Demonstration: DNSSEC-S/MIME-DANE Package for Microsoft Outlook

ICANN 57 Hyderabad, DNSSEC Workshop
7 Nov 2016 slamb@xtcn.com
Background

• Slow Uptake of DNSSEC
• Need killer-app
• DANE!! SMIMEA!!
• But still slow uptake
• Windows still king
• Outlook still king
• Kaminsky 2009 shoehorn DNSSEC into Outlook
• What about via Outlook Address book?
• Bingo! LDAP to DNSSEC validating convertor
• We now have any-2-any encrypted email
DEMO HERE

(Pray)
Certificate Customer Services <secureemail@>

Your certificate is ready for collection!

COMODO

Your Comodo FREE Personal Email Certificate is now ready for collection.
Certificate Customer Services <secureemail@comodogroup.com>

Your certificate is ready for collection!

To dttest03@email.com
Directories and Address Books
You can choose a directory or address book below to change or remove it.

- E-mail
- Data Files
- RSS Feeds
- SharePoint Lists
- Internet Calendars
- Published Calendars
- Address Books

New... Change... Remove

Name: Outlook Address Book
Type: MAPI
Directories and Address Books
You can choose a directory or address book below to change or remove it.

Directory Service (LDAP) Settings
You can enter the required settings to access information in a directory service.

Server Information
Type the name of the directory server your internet service provider or system administrator has given you.

Server Name: 127.0.0.1:3900

Logon Information

This server requires me to log on

User Name:
Password:
Account Settings

Directories and Address Books
You can choose a directory or address book below to change or remove it.

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>Outlook Address Book</td>
<td>MAPI</td>
</tr>
<tr>
<td>127.0.0.1:390</td>
<td>LDAP</td>
</tr>
</tbody>
</table>
Thank you for using LVDT Version 0.13 Beta (c) DCI
```
/cygdrive/c/users/lamb/documents

lamb@DCCOM-WIN10RL ~
$ cd /cygdrive/c/users/lamb/documents

lamb@DCCOM-WIN10RL /cygdrive/c/users/lamb/documents
$ tail -f lvdt.exe.log

WinMain: Closing logfile |C:\Users\lamb\Documents\lvdt.exe.log|
Started logging to |C:\Users\lamb\Documents\lvdt.exe.log|
Friendly name: Ethernet DNS: 192.168.0.1
Friendly name: Ethernet 3
Friendly name: Loopback Pseudo-Interface 1
Friendly name: isatap.{8DBA1F2C-7563-4685-B59B-FD8C5209618D}
Friendly name: Teredo Tunneling Pseudo-Interface
Using resolver at 192.168.0.1 for validation
ldap: CreateThread() is OK! ID=5260
```
If you can read this, it worked!
dtest03 <dtest03@dnssek.info>
send encrypted email

To dtest01@dnssek.info

If you can read this, it worked!
dtest03 <dtest03@dnsske.info>
send encrypted email

If you can read this, it worked!

Message Security Properties

Subject: send encrypted email

Messages may contain encryption and digital signature layers. Each
digital signature layer may contain multiple signatures.

Security Layers
Select a layer below to view its description.

- Subject: send encrypted email
- Encryption Layer
$ dig +dnssec -t type53
b8bcd91628f45536a4776929b99867d2c4f08b390edb0aa1619fc36a._smimecert.dnssek.info. @8.8.8.8

;; DiG 9.10.3 <<< +dnssec -t type53
b8bcd91628f45536a4776929b99867d2c4f08b390edb0aa1619fc36a._smimecert.dnssek.info. @8.8.8.8
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 27335
;; flags: qr rd ra ad; QUERY: 1, ANSWER: 2, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
;; EDNS: version: 0, flags: do; udp: 512
;; QUESTION SECTION:
b8bcd91628f45536a4776929b99867d2c4f08b390edb0aa1619fc36a._smimecert.dnssek.info. IN TYPE53

;; ANSWER SECTION:
b8bcd91628f45536a4776929b99867d2c4f08b390edb0aa1619fc36a._smimecert.dnssek.info. 3599 IN TYPE53 #
1349 0300003082053E30820426A003020102021100BD123431A7487BA82E
0597A3A2727711300D06092A864886F70D0101B050030819B310B30
09060355040613024742311B30190603550408131247726561746572
...
fPghFykI3T+kx6PngMCKW18fBbI1FouRNR2kEBROZQLRtEnSxeknT7/
iYCSBH2snjv3A GV f v setNtciabELx/z1r8DXA23rDBuwuj4pblRT4U Nq
XwZ3Xq1NvpNvZVEvD5Nh3/SorOuflN/XbdSb+Er0X7e98xusOv0o2B5 65Gt1g==

;; Query time: 1287 msec
;; SERVER: 8.8.8.8#53(8.8.8.8)
;; WHEN: Fri Nov 04 04:47:45 PDT 2016
;; MSG SIZE  rcvd: 1768
Test unsigned unencrypted email
Fri 11/4/2016 4:57 AM
smimea-noreply@zx.com
Your SMIMEA status

To: dtest03@dnssek.info

We removed extra line breaks from this message.

Checking for DNSSEC on dnssek.info ... OK :-) Checking for SMIMEA Record for dtest03@dnssek.info ... Got One :-)

SMIMEA cert info:

dig -t TYPE53 08cd7fc1bc6668138e77a08fb4e018f2de954d2be10834dbf1cc9b9f._smimecert.dnssek.info.
DANE type=030000
e-mail=dtest03@dnssek.info
serial=4CB7682138E25324A0DB1B631A07B03F
subject=/emailAddress=dtest03@dnssek.info

Trying to send encrypted message to you using above.

Try sending me a SMIME signed email.
You ARE using DANE/SMIMEA to lookup my certificate :-}
If you can read this, congratulations. You have secure end-to-end email using DNSSEC.
What Happened

1. Outlook queries its address book for information on dtest01@dnssek.info including S/MIME certificate. One of the LDAP entries points to local LDAP server at 127.0.0.1 port 390.

2. LVDT.EXE is a minimal, from scratch, LDAP server listening on port 390 that converts LDAP requests into DNS lookups.

3. DNS responses from ‘Net are DNSSEC validated by LVDT.EXE and only then converted back into a LDAP response for Outlook’s Address book to use. Outlook uses returned certificate to encrypt email.
Resources

- IETF draft-ietf-dane-smime
- lvdt.dc.org
- smimea@zx.com