



VERISIGN®

# DANE/SMIME A Mail User Agent Prototype

Lynch Davis, Senior Engineer, Innovation Lab

Eric Osterweil, Principal Scientist, Research Lab

October 15, 2014

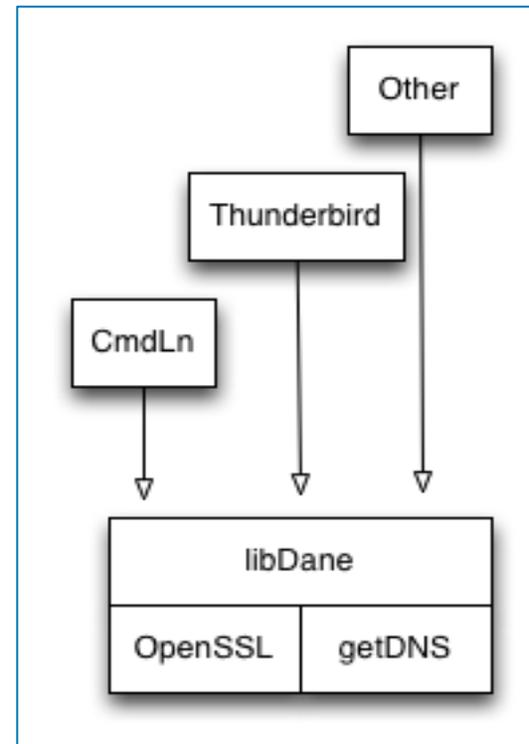
## Prototype Goals

- 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

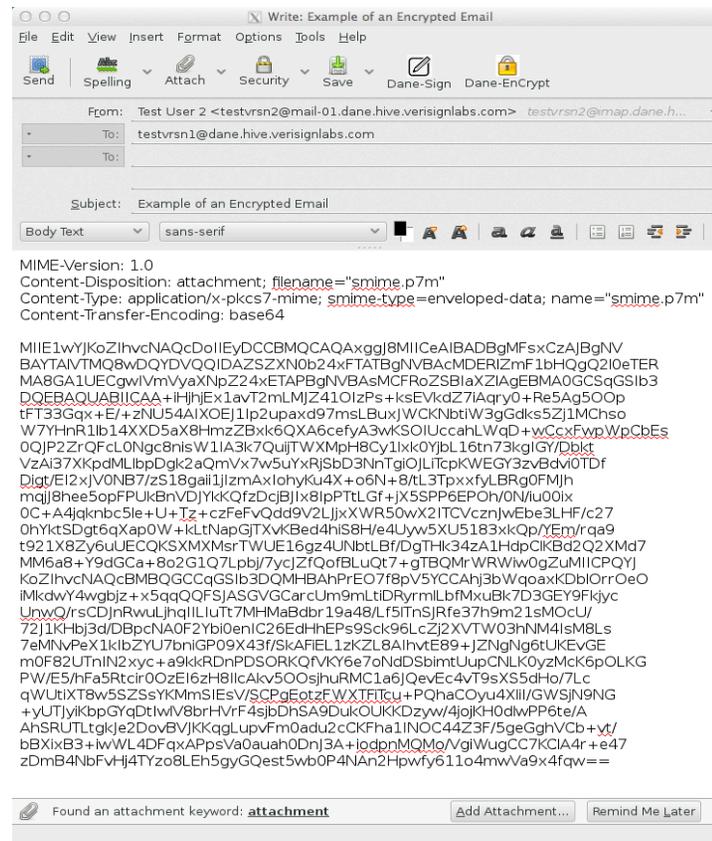
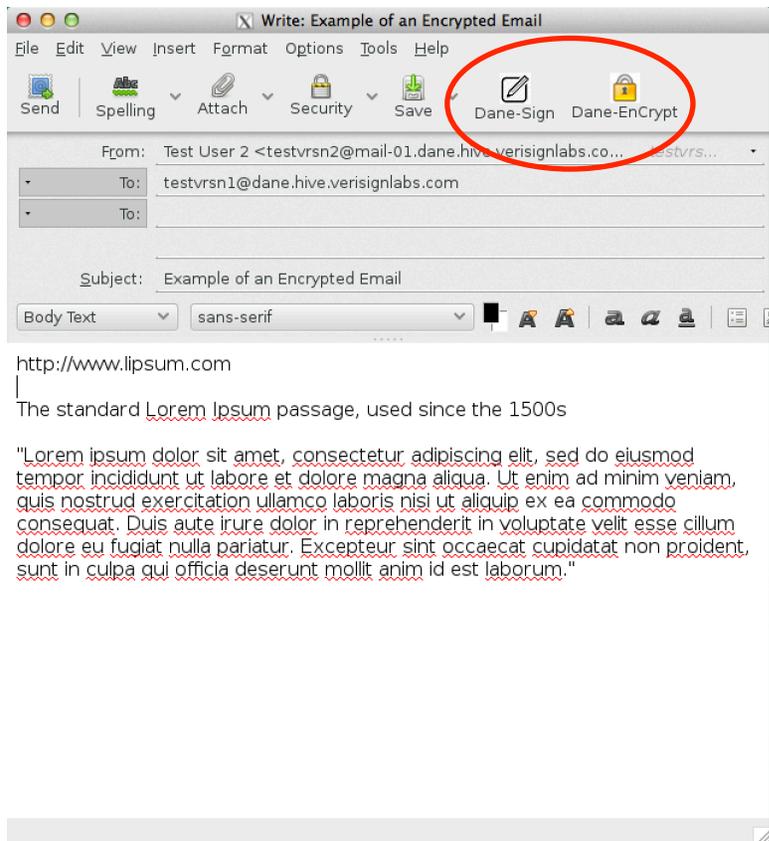
# Architectural Considerations

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

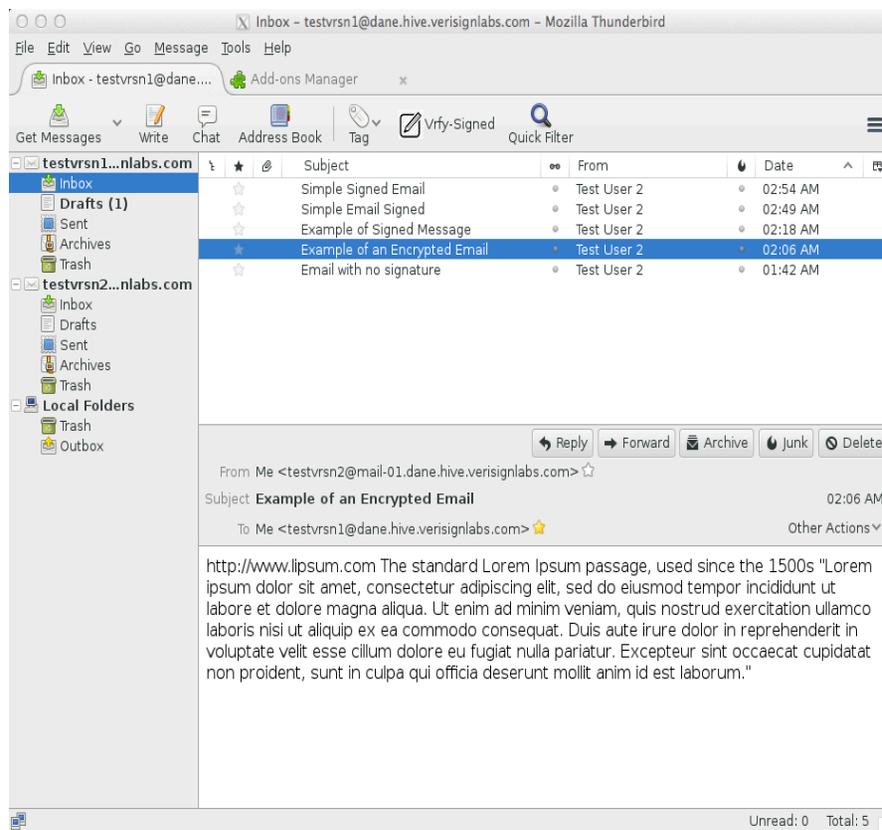


# Thunderbird Integration

# Encryption and Sending



# Encryption and Reading

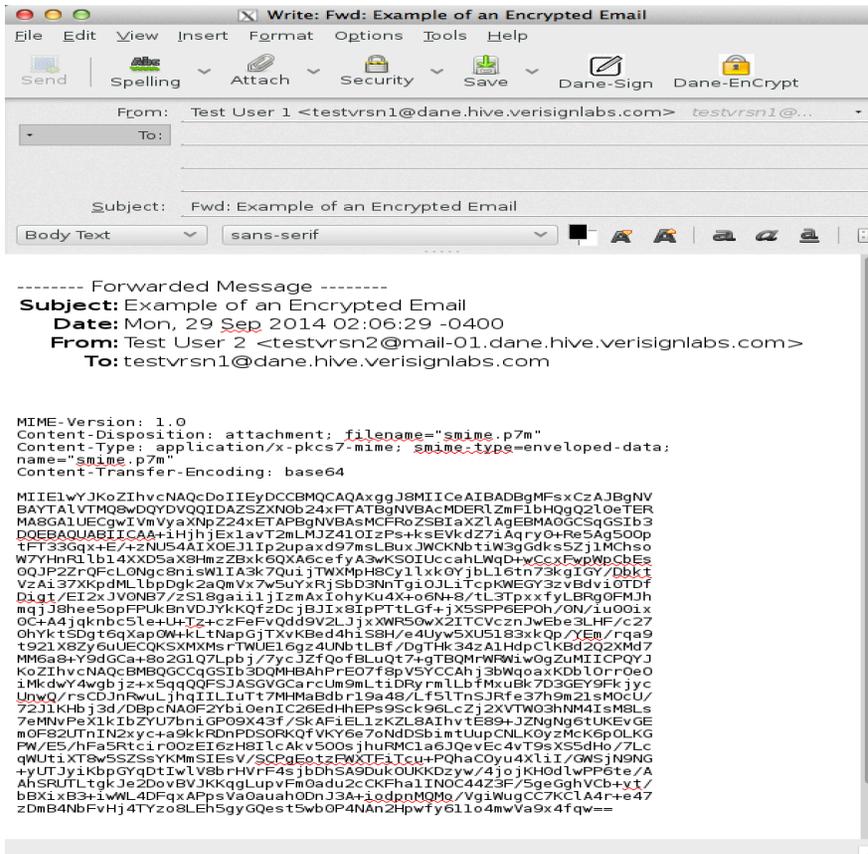


Decrypted for display pane only

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

Plugin scans email on selection

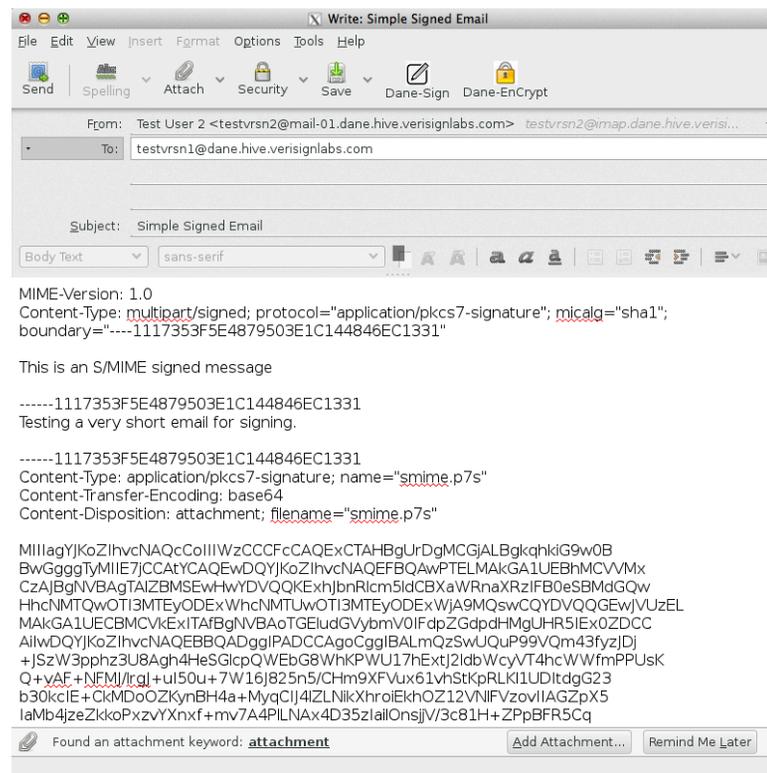
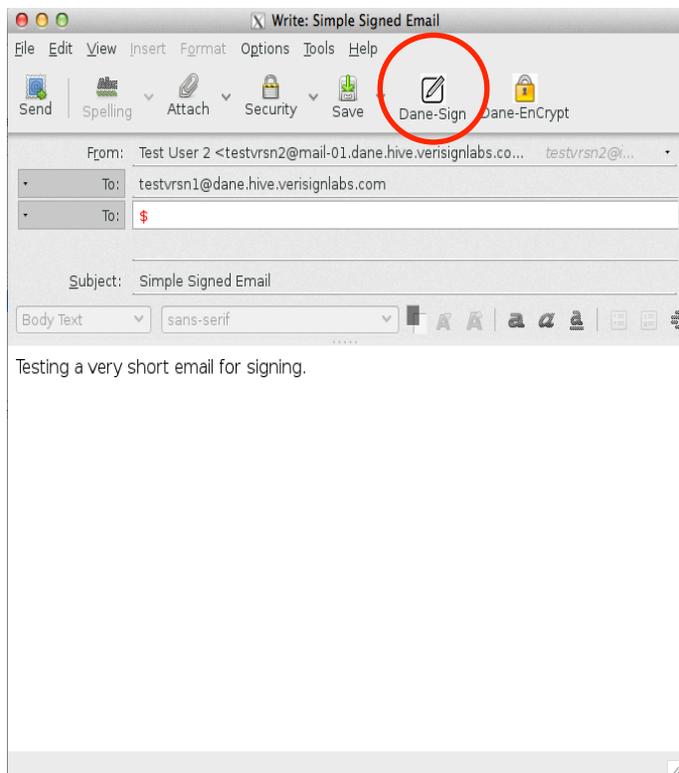
# Encryption and Reply/Forwarding



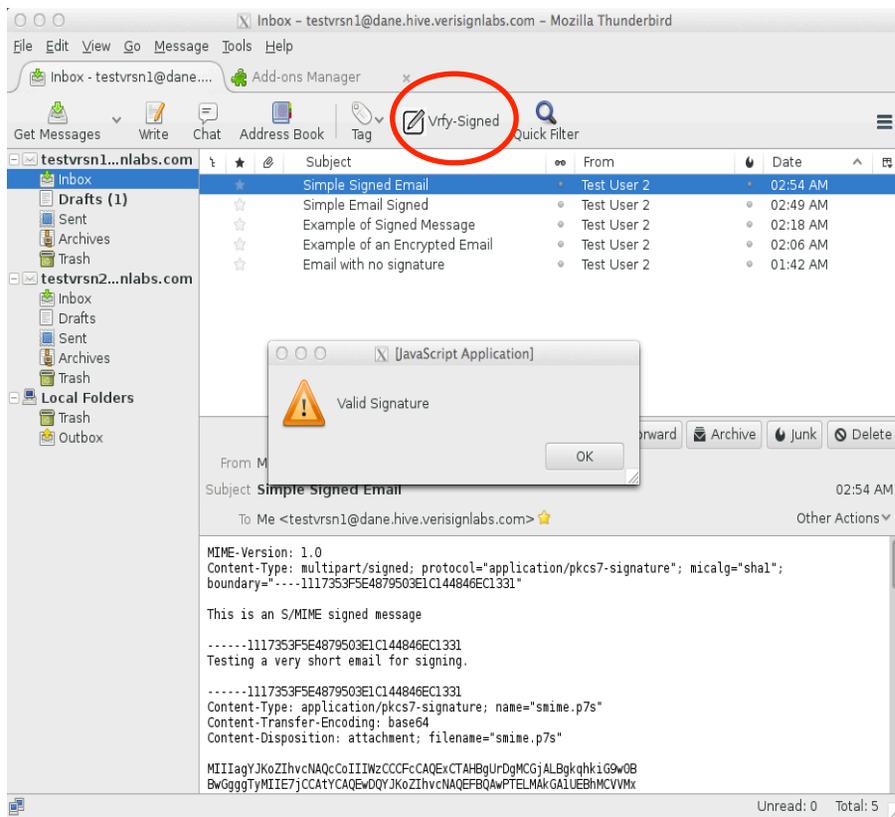
Encryption is preserved.

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

10	efed27b30a2b4c873e4dc54673a3f56d9bde40c52061f00abcd1e._encr._mimecert.dane.hive.verisignlabs.com.	86400	SMIMEA	RData: 2 0 0 4d4949466144434341314143415145774451594a4b6f5a49667 6634e151454642314177577a5c4dd16b7413154542684d 4356564d78447a414e42674e560a4241674d426c4a6c533527 6626a45564d424d4741315545427774d5247566d5958567364 434244613852354d524577447759a5651514b444168573a584 a700a6326c6e26a45524d413847413155454377749564768 6c49456870646d55774868634e45444784d6a45784d46b7aaf 5445775768634e5451784d6a457a0a44446b7aaf544577576 a3426444454c4d416b474131554542684d4356564d78447a41 4e42674e564241674d426c4a6c5335276626a45564d424d474 1 3155450a427774d5247566d5958567364434244615852354d5 24577447759445551514b444168573a5847063326c6e6626a45 524d4138474131554543777495647686c0a49456870646d557 847a413542676b71686b694739773042435145574c48526c63 33533636e4e794d5427459576c734c3441784c6d5268626d5 57561476c320a5a5335325a584a7063326c6e626d7868596e4d 75593239744d494943496a414e42676b71686b6947397730424 151454641414f43416738414d494943436741630a4167484175 4662476a736f4d6b687942742b522b706f356442644662375873 4174655a75546e554c6f41597034705448673165724e744b747 4 747563514a6a2f0a4477266366f7576526879766e6f4739799e 2b39327541636a55338a6e4346f586171456249643836385 079315268726852646132786d6a6a45554944666c0a7166216c5 935664c6175736f68526234e6c351344c68596f366f335a248 5a38506d6c573764d54716c0944c5a623376504c26754514f 6b41716a476e520a6157795a662b367362c6f77534c4f6b525a 4b56314b3176685774354d464338515454655a4252645778414 a6849724e2314d614a6b3522b4d764a6a5148890a50646872 476d524a337275686c446f15a313043504a6a79776f7246724f 75567341413376424245516a855367464e336776752438 4d43393238574748523770a656153324b6a594242c468686 13231466d696e4e65426f586a57694746384963614e465a6156 594f646d6b2b775a21676848476d6f59557646131594a20650a 447677497a78702b2623563686774774557626b73a20314 162374f99644a70544c37734f496467434879587451786756464 8707444616873548574e56490a7067746d37216646854714b 41635232754f3830342b6175463066656357337544577846526 6346d33672b53314768714885626d676e734e5359566b623144 2f0a634c7044a24b4872736596b326f616458796b53447647 6f56155376a495337394f3053616e34755575487156706573 31323206958342b75873486c71440a304838383797243737 170347144436d63474536f66376f64e25576517641267756 d367051387567675a6e4268214a36506a68314d326a7a6c6d324 667340a503861724b6724851654b2157327045624b75666b307 771654c366712b476c44321524b76b320463762b764132543 417745414154414e42676b71686b69470a39773042415155464 1414f4341674541754a446673453464356b53535664634b686f2 b2b4b506a56503244659357394b716c374707046653777 504565370a585a4a4e5668503546494251513264465558365a5 0742775846214f4537356b4f59554a4546464f5754413161 7936464f5357764173304242b696573683536720a71446269527 1526b6650726b486a4c2b4c61514161344f970616e305151477 9683384246516846544f1356e506886164a3639616e6d47 4f6675573243460a357a357446465141464b4e73505a7867504 a4431593939316532394950643939682f42437042354c2b7233 5a54584e614b704733326638633324e51656b36490a579796 466647676566c4557385a68316e50706a43786d7a6b43576f433 07035796d44844e6944786273574c4e4974525313935754564 366f6a3247a7439320a316a7833364e2f794267688073245245 5a3837356e49743436623370562b364d476c672b6a7168558 463487637a4d4a472f4a6a5a3552386c45574e6d53490a3966 4c38454b61446730716d3053444a74b6b36a67595397524b 794664316f712774715252486e56f647056425447675414839 736e636c475a786690a4150556787477676b5a25a723356 4f715245625172774879743471797a6559456c58344b34556e6 5536b7570464d54786562716a4f61493279716a695876660a39 6743396c37363657651385356c5a346563566660669463 3554b726b71715a36694565636b385a424175696f6a6854784c 2f72557455167354f514c4d0a6d454b6d59337a345a4c6b497a 4636d4f9524379304b63364316d496a397533616e34 5a334b4c79417757364c361527248325a75303478713354426 76a0a613642563862617330386661347a623644d7436c334963 3451345847527433500d4316f73545444646464646464646464 44c32632f634e675955673d0a0a <<less
----	---	-------	--------	--

# 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](mailto:jldavis@verisign.com)

Eric Osterweil, Principal Scientist, Verisign Labs  
[eosterweil@verisign.com](mailto:eosterweil@verisign.com)



**VERISIGN®**

© 2014 VeriSign, Inc. All rights reserved. VERISIGN and other trademarks, service marks, and designs are registered or unregistered trademarks of VeriSign, Inc. and its subsidiaries in the United States and in foreign countries. All other trademarks are property of their respective owners.

---