

TECHNICAL NOTE

Architecture for ACSI33 email security requirements

Implementation using janusSEAL and Clearswift MIMESweeper

Greg Colla

July 2005

This paper outlines the changes in the security policy for email within Australian Government agencies, specifically the email protective marking policy defined in the March 2005 edition of ACSI33.

Furthermore, it proposes a general email system architecture to fulfil these requirements.

Finally it shows how janusNET's janusSEAL and Clearswift's MIMESweeper are used together to implement this architecture.

This paper is intended for ICT security professionals working in Australian Government agencies.

This paper does not describe email security policies from previous editions of ACSI33, nor does it describe any changes to the cryptography security policy in ACSI33. These and other factors must be taken into account to develop a compliant email system.

1. ACSI33 email security requirements

A very brief introduction to ACSI33

ACSI33 is the Australian Government Information and Communications Technology Security Manual. It provides policies and guidance to Australian Government agencies on how to protect their ICT systems.

ACSI33 is authored and published by DSD, and is available from <http://www.dsd.gov.au/library/infosec/acsi33.html>.

The following section summarises those parts of ACSI33 that specifically pertain to email security policy.

ACSI33 Part 3 CHAPTER 5 – ICT Software Security

This section deals with topics such as malicious code and antivirus software, database security, web application security, email security, email protective marking policy and software development.

Electronic Mail Security

The electronic mail security section describes the following topics:

- ◆ Email Usage Policy
- ◆ Server auditing
- ◆ Access to web based email
- ◆ Automatic forwarding
- ◆ Centralised email gateway
- ◆ Email policies, plans and procedures

Electronic Mail – Protective Marking Policy

The email protective marking policy specifies the behaviour of the email system, specifically with regards to protective markings. It defines and discusses the following:

- ◆ Marking classified emails
- ◆ Marking unclassified emails
- ◆ Personal emails
- ◆ Protective marking standard
- ◆ Dealing with email originating outside Australian Government
- ◆ Marking emails from outside of the Australian Government
- ◆ Checking emails for a protective marking
- ◆ Blocking of unmarked emails
- ◆ Blocking of outbound emails
- ◆ Blocking of inbound emails
- ◆ Printing

The intent of the protective marking policy is to provide a means to manage and control the flow of sensitive information transported via email. This helps minimise the risk of information leakage via channels that do not provide adequate protection.

2. An architecture for email security

The solution consists of two components, being:

1. A change to the organisation's email clients to enforce user classification of email;
2. Modification of the organisation's email gateway to manage the delivery and audit of official information. This may include the addition of further perimeter filtering services where emails are relayed outside the immediate network.

A description of each of these components follows, along with a scenario that describes how they interact.

Classify your email, let the email system manage the protection

The solution requires a mechanism for users to classify their messages prior to transmission. Such a mechanism prompts the sender to classify the message before it is sent, and adds a protective marking to the message.

An email with a protective marking provides the email system with an indicator of which security procedures to follow for that message.

Configure the email gateway with capability to control the delivery of classified email

The solution requires the email gateway and any other perimeter filtering service be configured to implement the delivery rules shown in Table 1.

These rules provide filtering capabilities, additional to content based rules, based on the message's security classification, and the security classification of the route to the destination.

Message Classification	Route/Gateway/Network security rating			
	UNCLASSIFIED	IN-CONFIDENCE	PROTECTED	HIGHLY-PROTECTED
UNCLASSIFIED	forward	forward	forward	forward
IN-CONFIDENCE	reject	forward	forward	forward
PROTECTED	reject	reject	forward	forward
HIGHLY-PROTECTED	reject	reject	reject	forward

Table 1. Gateway delivery rules for classified messages

The upgraded email gateway has the following features:

- ◆ It provides a mechanism to enforce the organisation's email policy on the transmission of classified (official) information
- ◆ It removes the need for users to know whether a message is routed via secure or insecure interconnecting networks
- ◆ It minimises data leakage via email, and provides evidence when policy is abused

Description of Operation

The system deployment is shown in Figure 1. At a macro level, the system consists of two organisational networks, connected to each other via an interconnecting network. Within each organisation's network are a number of email clients and email servers. Each organisation's email network is connected to the interconnecting network with an email gateway.

In this scenario, a user in Organisation A wishes to transmit some sensitive information to a user in Organisation B, and the interconnecting network provides adequate protection for the message.

The steps to complete this scenario are as follows:

1. The originator generates the message and enters the recipient's email address using the standard email client. The sender activates the "send" function. The email client plug-in activates and prompts the user to classify the contents of the message. For this example, the user classifies the message as IN-CONFIDENCE. The email client plug-in marks the message with the security classification and forwards the message to the Organisation A's local mail server (2).
2. The local mail server inspects the recipient address of the message. The recipient is outside the local network, so it forwards the message to Organisation A's email gateway (3).
3. Organisation A's email gateway interrogates the message's security classification, and the recipient's domain. It is preconfigured with the security rating of the route to Organisation B and can calculate that the interconnecting network has adequate security for the message security classification. It then forwards the message to Organisation B's email gateway (4).
4. Organisation B's email gateway detects that the message is classified as IN-CONFIDENCE, and that the recipient's email inbox is within its own network. It also calculates that the message has adequate security on Organisation B's mail system. It forwards the message to Organisation B's Email Server (5).

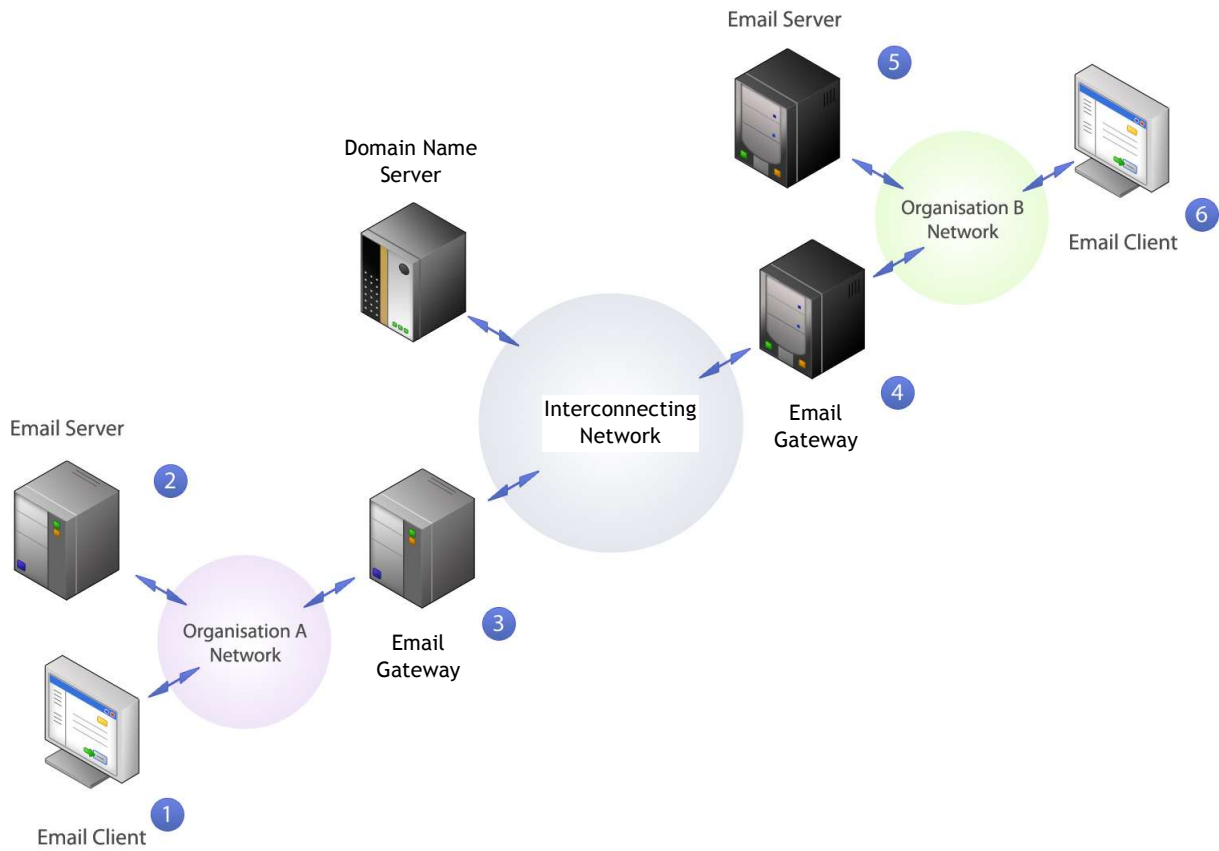


Figure 1. Transmission of classified email between users in two organisations

5. Organisation B's Email Server stores the message in the recipient's inbox.
6. The recipient retrieves the email message from Organisation B's Email Server and displays the message.

3. Implementation using janusSEAL and MIMESweeper

janusSEAL is the face of an organisation's email usage policy

janusSEAL is the email plug-in at the end-user desktop. It:

- ◆ forces the user to classify each message prior to its transmission
- ◆ applies the relevant protective marking to each messages
- ◆ controls the behaviour of the email client on a per classification basis, as defined in your policy
- ◆ quickly provides information about your email usage policy and security classification system to your users

System administrators configure janusSEAL with the organisation's email policy using Microsoft Group Policy. Policy settings can therefore be specified on a group basis, where groups can be sets of machines or users.

With the addition of janusSEAL Census, a reporting service, organisations can audit the flow of sensitive information throughout an organisation, and begin measuring the amount of sensitive information contained in the organisation's email system.

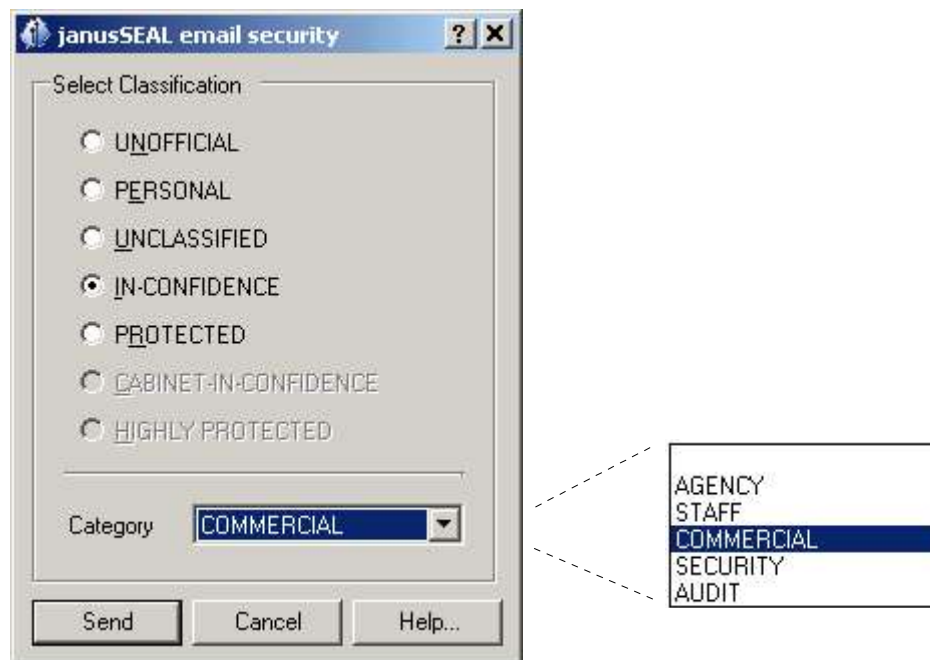


Figure 2. janusSEAL classification dialogue showing configured classifications and categories

MIMESweeper configuration

As the perimeter device between the organisation's network and external networks, MIMESweeper for SMTP can be used to act as an enforcement mechanism for the organisation's email protective marking policy.

Various components of MIMESweeper must be configured to implement the policy:

- ◆ Use MIMESweeper *Address Lists* to define the destination and delivery route security rating. Group these by security rating.
- ◆ Use MIMESweeper *References* to define the protective marking terms, as defined in "Protective Markings for Email Messages"
- ◆ Use MIMESweeper *Text Analysis Scenarios* to detect whether a message has a protective marking, and if so, the security classification of the message.
- ◆ Use MIMESweeper *Classifications* to apply the delivery rules defined by the organisation (the organisation's version of Table 1).

MAILsweeper can also be used within an organisation's email system to restrict the delivery of email to recipients' mailboxes.

About janusNET

janusNET is an Australian company which provides innovative security solutions for Australian Government agencies and commercial organisations.

janusNET builds tools that help these organisations manage the transmission and storage of sensitive information.

janusNET solutions start from well-known, standard security technologies before being uniquely refashioned into user-friendly and practical applications.

Recently, the directors of janusNET have been providing email security services to one of the Australian Government's largest agencies. They authored an open standard that specifies the format of protective markings in email messages for Australian Government agency usage. This standard is in draft status and is under review by other government agencies.

Contact details

Email: info@janus.net.au

Call the author on +61 (0)407 294 402

<http://www.janus.net.au>