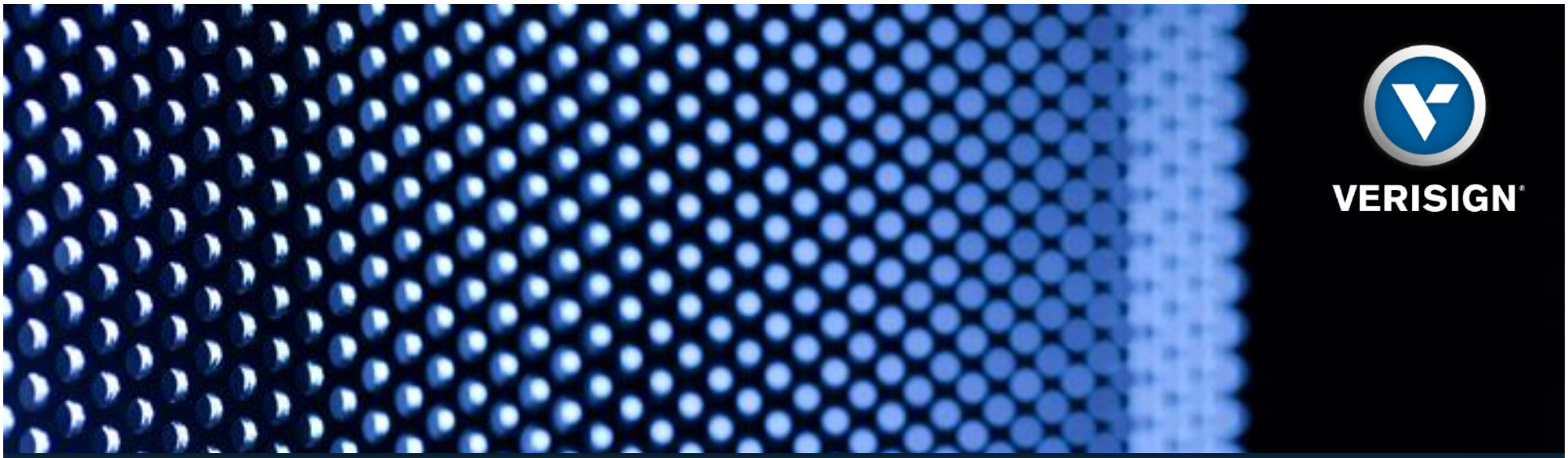


DANE/SMIME A Mail User Agent Prototype

Lynch Davis, Senior Engineer, Innovation Lab

Eric Osterweil, Principal Scientist, Research Lab

October 15, 2014

Prototype Goals

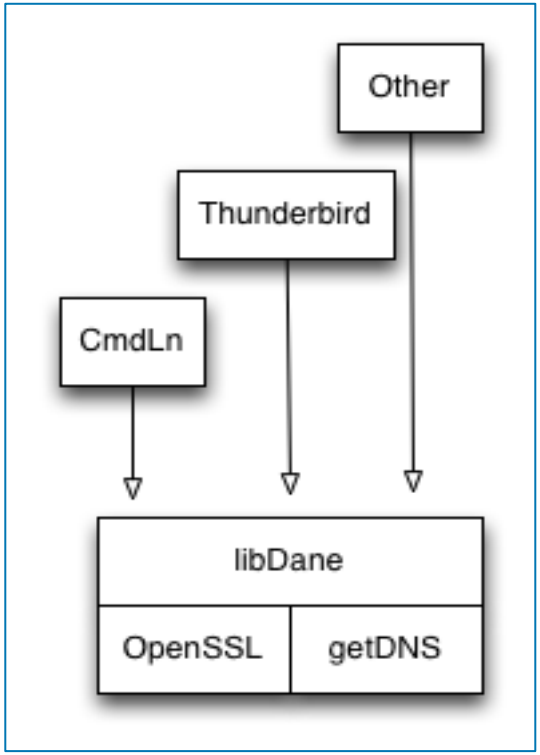
- Development of a S/MIME client that uses DANE work to support the discovery and usage of S/MIME certificates from DNS.

- Implementation of draft SMIME proposal
  - Includes _sign and _encr proposed enhancements
  - Support NAPTR as part of record
  - SHA224 encoding of local email

Prototype Architecture

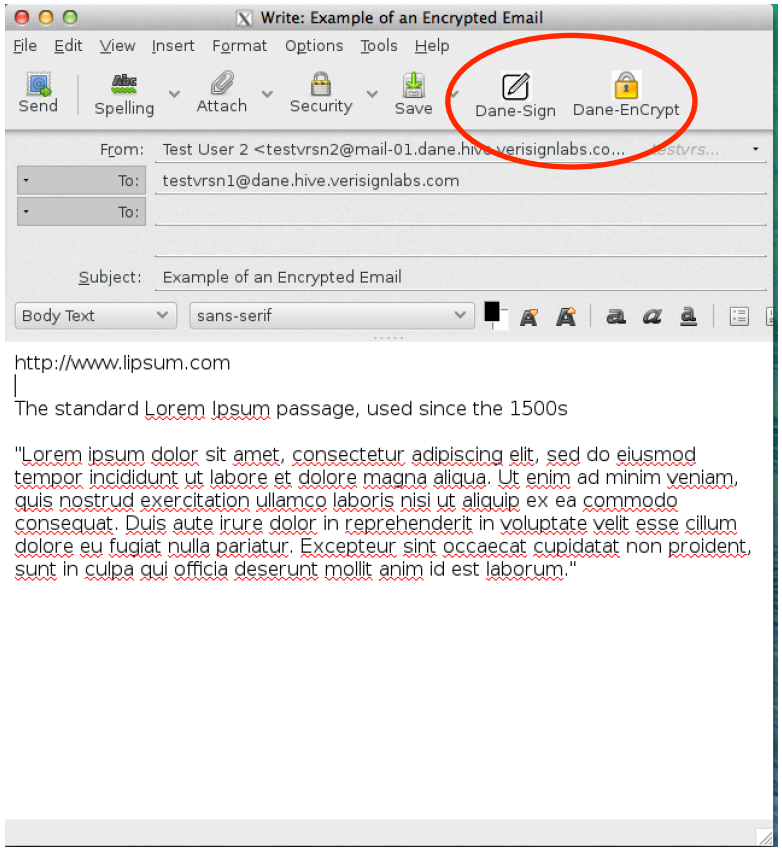
Architectural Considerations

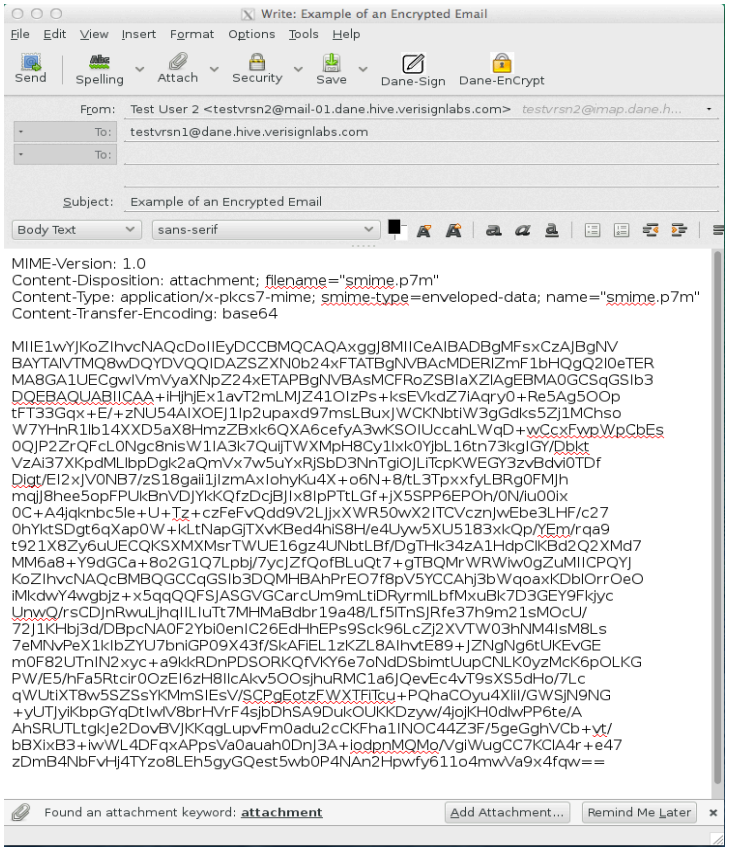
- Libraries/Class Abstraction
  - C/C++
  - Linux/Unix Platform
  - Shared Library
- Decoupled from UI
- Encapsulates getDNS
- OpenSSL



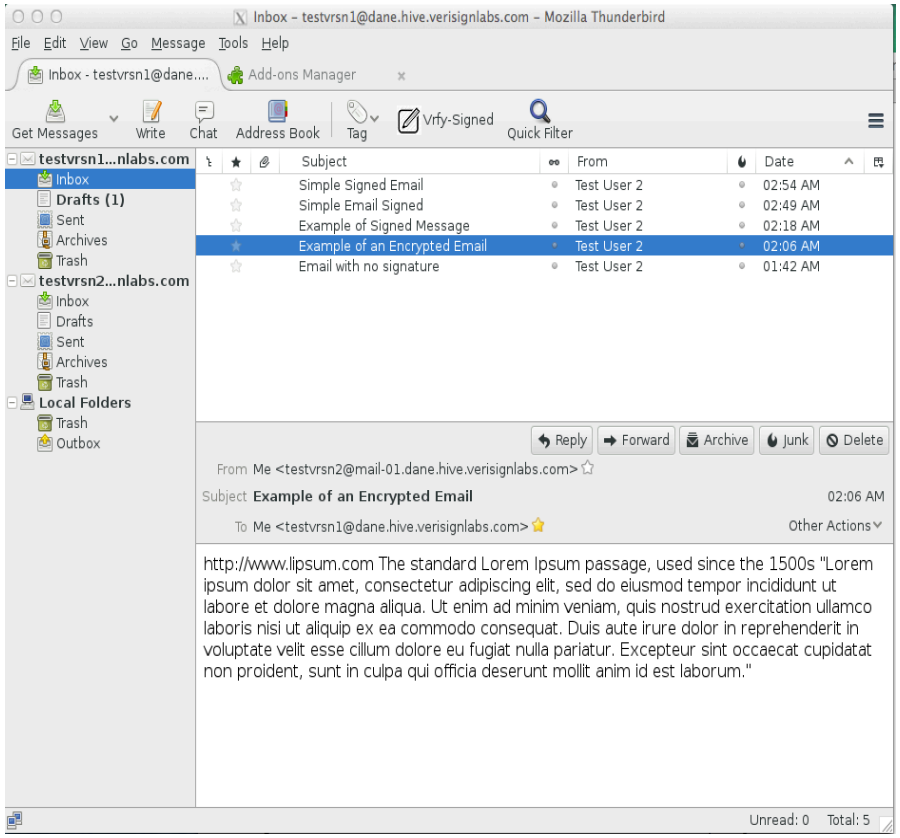
Thunderbird Integration

Encryption and Sending





Encryption and Reading

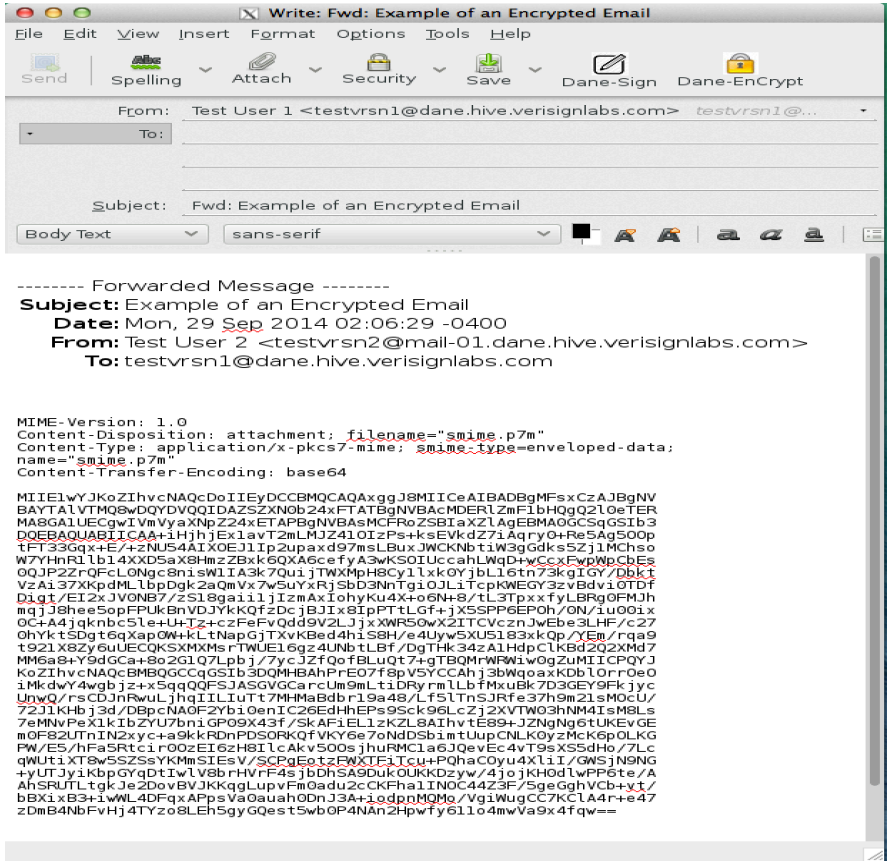


Decrypted for display pane only

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

Plugin scans email on selection

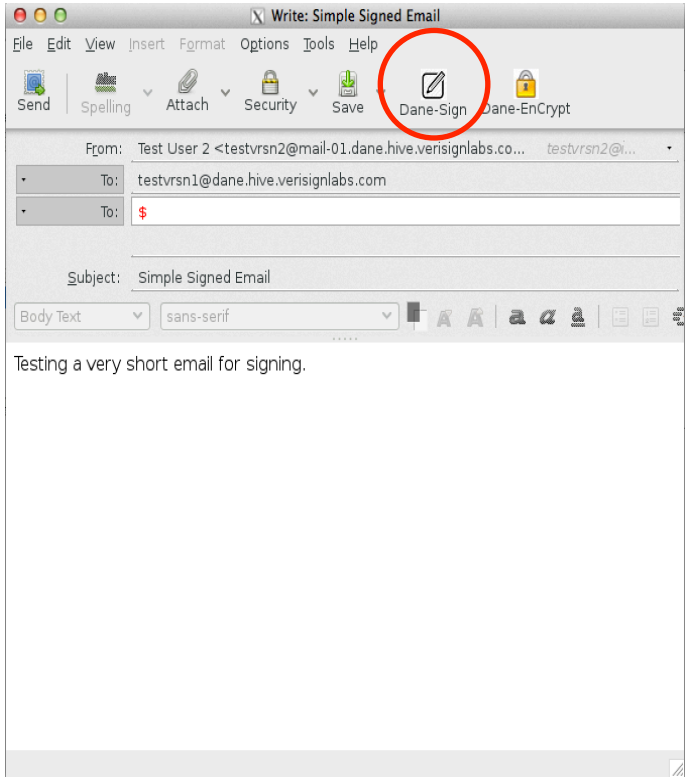
Encryption and Reply/Forwarding

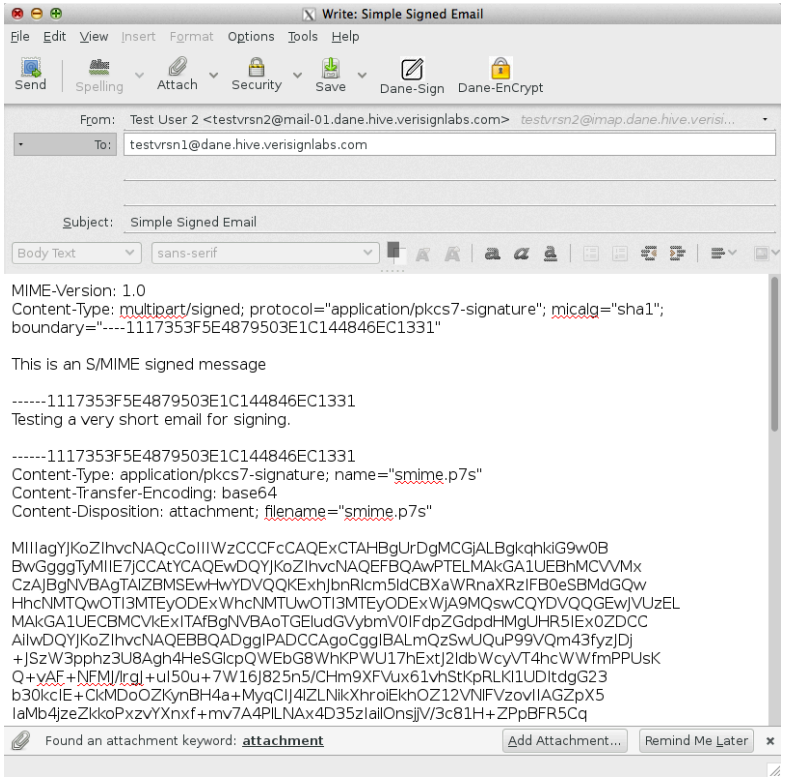


Encryption is preserved.

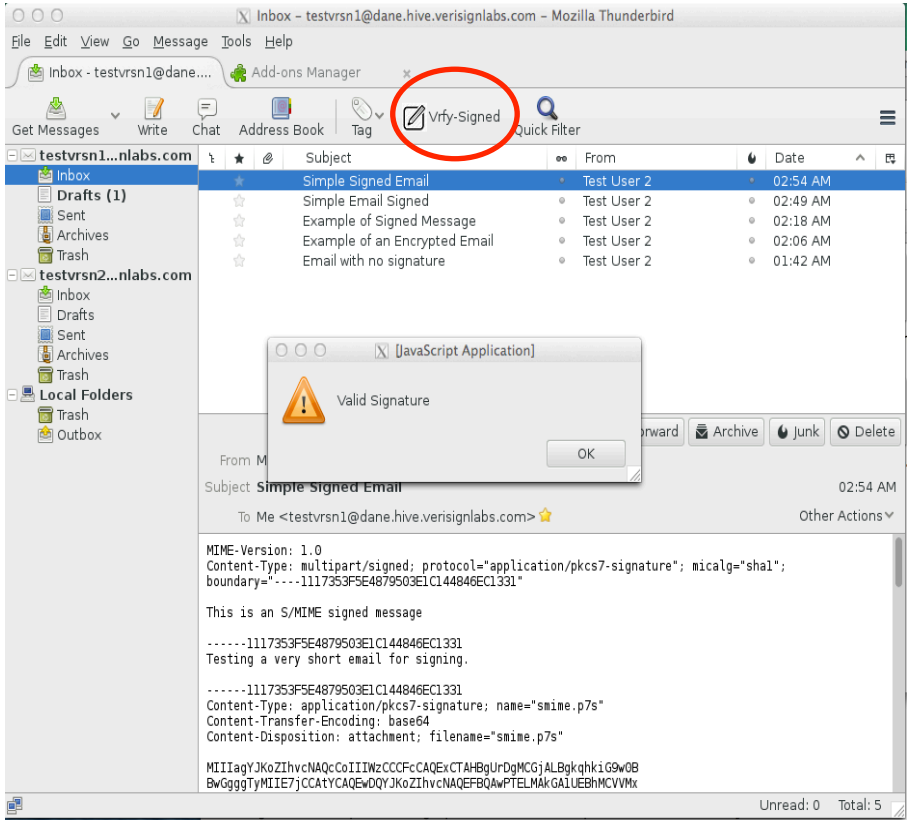
Original encryption must have included potential additional recipients for further dissemination

Message Signing/Verification





Message Signing/Verification



On Demand signer verification

- One button validation of the signature.

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

VERISIGN®