

SSL Certificates and E-mail Signing and Encryption

Presented By: Armen Varjabedian
Assistant Director, OIT
Microcomputer Support Services Group (MSSG)

SSL Certificates

- Commercial Certificate Authorities (CA)
 - University-signed
 - Self-signed
-

Commercial CA

- Cost money
 - Thawte - \$199 new, \$149 renewal
 - Recognized as valid by major browsers
 - Recommended for widely used sites, especially if used by non-University users
 - Available from Software Portal
-

University-signed

- ❑ Free
 - ❑ Gaining wider internal use over time
 - ❑ Certificate installation is easy
 - ❑ Ideal for University only sites, especially when user base is a specific group
 - ❑ Available from Software Portal
-

Self-signed

- Free
 - Limited recognition
 - Recommended for testing or development work only
 - Generated on local server
-

Software Portal

□ <https://software.rutgers.edu>

E-mail Signing

- Multiple free options
 - University signed
 - Commercially signed
 - Thawte Freemail Web
 - Comodo Trust Network
 - PGP/GPG
-

E-mail Signing

- University-signed
 - Identity is confirmed
 - Same drawback with the CA being recognized by e-mail clients
-

E-mail Signing

- Commercially signed
 - CA is recognized by e-mail clients
 - Identity is not confirmed by default
 - Identity confirmation is a manual/non-technical process
-

E-Mail Signing

PGP/GPG

- Requires installation of additional software on Windows
 - <http://www.gpg4win.org>
 - Client software requires plug-in
 - Outlook 2003 – GpgOL
 - Thunderbird - Enigmail
-

E-mail Encryption

□ Public/Private Key method

- Sender encrypts e-mail with public key of recipient
 - With SSL, recipient must provide public key
 - With PGP/GPG, public keys available from public keyservers
-