

Tools to Help DANE Adoption

Eric Osterweil, eosterweil@verisign.com

Glen Wiley, gwiley@verisign.com

Object Security via S/MIME (libsmaug)

- We've made some interesting observations, having implemented S/MIME with DANE
- The association between ID and crypto is nuanced
- Not *everything* has to be in DNS, it may just start there (ala URIs in the "Access" field)

Object Security via S/MIME (libsmaug)

- libsmaug leverages DANE for object security in applications
 - Email is just *one* use of S/MIME
- libsmaug optionally uses full featured resolver
- Implementation
 - Open source
 - C/C++
 - <https://github.com/verisign/smaug> and <https://github.com/verisign/smaug-tbird-plugin>

Thunderbird Add-on

The image shows a screenshot of the Thunderbird email client interface. The top window is the 'Add-ons Manager' for the 'Smaug 1.0.0a' add-on. Below it, the main email client window is open, displaying an inbox and a decrypted message.

Add-ons Manager - Smaug 1.0.0a

S/MIME using DANE for message encryption and authentication. This Add-on was forke... [More](#) [Preferences](#) [Disable](#) [Remove](#)

Thunderbird Main Window

Inbox

Get Messages | Write | Chat | Address Book | Tag | Quick Filter | Decrypt

Search... <⌘K>

Filter these messages... <⌘K>

Subject	From	Date
• test	• Osterweil, Eric	• 3/18/15, 6:03 PM
• test secure	• Osterweil, Eric	• 3/19/15, 7:56 AM
• Testing secure	• Osterweil, Eric	• 3/19/15, 10:14 AM
• KEEP QUIET	• Osterweil, Eric	• 3/19/15, 2:37 PM
• Sign test	• Osterweil, Eric	• 3/23/15, 3:26 PM
• slkjhsfkjh	• Osterweil, Eric	• 3/23/15, 3:58 PM
• test sign and encr	• gmadkatlinode	• 9:30 AM
• TEST sig	• Osterweil, Eric	• 10:43 AM

Smaug Decrypted message Details

From Me★ Reply Forward Archive Junk Delete

Subject **KEEP QUIET**

To Me★ 3/19/15, 2:37 PM

Date Thu, 19 Mar 2015 15:37:35 -0400

Message ID <550B257F.9070200@vantages.net>

User agent Mozilla/5.0 (Macintosh; Intel Mac OS X 10.9; rv:31.0) Gecko/20100101 Thunderbird/31.5.0

Return-Path <eosterweil@vantages.net>

THIS is SECRET

Eric

Unread: 0 Total: 37

DANE Provisioning

- Promote experimental RR types
- DANE Provisioning Portal
 - Free
 - Web UI and REST API
 - Per-RR Authorization
 - Tied to an authoritative name server
- Open invitation to leverage DANE Portal
 - Send requests to: eosterweil@verisign.com or gwiley@verisign.com
 - <https://dane-provisioning.verisignlabs.com>

Thanks

Questions and feedback to:

Eric Osterweil, eosterweil@verisign.com

Glen Wiley, gwiley@verisign.com