

---

# Encryption at the Mail Gateway

THE *Open* GROUP

**Mike Lambert**

A Fellow of The Open Group  
Director, Messaging Forum

GSM +44 7770 451167

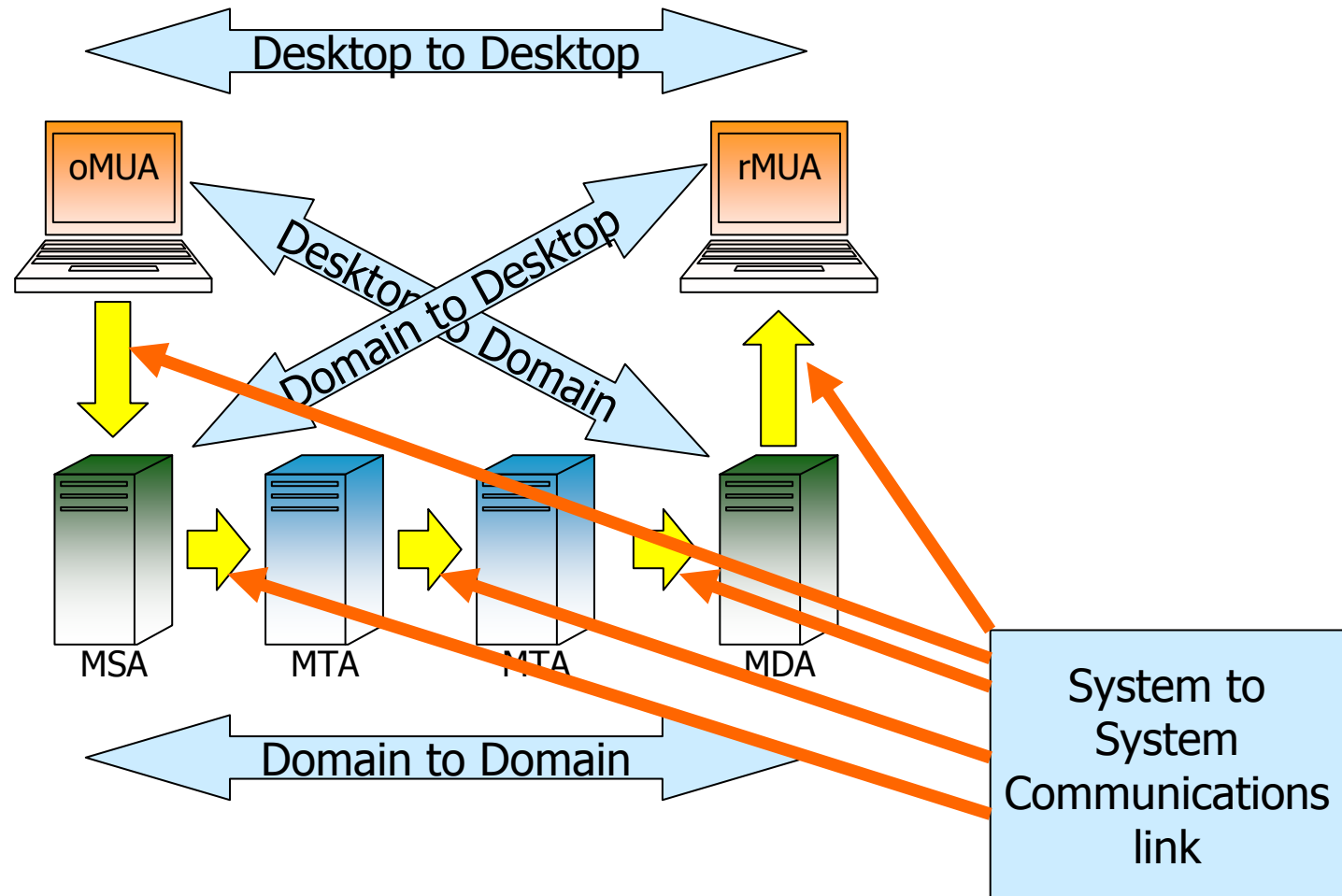
[m.lambert@opengroup.org](mailto:m.lambert@opengroup.org)

79, Camrose Way  
Basingstoke  
Hants, RG21 3AW  
United Kingdom

Tel +44 1256 414513  
Fax +44 20 7691 7868  
[www.opengroup.org](http://www.opengroup.org)

THE *Open* GROUP

# Encryption Options

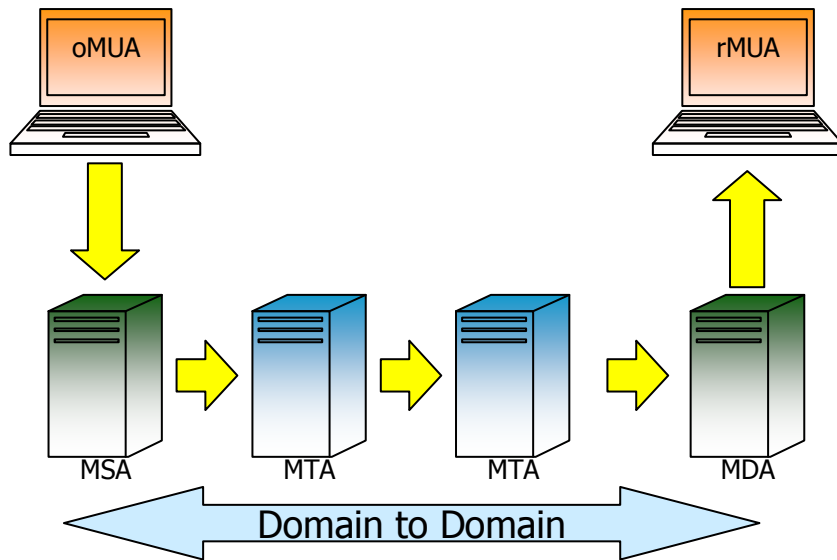


# Desktop S/MIME Challenges

---

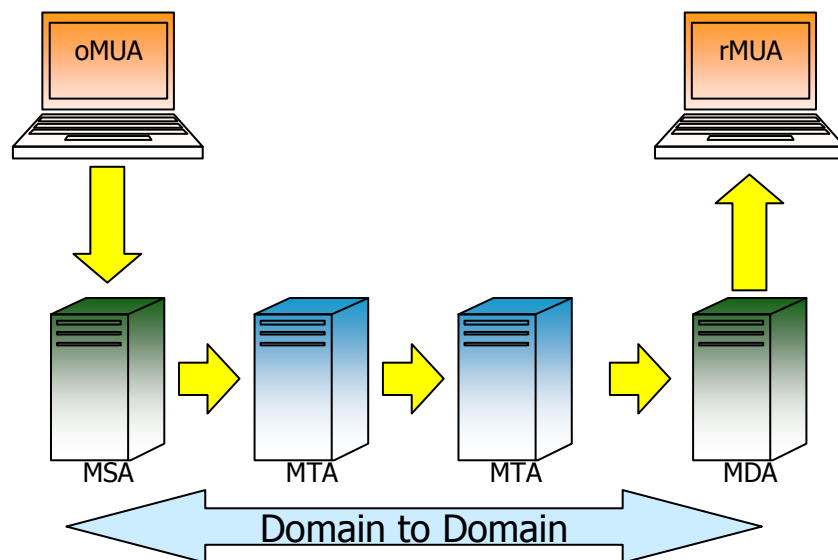
- ❑ Key Management
  - There is no universal Public Key Infrastructure
  - Certificate management is complex and expensive
- ❑ Encrypted messages can deliver Spam and malware to the desktop
  - Desktop-to-desktop encryption by-passes enterprise level scanning
- ❑ Too many options
  - No encryption algorithm mandated
  - No level of security mandated

# Domain to Domain Encryption



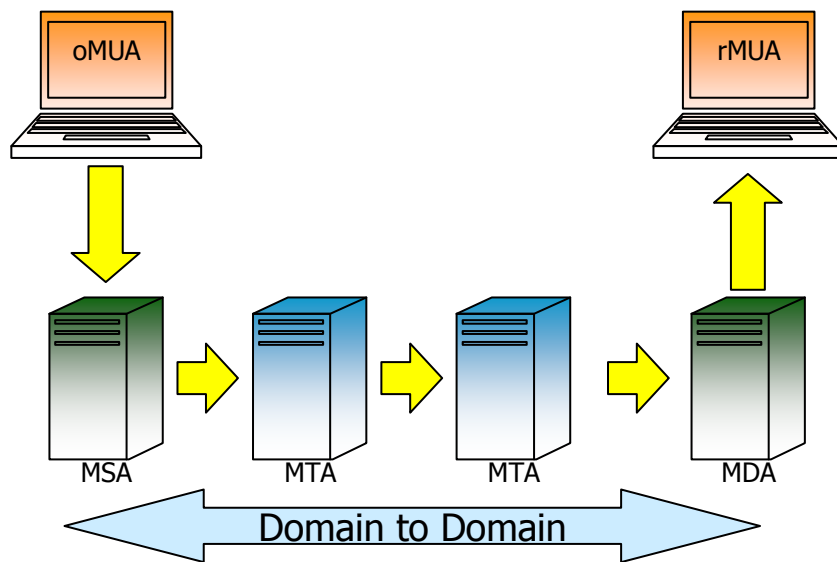
- Mail is
  - transmitted in the clear to the MSA at the domain boundary
  - encrypted at the originator's MSA
  - transmitted throughout the public network in an encrypted form
  - decrypted at the recipient's MDA at the domain boundary
  - transmitted in the clear to the recipients MUA
- The MUA does not need to be security aware

# Domain to Domain Encryption using TLS



- ❑ TLS can deliver Domain to Domain encryption but
  - if there are intervening MTAs, the message is processed in the clear
  - the mail system is not aware if any of the links are not encrypted, so policy cannot be enforced
  - TLS provides a basic level of security .. not sufficient for high value content

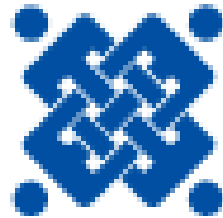
# Domain to Domain Encryption using S/MIME



- ❑ Overcomes major disadvantages of TLS
  - Message is encrypted throughout its transit of the public network
  - It is processed at relays and mediators in encrypted form
  - The MSA determines whether encryption is necessary

# July 2003 - Boston, MA

---

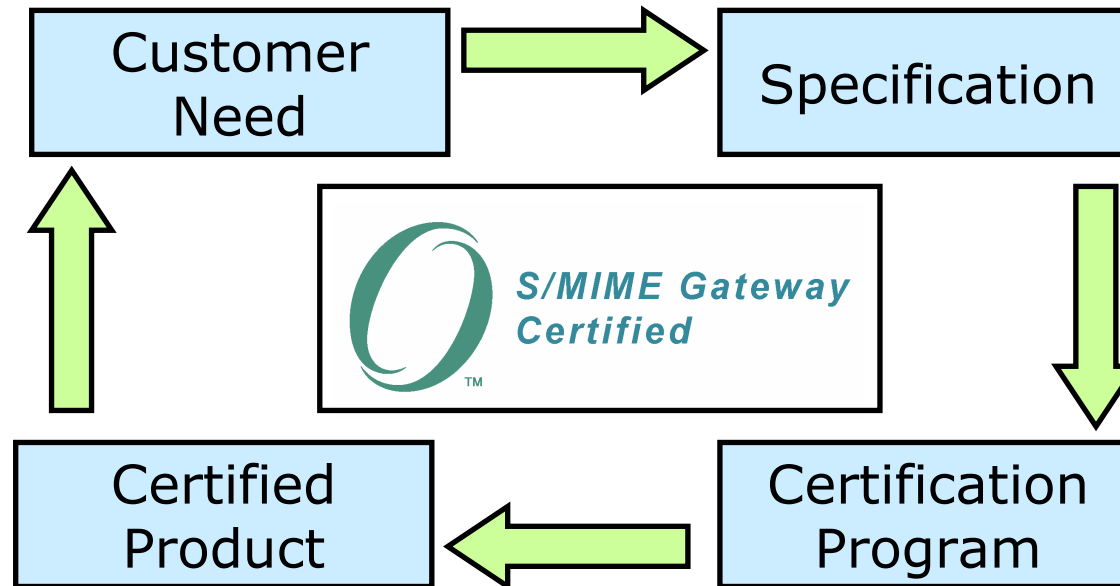


Massachusetts  
Health Data  
Consortium

THE *Open* GROUP

Easy to manage ability to encrypt e-mail containing personal health information (PHI) over public networks.

Vendors agree profile of IETF S/MIME standard for encryption of e-mail at organization boundary.



Customer procurement specifying certified products  
 → Products available that meet customer needs.

Guaranteed conformance to SMG specification.  
 Interoperability testing protocol.

# S/MIME Gateway Specification- v1

---

- ❑ A profile of S/MIME v3.1 (RFC 3851)
- ❑ Uses “Domain Certificates”
  - Same basic format as desktop-to-desktop S/MIME certificates
  - Fixes some options in certificate format
- ❑ Mandates minimum encryption strength
  - 1024-bit RSA, 3DES, SHA1
  - Others allowed
- ❑ Establishes a simple pragmatic mechanism for key exchange
  - Signed e-mail to a known address (Manual step to authenticate is permitted)
  - Send in standard format (e.g. on diskette)
  - Meets MHDC requirement (but does not scale)
- ❑ Defines a mandatory interoperability testing scheme

# S/MIME Gateway Features

---

- ❑ Co-exists with unencrypted SMTP
- ❑ Co-exists with desktop-to-desktop S/MIME
  - Will not decrypt/verify signatures
  - Will deliver to recipient with encryption/signature intact
  - Local policy may reject messages using desktop-to-desktop encryption (to enable virus or content checking)



*S/MIME Gateway  
Certified*



# Next Steps

---

- Work will start in April on development of version 2
  - Better integration with the desktop-to-desktop solution
  - Automated key exchange
  - Signatures

---

# Domain Gateway Encryption

THE *Open* GROUP

**Mike Lambert**

A Fellow of The Open Group  
Director, Messaging Forum

GSM +44 7770 451167

[m.lambert@opengroup.org](mailto:m.lambert@opengroup.org)

79, Camrose Way  
Basingstoke  
Hants, RG21 3AW  
United Kingdom

Tel +44 1256 414513  
Fax +44 20 7691 7868  
[www.opengroup.org](http://www.opengroup.org)

THE *Open* GROUP