Boldon James
A QINETIQ company

SAFEmail® Client And Server

A secure messaging solution for defence and intelligence environments using Microsoft Outlook & Exchange

At A Glance

SAFEmail® Client and Server extends COTS Microsoft Outlook and Exchange message functionality to enhance the systems to support Medium and High Grade messaging capabilities. The modular architecture of SAFEmail® provides the flexibility required for defence and intelligence messaging, allowing the handling and control of a wide range of data from sensitive but unclassified data, through to the high levels of restricted Government Classifications, at SECRET and above, across a variety of messaging environments. These capabilities allow organisations to protectively-mark emails and enforce security policies together with support for NATO compliant messaging standards such as STANAG 4406 and 4774/8 to ensure interoperability across nations.

SAFEmail® Client Features

Labeller

SAFEmail® Labeller provides a Security Label user interface applicable to all levels of system sensitivity. The Labeller supports security policies containing any number of label elements, from a basic user interface for policies with less than three label elements (such as OFFICIAL) to an extended user interface for those policies with complex labels and caveats (such as at SECRET and above). A coloured banner is used to provide the user with a visual indication of the message sensitivity. The sensitivity of the system dictates where the Security Label is stored in the message;

Key Benefits

- Get the system you need with ultra-flexible module selection and build
- Makes conforming to high grade military messaging standards easier
- Easy to use and consistent for maximum operational flexibility
- Enhanced security with controlled document access
- Reduces compliance costs
- Seamless integration with Microsoft Office & Exchange
- A familiar interface for user training and transition

printable text versions of the Security Label can be stored in Subject, First-Line-Of-Text (FLOT) and/or X-Header. The ESS Security label provides a 'standards' defined method of cryptographically binding the Security Label with the Message Content through the use of an S/MIME digital signature. Some systems may mandate a message must include additional security (digital signature and/or message encryption) when a particular security label element is chosen, the Labeller can therefore drive SAFEmail® Security or Windows Rights Management.

Capability Checker

Capability Checker examines the contents of a message to ensure it has been appropriately composed and that its recipients have security clearance to receive it. Along with the message size and message type, other attributes (attachments, SIC (Subject Indicator Code), ACP127 body format & security group membership) may also be examined by the Capability Checker. Sensitive environments may dictate received messages are examined by the capability checker, this follows good security in depth principals where 'bad' messages should be captured by a border device. Black and White lists of email addresses and email domains may be defined to restrict who the user can / cannot send messages to. This is further enhanced with address compatibility rules, which describe email addresses and email domains that are incompatible when used on the same message, but have earlier passed the Black and White list checks.

Security

The SAFEmail® Security component provides security management through S/MIME, a security standard published by the IETF and used to provide digital signatures (for non-repudiation) and encryption (for confidentiality). The SAFEmail® Security component interfaces with Microsoft CAPI to implement cryptography algorithms or alternatively provides its own algorithms when used with PKCS12 private key file. Verification of the digital signature uses CRL or OCSP standards for certificate revocation checks. This component also has the ability to define which signing key is used in role-based environments (using multiple mailboxes), automatic inclusion of gateway certificates for encrypted messages and certificate binding checks to ensure originator email address matches the email address used to create the digital signature.

Military Forms

SAFEmail® Forms provides support for an RFC6477 (and STANAG 4406, 4774/8) compliant message used with formal messaging systems. The Administrator can customise the descriptive text presented on the Form, together with definition of those message attributes which are optional, mandatory or unused. A built-in SIC (Subject Indicator Code) browser allows users to browse an LDAP Directory for the definition and selection of a SIC. Populating the 'From' field on the Form presents only those roles applicable to the user and not the entire Address Book.

Custom Fields

As an alternative to the SAFEmail® Forms component, the Administrator can use Custom Fields to define additional message attributes (in addition to the standard attributes provided by Microsoft Outlook e.g. From, To and Subject) which are presented on the Outlook ribbon bar and transmitted using an Internet Message X-Header attribute. Custom Fields have been used to transmit standard military attributes e.g. 'Precedence' and also non-standard system proprietary attributes.

Draft And Release

Organisational messaging is commonly used in High Grade Military environments, where 'roles' compose messages on behalf of the 'organisation'. These messages must then be approved before they are submitted from the 'organisation'. Draft and Release allows the Drafter of the message to pass the message for review by a pre-defined list of reviewers (or a dynamic list of reviewers). Reviewers may alter the message, append comments before finally the Releaser allows the message to be submitted. In conjunction with E-Tracker, the original Drafter can keep track of where in the review process the message currently resides.

Document Management

Sensitive documents are increasingly being stored in electronic document & records management systems (EDRMS) to manage the document life-cycle, from creation to destruction. The Content Management Interoperability Standard (CMIS) is the ratified OASIS standard used for client access to an

EDRMS. The SAFEmail® Document Management component is used to interface with any CMIS-compliant EDRMS (e.g. SharePoint 2010) and allows any document to be attached as a link to the document stored in the EDRMS. Metadata holding the Security Label is retrieved by SAFEmail® and used as a template for the message Security Label. Documents in received messages may also be uploaded into the EDRMS.

E-Tracker

Environments exist where the monitoring of delivery reports and read receipts is required to ensure sensitive messages are delivered and read in a timely manner. E-tracker correlates received reports and receipts with the originally submitted message, and provides a summary report to the user on the exact status of the message. E-Tracker supports both SMTP (DSN and MDN messages) and X.400 (DR and RN messages) network environments (including ESS Signed Receipts). In addition, E-tracker can optionally delete any correlated reports and receipts from the Inbox folder to ensure this folder remains clear for receiving messages.

P7 Transport

The P7 Transport extends the range of messaging solutions supported by SAFEmail® to include the X.400 Message Store. It can also be used in conjunction with other messaging solutions (e.g. Microsoft Exchange) to provide message grade separation (e.g. High Grade over X.400 and medium Grade over SMTP).

SAFEmail® Server Features

SAFEmail® Exchage Capability Checker

Running as a Transport Agent on the Microsoft Exchange Server (Hub or Edge) the Capability Checker monitors email messages in transmission, inspecting them to validate they conform to local policy. Inspection can include:

- Determine whether the intended recipients have sufficient security clearance to receive the message.
- Validate the Message Security Label, Attachment Types and Message size.
- Validate the Message Signature (S/MIME) and optionally downgrade to a plain message for those recipients unable to support S/MIME.
- Address Compatibility. Ensuring the recipients on an email are compatible with each other, forking the email if they are not.
- Integration with Electronic Document and Records Management Systems (EDRMS) to file attachments found on received messages into the EDRMS, replacing the attachment on the message with a short-cut.

For those messages that fail the inspection policy a number of actions can be performed including removing recipients from the message, returning a non-delivery report or quarantining the entire message for further examination by a security officer.

SAFEmail® Fire And Forget

In defence environments, it's common to find email systems where it is mission critical that high precedence messages (e.g. Flash) are delivered and processed in a timely manner. Fire and Forget monitors a message from the moment the originator hits send to manage it throughout its journey, so that once sent, it is guaranteed to be delivered and processed by a recipient within the timescales defined by their local security policy. SAFEmail® Fire and Forget is located on the Microsoft Exchange Server and monitors all email transmission, looking for email of a particular type and precedence (priority may also be examined). For each monitored email the Fire and Forget system looks for corresponding delivery reports (indicating the message has been delivered to the destination mailbox) and read

notifications (indicating the message has been read by the recipient). If a delivery report or read notification isn't received within the pre-defined time period, the message is forwarded onto a guaranteed action point - a mailbox whose contents are monitored 24 hours a day. Fire and Forget can send courtesy messages to the intended recipients, and message originator when a message is forwarded onto a guaranteed action point, explaining what has happened to the message.

SAFEmail® Exchage Capability Checker

In security sensitive environments, users can have multiple mailboxes to monitor, possibly in different physical locations or security domains to their primary mailbox. SAFEmail® Notifier is installed on a Microsoft Exchange Server and informs users when they have messages in other mailboxes, by sending a notification email to their primary inbox, allowing them to remotely monitor their additional mailboxes and only access them when new mail is waiting to be read.

SAFEmail® X.400 Bridgehead

Microsoft Exchange Server is arguably one of the most commonly used email systems around the world. However, Microsoft Exchange Server 2003 was the last version to fully support an X.400 MTA, including support for the ACP120, ACP123 and STANAG 4406 and 4774/8 military standards. The SAFEmail® Bridgehead was introduced with Microsoft Exchange Server 2007 and continues the X.400 support in Microsoft Exchange. The SAFEmail® Bridgehead supports the commercial P2/P22 message content, and in conjunction with the SAFEmail® Client, STANAG 4406 compliant messages continue to be supported in the Microsoft Exchange environment.

System Requirements
Software

- Windows 7, Windows 8 and Windows 10
- Microsoft Office 2010, 2013 and 2016
- Microsoft Exchange Server 2010, 2013 and 2016

Try Before You Buy

Contact your Boldon James representative or visit: **boldonjames.com/on-demand-demo**