

# SecMX

A modest proposal to enhance MTA <-> MTA security

Andrew McMillan

NZNOG, Wellington, 2006

# History (Secure email)

- SEEMail – govt-to-govt (1999)
  - Individual S/MIME (end-to-end)
    - Client software issues
    - Content review issues
    - Info mgmt issues
  - Gateway S/MIME (boundary-to-boundary)
    - Useful (40+ agencies) / successful
    - Big issues if you lose the key or CRL

# History (Secure email)

- Govt-to-citizen
  - Agencies / webmail
  - Citizen not in control
  - Many mailboxes / logins
- Working group with NZ ISPs
  - Normal email with security
  - SEEMail (gateway S/MIME)?

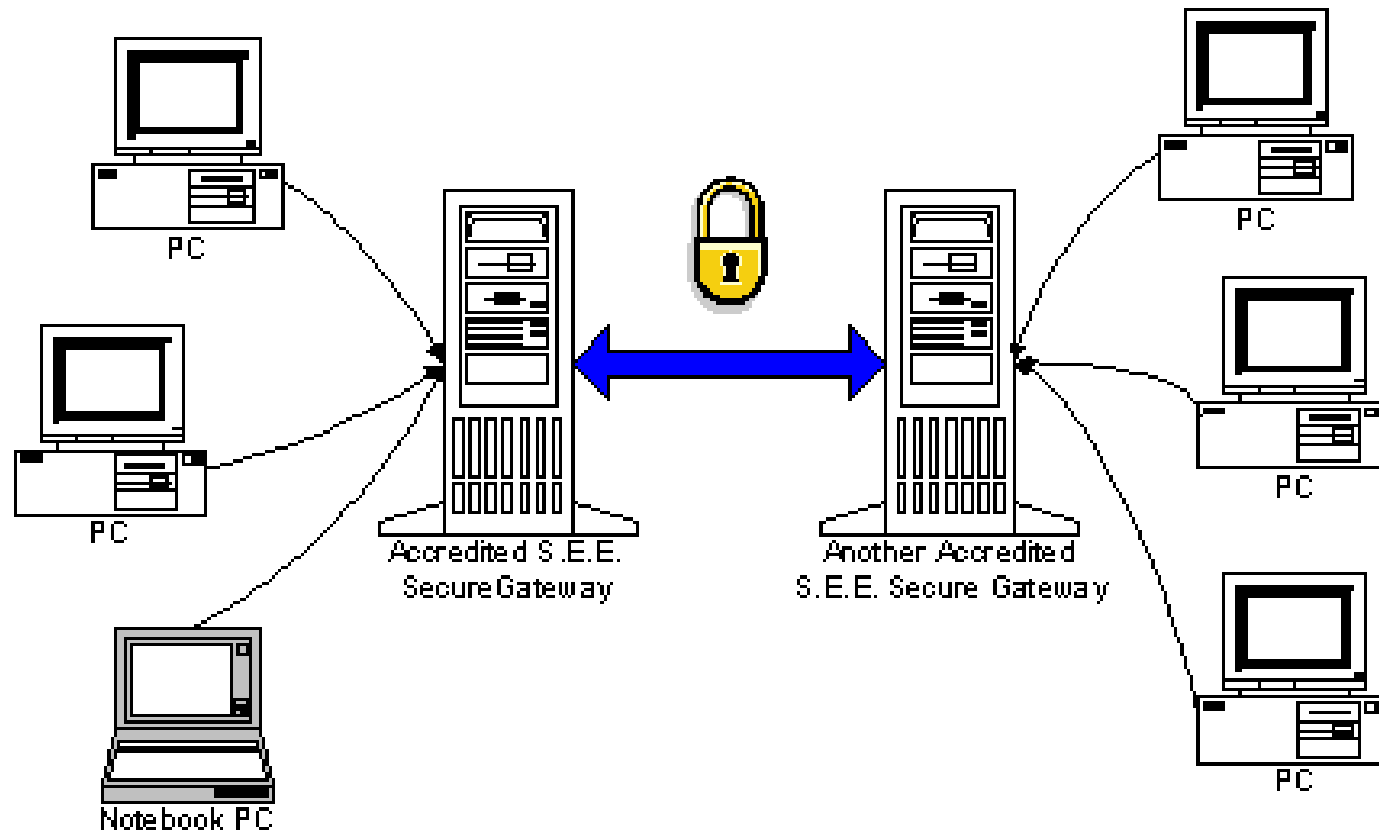
# SEEMail issues - ISP

- Cost
  - Per seat licensing / will users pay for it?
- Fail-safe
  - If it fails, will it cause problems?
- Existing experience
  - Can I find staff that understand it?

# Gateway

- Gateway TLS (SSL) functionality
  - It exists and is standardised
  - It is active – 10% .nz domainspace
  - So why isn't it used?
- Chicken n' egg issue

# A secure building block



# But that's not secure!

- Security obligation:
  - Government – post – citizen
  - Government – post – pobox – citizen
- SecMx obligation
  - Government – email – mailbox – citizen
- Existing ISP services
  - Webmail with SSL
  - POPS, IMAPS

# Security by default

- BES
  - Best Effort Sender
  - Turn it on - use TLS if possible
- BER
  - Best Effort Receiver
  - Turn it on - use TLS if possible
- Do we need minimum standards
  - TLS
  - Sender authentication

# Remaining Issues

- All government agencies will use TLS if available  
BUT some sensitive messages must ONLY be sent securely
- How do you “send-safe” (fail-safe) ?

# SecMx – Stage 2

- BES
  - Best Effort Sender
  - Use SOR if possible or use TLS if possible
- BER
  - Best Effort Receiver
  - Use TLS if possible
- SOS
  - Secure Only Sender
  - Custom code - find a SOR or bounce message
- SOR
  - Secure Only Receiver
  - Port 25 – only accept TLS

# Technical stuff

- How do you discover and connect to a secure server (SOR)?
  - SRV record
  - MX weighting convention: 51966
  - Domain naming convention: secmx.agency.govt.nz
  - New DNS type record

# What SecMX is not

- Assumes sender authentication happens
  - SPF, SenderID, Digital certificates
- Assumes TLS negotiation is between parties
- Assumes each party (sender, receiver) is responsible for their own internal security
- Assumes DNS is good-enough for now; DNSSEC is a future option