



# The Message

Volume 4, Issue 1

January 2006



S/MIME Secure  
Messaging

## S/MIME Secure Messaging Certification – Addressing the Skills Gap

The market demand for e-mail encryption is growing explosively, due a combination of legislation and a growing awareness of the value of the information that is being carries by e-mail. However, the number of companies who have the skills needed to deploy secure messaging systems is still relatively small. Those companies who identify a business need to deploy this capability are reporting difficulties finding skilled resources to help them.

The [S/MIME Secure Messaging \(SSM\) Certification](#) program, to be introduced by The Open Group Messaging Forum later this month is designed to address this barrier to the adoption of secure e-mail.

The foundation of the program is the [S/MIME Secure Messaging Architecture](#), which defines a standards based approach secure e-mail and the [S/MIME Secure Messaging Core Syllabus](#) which defines a core body of knowledge needed to deploy such a system.

The [S/MIME Secure Messaging Certification](#) program will identify

- ✚ Professional services offered in support of deployment of the SSM Architecture
- ✚ Training courses that enable secure messaging professionals to acquire the necessary knowledge and awareness of the SSM Architecture to able to install and configure secure e-mail systems
- ✚ Messaging professionals with the necessary knowledge, understanding and awareness of the SSM Architecture to be able to design, deploy and configure secure e-mail systems

The program is backed by The Open Group certification processes that ensure that certified services and individuals do indeed meet the appropriate criteria. A public register of certified services and individuals is maintained by The Open Group.

This provides a valuable starting point for organizations looking for skilled assistance in planning and/or deploying a secure messaging system and a valuable method of promotion for service companies with the necessary skills.

### S/MIME Secure Messaging Architecture

Members of the Messaging Forum will present a half day tutorial on the S/MIME Secure Messaging Architecture as part of The Open Group Architecture Practitioners' Conference in Barcelona, Spain on Tuesday January 24, 2006

### The Message

The Message is the magazine of The Open Group Messaging Forum.

Published around 6 times per year and available free of charge to subscribers, The Message brings up to date information about the world of electronic messaging and the activities of The Open Group Messaging Forum.

### The Messaging Forum

The Open Group Messaging Forum is a membership based consortium of messaging professionals. Its mission is to maintain and enhance the effectiveness of electronic messaging for inter-personal communication and as a backbone for e-business.

#### Co-Chairs:

Russ Chung, Russ Chung Consulting  
Wen Fang, The Boeing Company

#### Director:

Mike Lambert, The Open Group

#### Web site:

[www.opengroup.org/messaging](http://www.opengroup.org/messaging)

### In This Issue

|                                       |   |
|---------------------------------------|---|
| S/MIME Secure Messaging Certification | 1 |
| S/MIME Secure Messaging Architecture  | 2 |
| Letter from the Chairs                | 4 |
| Messaging Forum active projects       | 4 |
| Upcoming events                       | 4 |

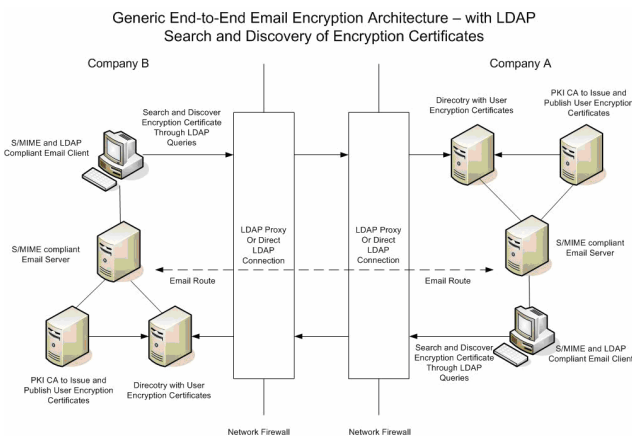
## S/MIME Secure Messaging Architecture

The S/MIME Secure Messaging Architecture defines the components of a secure messaging system based on the S/MIME set of standards, their relationships to each other and to the environment in which they operate.

There are currently several different approaches to e-mail encryption. To ensure interoperability, the architecture is restricted to secure e-mail systems that use cryptographic approaches based on the IETF S/MIME and related standards.

The architecture includes two modes of operation:

- ✚ Desktop-to-desktop (illustrated below). This provides the most secure system, since the message is encrypted from desktop-to-desktop and does not appear "in the clear" at any point in the transmission.
- ✚ Gateway-to-gateway. Messages are encrypted at the e-mail gateway for transmission across public networks and decrypted at the receiving gateway. This simpler to manage mode meets the needs of many organizations.



Messaging professionals who know and understand the content of the S/MIME Secure Messaging architecture should be capable of designing and/or deploying a secure messaging system based on the S/MIME set of standards.

The S/MIME Secure Messaging Architecture document offers a high level description of the S/MIME Secure Messaging Architecture and is intended for anyone involved in the planning, design or deployment of a secure messaging system based on the S/MIME set of standards and in particular for organizations and individuals planning to achieve certification under The Open Group's S/MIME Secure Messaging (SSM) certification program.

The architecture assumes expertise in information security principles.

Larger and easier to read versions of diagrams included in this article are available in the architecture document.

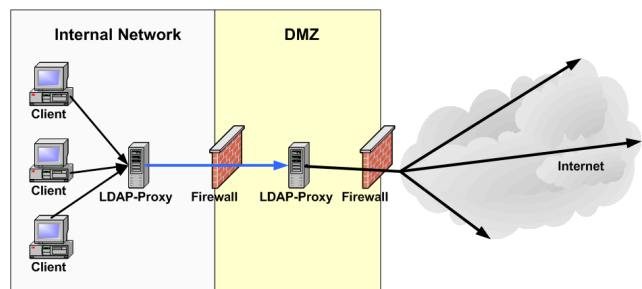
## How to get the SSM Architecture Document

The S/MIME Secure Messaging Architecture document is available for download, free of charge, via The Messaging Forum Web site.

<http://www.opengroup.org/messaging>

## The LDAP Proxy

A unique feature of The Open Group SSM Architecture is the introduction of the LDAP proxy to facilitate the publication and retrieval of security certificates.



The LDAP Proxy (illustrated above) provides a safe mechanism for an organization to make public a subset of the contents of their corporate directory, which may contain additional information which cannot be published. This avoids problems associated with data replication and reconciliation.

LDAP proxies may be chained in a bridge infrastructure.

The LDAP proxy used the standard LDAP protocols, so may be used with Commercial Off-the-Shelf e-mail software. Originally developed by Boeing as part of the original Messaging Forum Secure Messaging Challenge project, an open source implementation of the LDAP proxy is now available.

## S/MIME Secure Messaging Architecture - Contents

- ✚ Introduction
- ✚ Scope of the SSM Architecture
- ✚ Components of the SSM Architecture
- ✚ "To End" Desktop Solution
- ✚ "To Site" Gateway Solution
- ✚ Certification Authority Service Models
- ✚ Directory Services
- ✚ Validation Services
- ✚ Bridge Infrastructure Solutions

## S/MIME Secure Messaging Architecture Training and Examination

### Training Courses

A certified training course must address all of the topics identified in the core syllabus (box right).

Although attendance at a suitable training course is not mandatory for individual certification, it is strongly recommended as preparation for the examination.



Wen Fang of Boeing leads the first S/MIME Secure Messaging Training Course in Tokyo in November 2005.

A set of presentation material that can be used as the basis for building a certifiable course will shortly be available from The Messaging Forum. The Forum itself will be arranging a series of courses around the world during 2006.

### The Examination

An individual who wishes to be certified as having the necessary knowledge and understanding to deploy a secure e-mail system must pass an examination.

The examination takes the form of a workbook containing approximately thirty questions. Most of the questions are purely factual. Three questions will require a great deal more thought and are designed to test understanding.

Examination papers may either be obtained directly from The Open Group, or from a training organization at the end of a certified training course, and when completed must be returned to a designated examiner,

The examination is un-timed and open book.

### Program Introduction Plans

The S/MIME Secure Messaging Certification program is already open for applications from organizations and individuals wishing to achieve certification. Until the public launch of the program, these applications will be confidential.

The program will be launched, around the end of January 2006, at which point the first register of Certified Individuals will be published.

### Core Syllabus

Certified training courses must cover all of the mandatory elements in the core syllabus. The examination for individual certification may include questions on any of the mandatory elements in the core syllabus.

#### Mandatory elements:

- ✚ Rationale for Secure E-Mail
- ✚ Basic Internet E-Mail Architecture
- ✚ Information Security Principles
- ✚ Introduction to E-Mail Security
- ✚ Pre-requisites for Secure E-Mail
- ✚ Architecture Models for Secure E-Mail
- ✚ Components of a PKI
- ✚ Usage of a PKI
- ✚ Bridge Infrastructures
- ✚ Implementing a Gateway Encryption System

#### Optional elements:

- ✚ Secure Web E-Mail
- ✚ E-Mail Sender Authentication
- ✚ Content Management
- ✚ Configuration of specific E-Mail Products for Security
- ✚ Hands-on Sequence of Product Configuration

### The Secure Messaging Imperative

The S/MIME Secure Messaging Certification program is being introduced in response to a clear market need.

As an example of this market, one aerospace company is requiring all of its business partners working on an important new program to use e-mail encryption. By the middle of 2006, this means that 900 companies worldwide will need to deploy strong e-mail encryption.

The majority of these companies do not currently have the necessary knowledge and skills and will require professional assistance. This will range from:

- Training their own staff
- High level planning and implementation support (estimated at up to 2 person weeks per deployment)
- Turnkey deployments (estimated at up to 10 person weeks per deployment)

This is just one example. The automotive industry in Europe is starting to deploy e-mail encryption; HIPAA in the US and equivalent legislation in Europe is forcing the Healthcare Community to deploy e-mail encryption. The US Dept of Defence, the UK Ministry of Defence and other agencies worldwide are all mandating e-mail encryption.

## Letter from the Co-Chairs

Happy New Year!

We hope that you are enjoying this issue of the Message Magazine. The Electronic Mail Association (EMA) was founded in 1983, "devoted to promoting e-mail, voice mail, fax, EDI and other messaging technologies".

Today, the needs of the Messaging community are much different than when EMA was founded.

- In the 1980s, the need was to promote the use of e-mail and related technologies.
- By the 1990s, e-mail had become a widely used means of communication, and the need was to interconnect the "islands" of proprietary enterprise messaging systems.
- In 2001, The Open Group took over the work of EMA and created the Messaging Forum.
- Today, Messaging Professionals are faced with challenges that were unheard of when our organization was founded. E-mail viruses, unsolicited e-mail (SPAM), wireless messaging, instant messaging, regulatory compliance, e-mail security and unified communications are just some of the challenges that we face.

The Message Magazine is an important tool to help us publicize the work we have been doing in the Forum. In this issue of the Message Magazine, we focus on the S/MIME Secure Messaging (SSM) Certification Program.

The program is the first of a series of professional certifications that will encompass the knowledge and skills that are needed by today's Messaging Professionals.

The next edition, to be published in March will focus on Secure Messaging Gateways. In May, the Message will present a status update on the work that we are just now starting on Federated Free/Busy time searches.

Subsequent issues will address topics like Standardized PKI Policy Assurance, Bridging Certificate Authorities, Desktop E-mail Encryption, and Sender Authentication.

We invite you to join us in addressing the challenges that we face. We hope to see you at our next Messaging Forum meetings which will be held in conjunction with the Open Group Conference in Barcelona, Spain, January 23-25, 2006 and in Washington, DC, April 24-26, 2005.

Wen Fang, Russ Chung  
(Co-Chairs)

## Messaging Forum Active Work

Other projects within the Messaging Forum will be featured in detail in future issues of [The Message](#).

### Federated Free/Busy

The Messaging Forum is working together with The Calendaring and Scheduling Consortium on a vendor challenge project:

"By the end of Q2 2006 there should be a real-time mechanism that is able to extract and collate/display free/busy information from at least 3 major groupware packages using open standard protocols for a constrained list of named attendees and constrained list of times".

### S/MIME Gateway Certification

The SMG Certification program was introduced in July 2004 to ensure the interoperability of products that encrypt E-Mail at the organization gateway.

Four products are certified (from BT Syntegra, NetIQ Tumbleweed and ZixCorp) and have been successfully deployed by the Massachusetts Health Data Consortium.

In April 2006, the Forum plans to start work on version 2 of this program which will improve interoperability with Desktop-to-Desktop systems.

## Upcoming Events

### January, Barcelona, Spain

24 SSM Architecture Tutorial  
25/26 Forum Working Meeting

### April, Washington DC (Provisional)

24/25 SSM Architecture Training  
26/27 Forum Working Meeting

### July, Miami, Florida (Provisional)

18 Messaging Status Report  
19/20 Forum Working Meeting

### October, Lisbon, Portugal

24 Messaging Status Report  
25/26 Forum Working Meeting

For full details visit [www.opengroup.org/messaging](http://www.opengroup.org/messaging)

## In the next issue

The next issue of The Message to be published in March 2006 will focus on the S/MIME Gateway program.