DANE/SMIME A Mail User Agent Prototype
Lynch Davis, Senior Engineer, Innovation Lab
Eric Osterweil, Principal Scientist, Research Lab
October 15, 2014
Prototype Goals

- Development of a S/MIME client that uses DANE work to support the discovery and usage of S/MIME certificates from DNS.

- Implementation of draft SMIME proposal
  - Includes _sign and _encri proposed enhancements
  - Support NAPTR as part of record
  - SHA224 encoding of local email
Prototype Architecture
Architectural Considerations

- Libraries/Class Abstraction
  - C/C++
  - Linux/Unix Platform
  - Shared Library
- Decoupled from UI
- Encapsulates getDNS
- OpenSSL
Thunderbird Integration
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."
Encryption and Reading

Decrypted for display pane only

Encryption is preserved (clear text not written to disk).

Plugin scans email on selection

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."
Encryption and Reply/Forwarding

Encryption is preserved.

Original encryption must have included potential additional recipients for further dissemination.
Testing a very short email for signing.

This is an S/MIME signed message

------1117353F5E4879503E1C144846EC1331
Testing a very short email for signing.

------1117353F5E4879503E1C144846EC1331
Testing a very short email for signing.

MIME-Version: 1.0
Content-Type: multipart/signed; protocol="application/pkcs7-signature"; micalg="sha1"
boundary="----1117353F5E4879503E1C144846EC1331"

This is an S/MIME signed message

------1117353F5E4879503E1C144846EC1331
Testing a very short email for signing.

------1117353F5E4879503E1C144846EC1331
Testing a very short email for signing.

MIME-Version: 1.0
Content-Type: multipart/signed; protocol="application/pkcs7-signature"; micalg="sha1"
boundary="----1117353F5E4879503E1C144846EC1331"
Message Signing/Verification

On Demand signer verification
- One button validation of the signature.
Challenges & Findings
Provisioning/Management

- Record management must be simplified
  - Provisioning Platform
  - Tools for Enterprise
  - Tools for Registrars

- Need to abstract certificate from user
  - Better integration with MUA
  - Need adoption by developers
Limitations of Libraries

- Lacking configuration flexibility in the Thunderbird UI
- Smooth integration with MUA/UI depends on open interfaces
  - Struggle for access to complete Thunderbird data structures
  - Existing Thunderbird API likes to format for presentation
    - Impacts verification due to changes to format/content!
    - Only supports signing for small messages
- Current code utilizes self-signed certs rather than CA
- Enhancement needed for passcodes/passwords for private keys
- Signing to compare key to _sign key from DNS
Questions/Contact

Lynch Davis, Sr. Engineer, Verisign Innovation Lab
jldavis@verisign.com

Eric Osterweil, Principal Scientist, Verisign Labs
eosterweil@verisign.com