MOBILE-ID
Anytime, Anywhere

TRUSTED HUB

Secure Email Appliance™

- An appliance-based drop-in solution
- Works with existing email infrastructures
- Signs/verifies emails or attachments
- Uses filters to select the emails to act upon

Email is used extensively within every organization 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.

Trusted Hub Secure Email Appliance overcomes these threats by applying digital signatures to emails and their attachments. When such an email is received the same appliance 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 Appliance Architecture

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

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

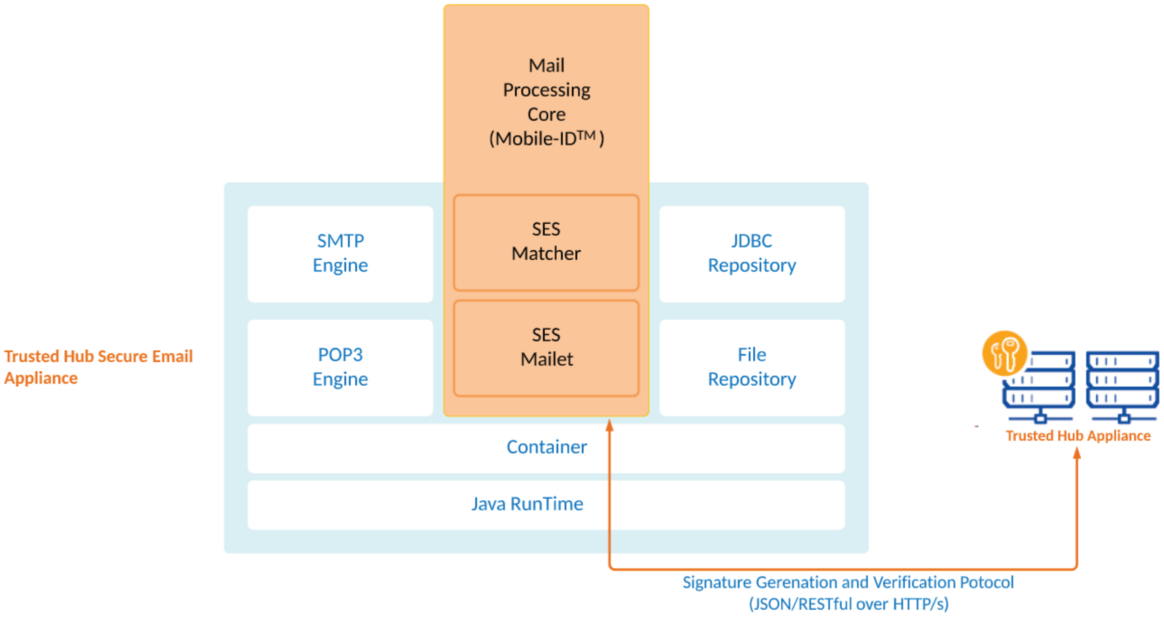
Mailets: These provide message processing services and are written specifically to process the filtered email. Within Secure Email Appliance the Mailet calls Trusted Hub Appliance to digitally sign or verify the email or its attachment.

The high-level architecture of Secure Email Appliance 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 Mobile-ID™ core mail processing engine is shown by the orange boxes representing a specific Matcher and Mailet for handling digital signature creation and verification functionality. For outgoing mails, if the Matcher rules determine that the email requires signing, the Mailet sends a signing request message to the safely located Trusted Hub Appliance.

For incoming emails, the Secure Email Appliance Matcher filters those emails and attachments that are signed and then the Mailet makes a request to the Trusted Hub Appliance to verify these signatures. The original email and the verification results are then passed to the internal email appliance 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.

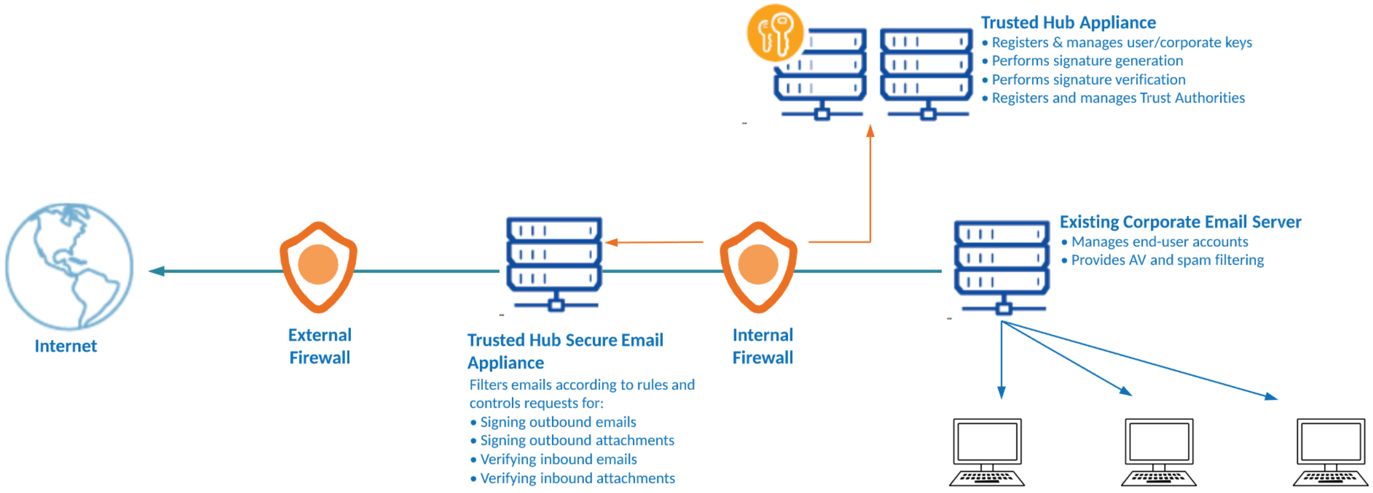
The Matcher can be configured to meet organizational needs. Mails can be filtered based on text matches within these fields: From, To, Cc, Bcc, Subject, the email Body, any attachments that are present and their properties, and whether the email is already signed.



The Secure Email Appliance 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.

A Typical Deployment

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


Trusted Hub Appliance
• Registers & manages user/corporate keys
• Performs signature generation
• Performs signature verification
• Registers and manages Trust Authorities
Existing Corporate Email Server
• Manages end-user accounts
• Provides AV and spam filtering
Internet
External Firewall
Trusted Hub Secure Email Appliance
Filters emails according to rules and controls requests for:
• Signing outbound emails
• Signing outbound attachments
• Verifying inbound emails
• Verifying inbound attachments
Internal Firewall

With so many options Mobile-ID™ 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 Trusted Hub Appliance can be used to solve today's needs and also offer tremendous investment protection to meet the changing needs of tomorrow.

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

Trusted Hub Infrastructure Appliance offers similar capabilities to managed service providers and regional trust schemes.

Trusted Hub Secure Email Appliance 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 CAdES 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.

Trusted Hub Secure Email Appliance Standards Compliance:

Signature generation:	Any Trusted Hub Appliance supported type
Signature verification:	Any Trusted Hub Appliance supported type
Operating Systems:	Windows Server 2016/2012 R2/2012/2008 R2
Interfaces:	SMTP and POP3