Dane/SMIMEA Mail User Agent Prototype

Eric Osterweil
Lynch Davis
Gowri Visweswaran

November, 2014

Prototype Goals

- Learn about usage of S/MIME with DANE within a common MUA
- Give an open/free utility to the community

- Step 1:
  - Develop an S/MIME client that uses DANE work to support the discovery and usage of S/MIME certificates from DNS.
- Step 2:
  - Consider observed pain-points and other foreseeable deployment issues

- Based on our prototype/evaluation of the draft SMIMEA proposal:
  - We included _sign and _encr proposed enhancements
  - Support Cert Access field (NAPTR) as part of record
  - SHA224 encoding of local email

SMIMEA aspects

- We did query and processing in demo software using the getdns library / API
  - All DANE logic is encapsulated into a library shim above libgetdns
- We manually provisioned SMIMEA records into VerisignLabs.com test domain
  - Then signed normally
- Currently, users drive when DANE is used, using UI buttons
  - It's not automagic (yet), users still invoke actions

Encryption and Sending

http://www.lipsum.com

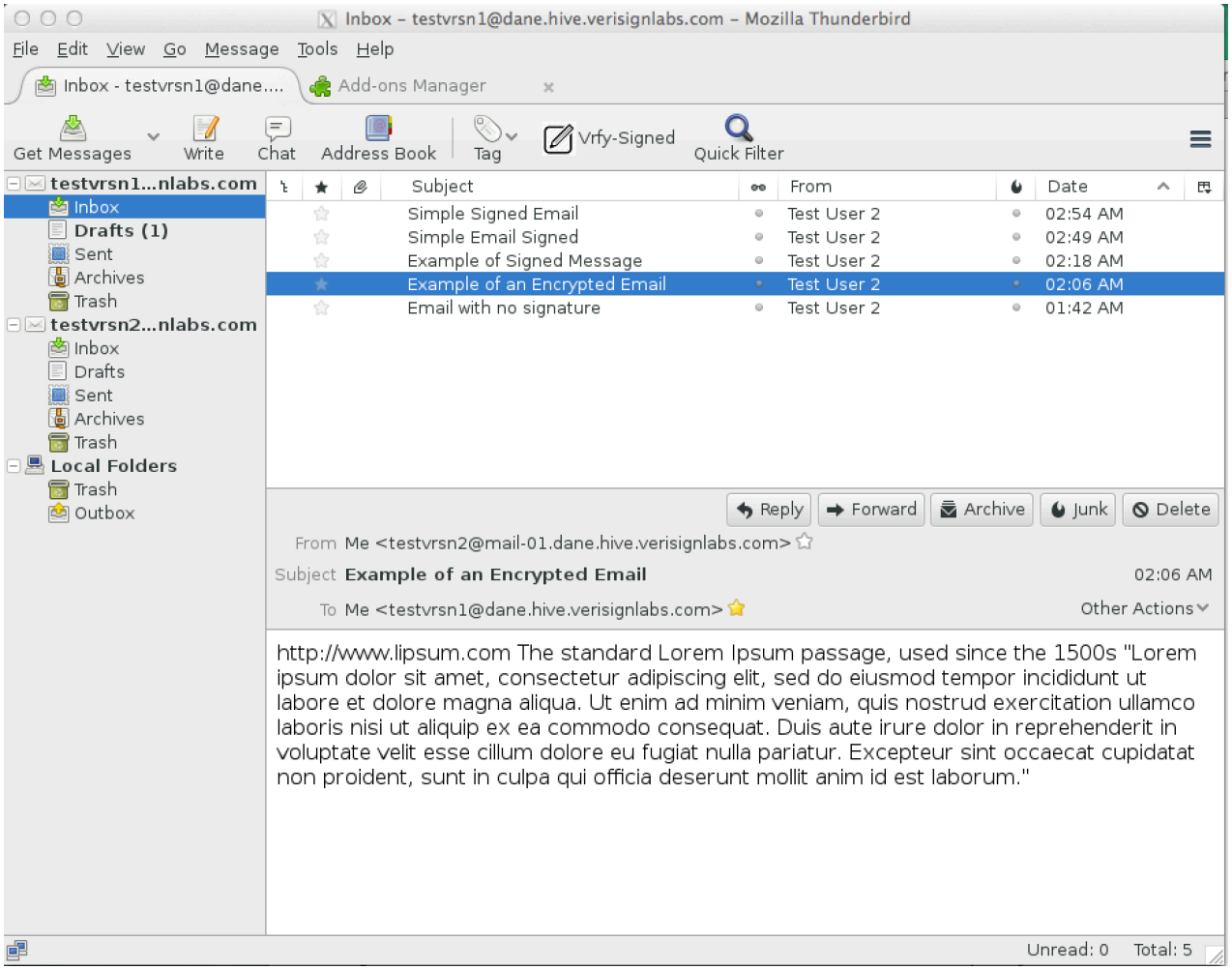
The standard Lorem Ipsum passage, used since the 1500s

"Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed do eiusmod tempor incididunt ut labore et dolore magna aliqua. Ut enim ad minim veniam, quis nostrud exercitation ullamco laboris nisi ut aliquip ex ea commodo consequat. Duis aute irure dolor in reprehenderit in voluptate velit esse cillum dolore eu fugiat nulla pariatur. Excepteur sint occaecat cupidatat non proident, sunt in culpa qui officia deserunt mollit anim id est laborum."

MIME-Version: 1.0
Content-Disposition: attachment; filename="smime.p7m"
Content-Type: application/x-pkcs7-mime; smime-type=enveloped-data; name="smime.p7m"
Content-Transfer-Encoding: base64

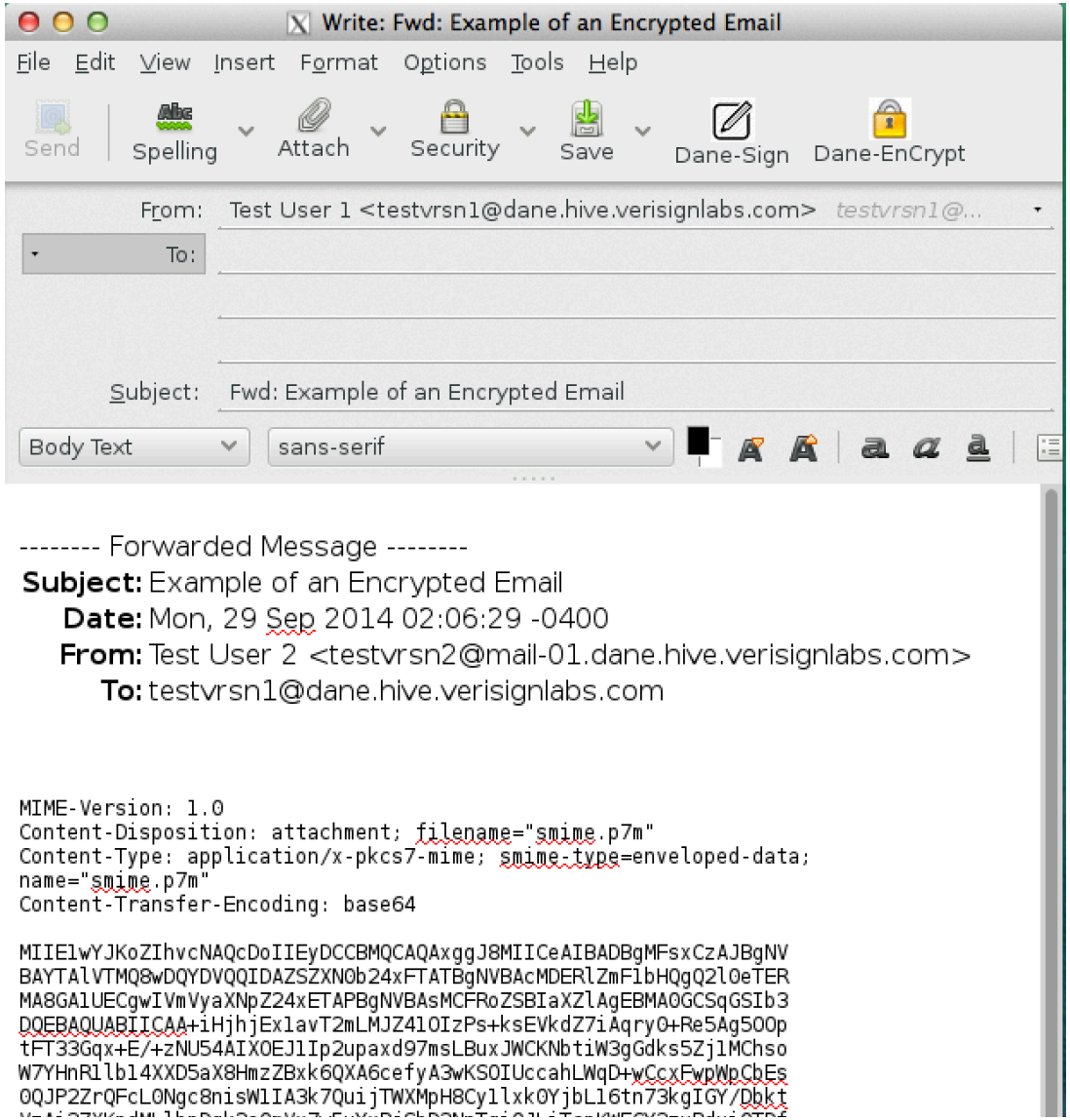
MIIE1wYJKoZIhvcNAQcDoIIEyDCCBMQCAQAxggJ8MIICeAIBADBgMFsxCzAJBgNV
BAYTAlVTMQ8wDQYDVQQIDAZSZXN0b24xFTATBgNVBAcMDERlZmF1bHQgQ2l0eTER
MA8GA1UECgwIVmVyaXNpZ24xETAPBgNVBAsMCFRoZSBlaXZlAgEBMA0GCSqGSIb3
DQEBAQUABIICAA+iHjhjEx1avT2mLMJZ41OIzPs+ksEVkdZ7iAqry0+Re5Ag5OOp
tFT33Gqx+E/+zNU54AIXOEJ1lp2upaxd97msLBuxJWCKNbtiW3gGdks5Zj1MChso
W7YHnR1lb14XXD5aX8HmzZBxk6QXA6cefyA3wKSOIUccahLWqD+wCcxFwpWpCbEs
0QJP2ZrQFcL0Ngc8nisW1IA3k7QuijTWXMpH8Cy1Ixk0YjbL16tn73kgIGY/Dbkt
VzAi37XKpdMLlbpDgk2aQmVx7w5uYxRjSbD3NnTgiOJLiTcpKWEGY3zvBdvi0TDf
Digt/El2xJV0NB7/zS18gaii1jIzmAxIohyKu4X+o6N+8/tL3TpxxfyLBRg0FMJh
mqjJ8hee5opFPUkBnVDJYkKQfzDcjBJIx8IpPTtLGf+jX5SPP6EPOh/0N/iu00ix
0C+A4jqknbc5le+U+Tz+czFeFvQdd9V2LJjxXWR50wX2ITCVcznJwEbe3LHF/c27
0hYktSDgt6qXap0W+kLtNapGjTXvKBed4hiS8H/e4Uyw5XU5183xkQp/YEm/rqa9
t921X8Zy6uUECQKSXMXMsrTWUE16gz4UNbtLBf/DgTHk34zA1HdpClKBd2Q2XMd7
MM6a8+Y9dGCa+8o2G1Q7Lpbj/7ycJZfQofBLuQt7+gTBQMrWRWiw0gZuMIICPQYJ
KoZIhvcNAQcBMBQGCCqGSIb3DQMHBAhPrEO7f8pV5YCCAhj3bWqoaxKDblOrrOeO
iMkdwY4wgbjz+x5qqQQFSJASGVGCarcUm9mLtiDRyrmlLbfMxuBk7D3GEY9Fkjyc
UnwQ/rsCDJnRwuLjhqIILIuTt7MHMaBdbr19a48/Lf5lTnSJRfe37h9m21sMOcU/
72J1KHbj3d/DBpcNA0F2Ybi0enIC26EdHhEPs9Sck96LcZj2XVTW03hNM4IsM8Ls
7eMNvPeX1klbZYU7bniGP09X43f/SkAFiEL1zKZL8AIhvtE89+JZNgNg6tUKEvGE

Encryption and Reading



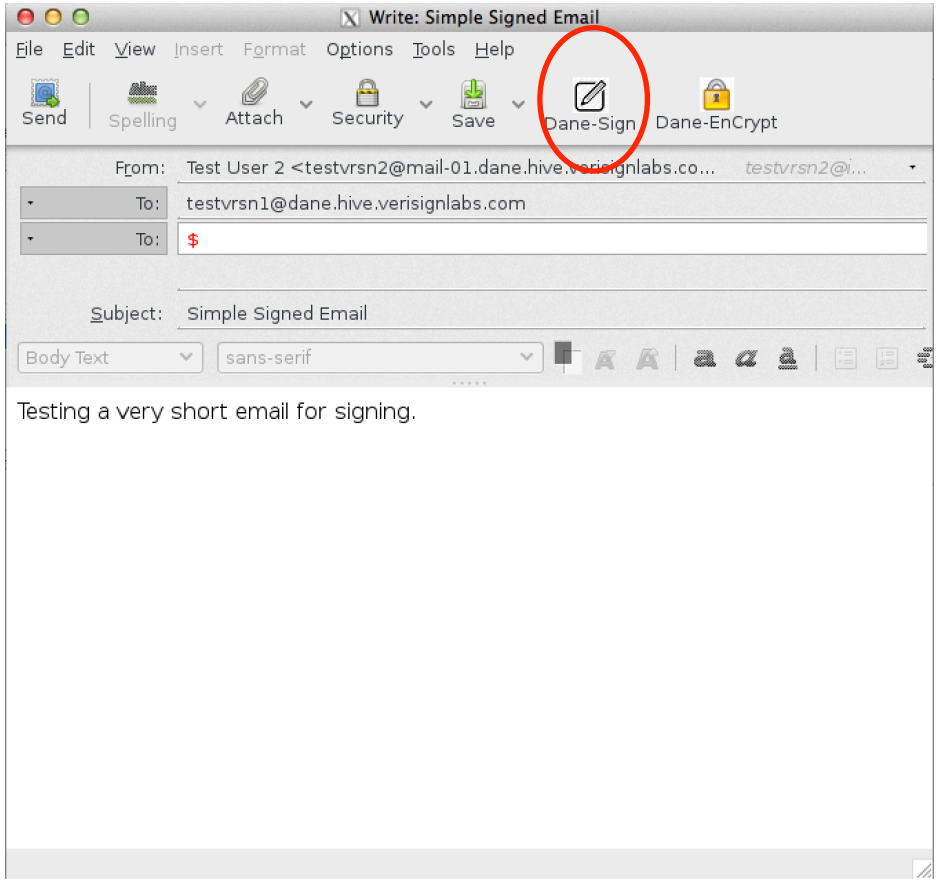
- Decrypted for display pane only
- Encryption is preserved (clear text not written to disk).
- Plugin scans email on selection

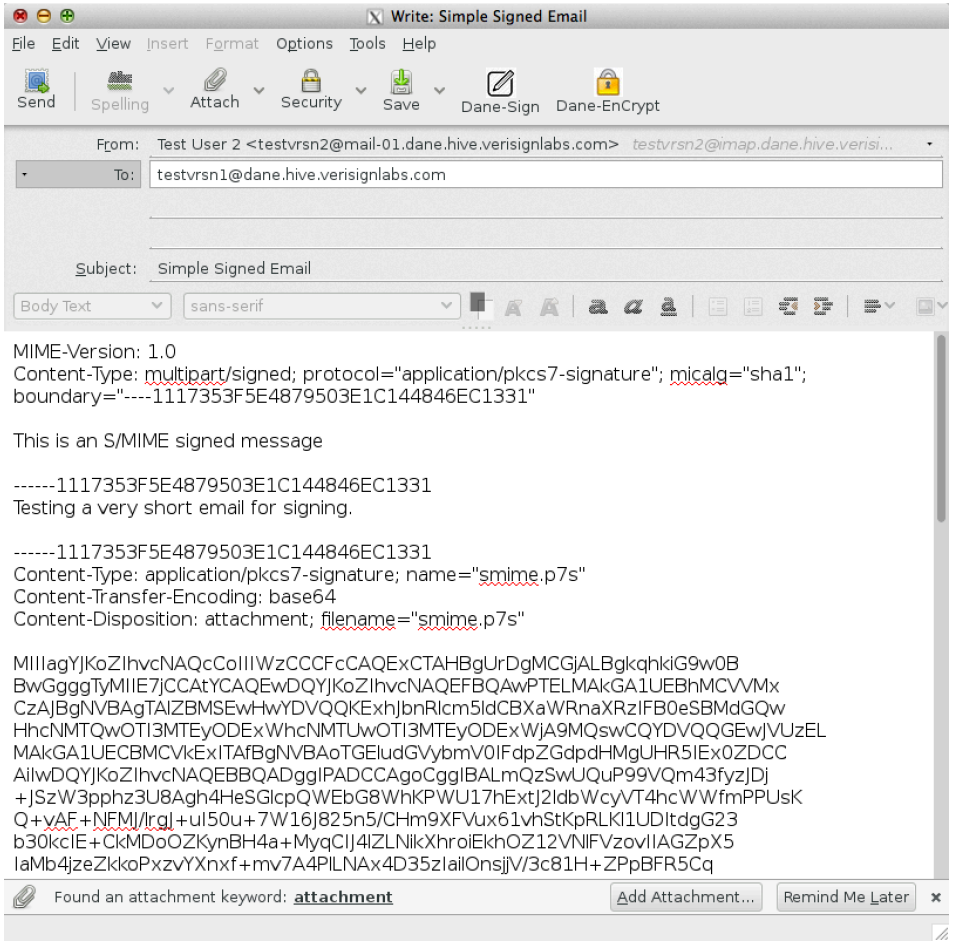
Encryption and Reply/Forwarding



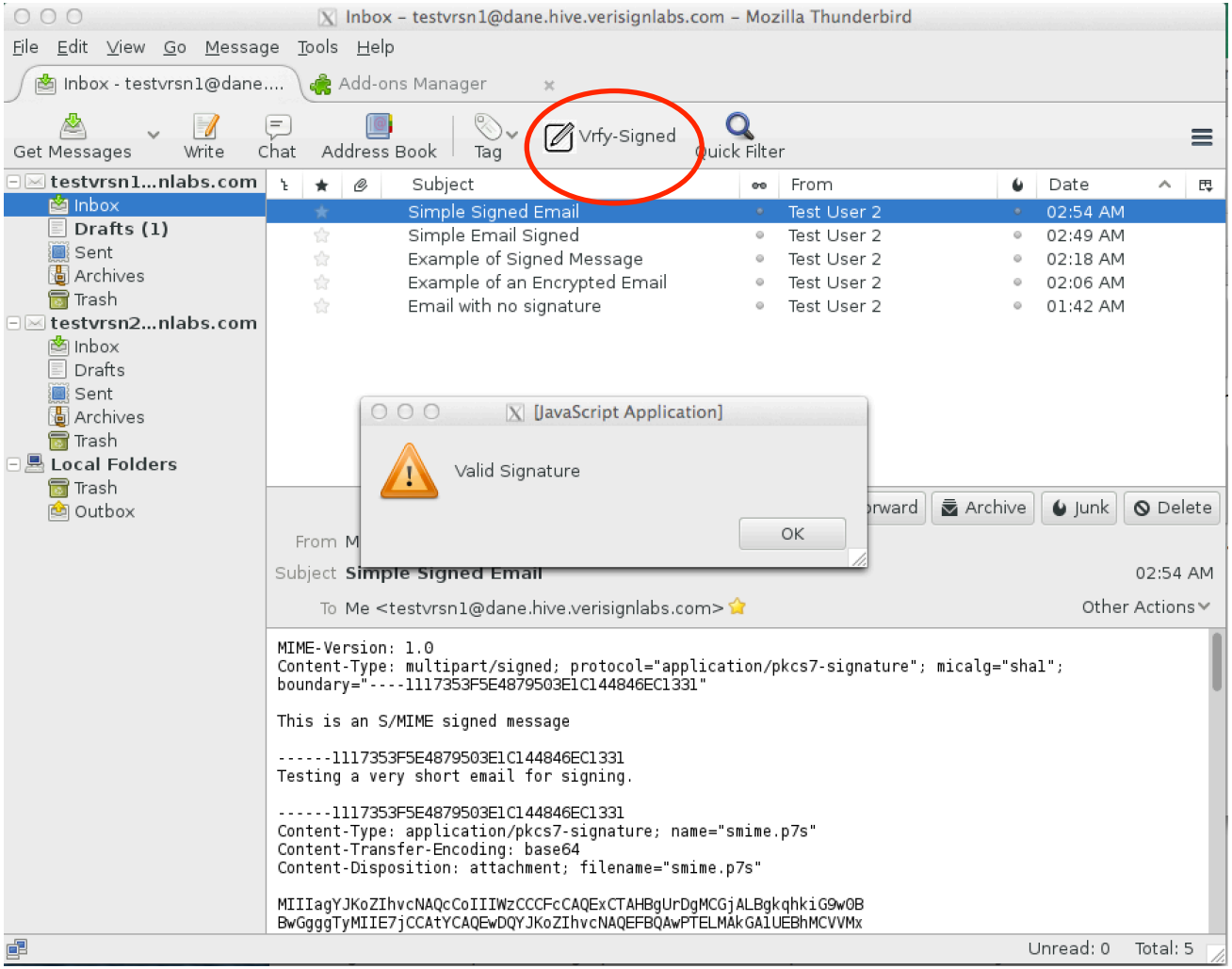
- Encryption is preserved.
- Original encryption must have included potential additional recipients for further dissemination

Message Signing/Verification





Message Signing/Verification



- On Demand signer verification
- One button validation of the signature.

Thanks