the orange boxes representing a specific Matcher and Maillet for handling digital signature creation and verification functionality.

For outgoing mails, if the Matcher rules determine that the email requires signing, the Maillet sends a signing request message to the safely located ADSS Server.

For incoming emails, the Secure Email Server Matcher filters those emails and attachments that are signed and then the Maillet makes a request to the ADSS Server to verify these signatures. The original email and the verification results are then passed to the internal email server for later delivery to the internal mail recipient(s). It is recommended that they are delivered to security administrators if the signatures fail to verify.

The Matcher can be configured to meet organisational needs. Mails can be filtered based on text matches within these fields: FROM, TO, CC, BCC, Subject, the email Body, any attachments that are present and their properties, and whether the email is already signed.

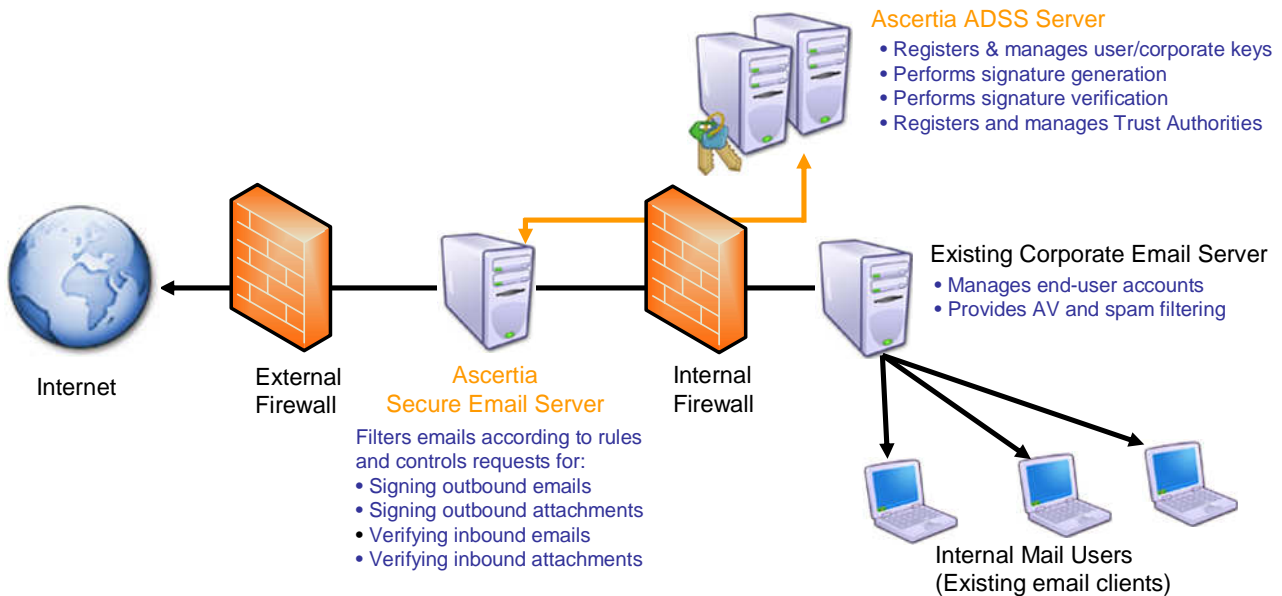


The Secure Email Server can also be used to sign and archive received emails and attachments to provide evidence of what has been received and when it was received from external parties. A future release will also be able to encrypt and decrypt emails if required.

Delivering Trust for Business Documents sent by Email

A Typical Deployment

A typical deployment of Secure Email Server is shown below, with an existing email server handling emails and attachments as normal and then routing outgoing mails to the Secure Email Server for signing if applicable. For incoming signed mails or attachments, these are passed to ADSS Server for verification before being forwarded to the existing mail server.



With so many options Ascertia and its delivery partners can help you to define the best way to meet the various business, legislative and regulatory needs and reduce the risks and costs involved in creating, sending, receiving and storing unprotected business documents. The multiple capabilities of ADSS Server can be used to solve today's needs and also offer tremendous investment protection to meet the changing needs of tomorrow.

ADSS Enterprise Server has been designed to meet the digital signature and verification needs of SMEs as well as large national and multi-national organisations. It does this by providing flexibility, resilience and scalability, combined with well designed internal security, management, audit logging and reporting.

ADSS Infrastructure Server offers similar capabilities to managed service providers and regional trust schemes.

Secure Email Server Features:

Signing Outgoing Mails:	Using standard S/MIME digital signatures that are verifiable by most email clients e.g. Microsoft Outlook, Lotus Notes & Thunderbird.
Signing Mail Attachments:	Using PDF, XML or PKCS#7/CMS digital signatures. Options exist to support advanced long-term signature profiles using CAeS and XAdES and the PDF equivalent.
Verifying Signed Emails:	Including identity checking the sender's certificate using real-time OCSP or CRL, plus optional signer's certificate quality checking.
Verifying signed attachments:	Including checking the document author's signing certificate using OCSP or CRL, plus optional certificate quality checking.
Archiving emails:	So that operators can recover, review and resend previously processed emails.
Encrypting/Decrypting emails:	(to be provided in a future version)

Secure Email Server Standards Compliance:

Signature generation:	Any ADSS Server supported type
Signature verification:	Any ADSS Server supported type
Operating Systems:	Windows 2003 Server, others on request
Interfaces:	SMTP and POP3

Ascertia Limited
Web: www.ascertia.com
Email: info@ascertia.com
Tel: +44 1256 895416 US: +1 508 283 1890
40 Occam Road, Guildford, Surrey, GU2 7YG, UK
© Copyright Ascertia Limited 2009. All Rights Reserved, E&OE