

# 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)**

Recycle Bin



Inbox - dtest01@dnssek.info - Outlook

FILE HOME SEND / RECEIVE FOLDER VIEW

New Email New Items Delete Reply Reply All Forward Meeting Move to: ? To Manager Team Email Reply & Delete Create New Move Rules Unread/Read Follow Up Search People Address Book Filter Email Send/Receive All Folders

Search Current Mailbox (Ctrl+E) Current Mailbox

All Unread By Date Newest

Two Weeks Ago

Certificate Customer Ser...	Your certificate is ready for colle...	10/20/2016
Microsoft Outlook	Microsoft Outlook Test Message	10/20/2016

Reply Reply All Forward

Thu 10/20/2016 11:02 PM

Certificate Customer Services <secureemail@>

Your certificate is ready for collection!

To dtest01 lamb

**COMODO**

**Your Comodo FREE Personal Email Certificate**



Recycle Bin

Atmel Studio 7.0

ownCloud

Spike.exe

Inbox - dttest03@dnssek.info - Outlook

FILE HOME SEND / RECEIVE FOLDER VIEW

New Email New Items Ignore Clean Up Delete Reply Reply All Forward Meeting Move to: ? To Manager Team Email Move Rules OneNote Unread/ Read Follow Up Search People Address Book Filter Email Send/Receive All Folders Send/Receive

Drag Your Favorite Folders Here

Junk E-mail  
Outbox  
Search Folders

dttest03@dnssek.info

**Inbox 2**  
Drafts  
Sent Items  
Deleted Items 2

Search Current Mailbox (Ctrl+E) Current Mailbox

All Unread By Date Newest

Two Weeks Ago


Certificate Customer Ser...	Your certificate is ready for colle...	10/20/2016
dttest01	RE: Test message Ack 01	10/20/2016
dttest05		

Reply Reply All Forward

Thu 10/20/2016 5:08 PM

Certificate Customer Services <secureemail@comodogrou>  
Your certificate is ready for collection!

To dttest03 lamb



send test encrypted email - Message (HTML)

FILE MESSAGE INSERT OPTIONS FORMAT TEXT REVIEW

Themes Colors Fonts Effects Page Color Bcc Show Fields Permission Encrypt Sign Use Voting Buttons Request a Delivery Receipt Request a Read Receipt Save Sent Item To Delay Delivery Direct Replies To More Options

From dttest03@dnssek.info

To dttest01@dnssek.info

Cc

Subject send test encrypted email

Can you read this?

Encryption Problems

Microsoft Outlook had problems encrypting this message because the following recipients had missing or invalid certificates, or conflicting or unsupported encryption capabilities:

dttest01@dnssek.info

Continue will encrypt and send the message but the listed recipients may not be able to read it.

Send Unencrypted Continue Cancel



Recycle Bin



Atmel Studio 7.0



ownCloud



Spike.exe



Chrome App

Recycle Bin



Atmel Studio 7.0



ownCloud



Spike.exe

Inbox - dtest03@dnssek.info - Outlook

FILE HOME SEND / RECEIVE FOLDER VIEW

New Email New Items

Ignore Clean Up Junk Delete

Drag Your Favorite Folders Here

Search Folders

dttest03@dnssek.info

**Inbox** 2

Drafts

Sent Items

Deleted Items 2

Account Settings

**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	Type
Outlook Address Book	MAPI



Recycle Bin



Inbox - dtest03@dnssek.info - Outlook

FILE HOME SEND / RECEIVE FOLDER VIEW

New Email New Items Delete

Ignore Clean Up Junk Delete

Account Settings

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

Add Account

**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: 127.0.0.1:390

**Logon Information**

This server requires me to log on

User Name:

Password:



Recycle Bin



Intel Studio 7.0



ownCloud



Spike.exe



Chrome App Launcher

Inbox - dtest03@dnssek.info - Outlook

FILE HOME SEND / RECEIVE FOLDER VIEW

New Email New Items

Ignore Clean Up Junk Delete

Drag Your Favorite Folders Here

Search Folders

dtest03@dnssek.info

**Inbox 2**

Drafts

Sent Items

Deleted Items 2

Junk E-mail

Outbox

Sync Issues (This computer only)

Search Folders

Account Settings

**Directories and Address Books**

You can choose a directory or address book below to change or remove it.

Add Account

**Directory Service (LDAP) Settings**

You can enter the required settings to access information in a directory service.

**Add E-mail Account**

**Server Info**

Type the name of the directory service administrator.

Server Name

**Logon Info**

This server requires authentication.

User Name:

Password:

**You must restart Outlook for these changes to take effect.**

OK

Recycle Bin

tmel Studio 7.0

ownCloud

Spike.exe

Inbox - mydatafiles - Outlook

FILE HOME SEND / RECEIVE FOLDER VIEW

New Email New Items

Ignore Clean Up Junk Delete

Drag Your Favorite Folders Here

mydatafiles

- Inbox
- Drafts
- Sent Items
- Deleted Items
- Junk E-mail
- Outbox
- RSS Feeds
- Search Folders

dttest02@dnssek.info

### Account Settings

#### 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	Type
Outlook Address Book	MAPI
127.0.0.1:390	LDAP



Application Tools Documents

Share View Manage


> This PC > Documents Search Documents

Name	Date modified	Type	Size
lvdt.exe.log	11/3/2016 10:20 PM	Text Document	126 KB
lvdt.exe	10/21/2016 4:37 PM	Application	277 KB
dtest04.cer	10/20/2016 5:40 PM	Security Certificate	2 KB
dtest03.cer	10/20/2016 5:12 PM	Security Certificate	2 KB
dtest02.cer	10/20/2016 5:11 PM	Security Certificate	2 KB
oldcrow.png	7/3/2016 2:08 PM	PNG File	343 KB
Picture1.png	2:03 PM	PNG File	993 KB
Notes	16 4:15 PM	File folder	
Visual Studio 2015	6 9:36 PM	File folder	
SignalHound	6 9:31 PM	File folder	
Atmel Studio	5 7:12 PM	File folder	
eFax Messenger 4.4	15 12:40 ...	File folder	
Custom Office Tem	5 1:01 PM	File folder	

LVDT

Thank you for using LVDT  
Version 0.13 Beta (c) DCI

OK

 /cygdrive/c/users/lamb/documents

lamb@DCCOM-WINI0RL ~

\$ cd /cygdrive/c/users/lamb/documents

lamb@DCCOM-WINI0RL /cygdrive/c/users/lamb/documents

\$ tail -f lvdtd.exe.log

WinMain: Closing logfile |C:\Users\lamb\Documents\lvdtd.exe.log|

Started logging to |C:\Users\lamb\Documents\lvdtd.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



The screenshot shows a Windows desktop environment with several applications open. On the left, the taskbar includes icons for Recycle Bin, Atmel Studio 7.0, ownCloud, Spike.exe, and a Start menu button. The desktop background is orange.

Three windows are visible:

- Terminal Window:** The title bar shows the path `/cygdrive/c/users/lamb/documents`. The command prompt shows the user `lamb@DCCOM-WIN10RL` and the command `$ cd /cygdrive/c/users/lamb/documents`. Below this, there are several lines of text, including `$ tail -f lvd`, `WinMain: Close`, `Started logging`, and `Using resolver`.
- File Explorer Window:** The title bar shows the path `/cygdrive/c/users/lamb/documents`. The ribbon includes tabs for FILE, HOME, SEND / RECEIVE, FOLDER, and VIEW. The ribbon contains various icons for file operations like New, Delete, Reply, Forward, and Meeting.
- Outlook Window:** The title bar shows `Inbox - dtest03@dnssek.info - Outlook`. The ribbon includes tabs for FILE, HOME, SEND / RECEIVE, FOLDER, and VIEW. The ribbon contains various icons for email actions like Reply, Forward, and Meeting. The main pane shows a list of emails with columns for All, Unread, and By Date. The selected email is from `dttest01` with the subject `RE: Test message` and the body `Ack 01`. The right pane shows the email content, which includes a message from `Certificate Customer Services` with the subject `Your certificate is ready for collection!` and a **COMODO** logo at the bottom.



Recycle Bin



Atom Studio 7.0



ownCloud



Spike.exe

```

/cygdrive/c/users/lamb/do
Tamb@DCCOM-WIN10RL ~
$ cd /cygdrive/c/users/la
Tamb@DCCOM-WIN10RL ~
$ tail -f lvd
WinMain: Close
Started logging
Friend
Friend
Friend
Friend
Friend
Using resolver
ldap: CreateTh

```

FILE

New Email

New Items

Inbox 2

Drafts

FILE MESSAGE INSERT OPTIONS FORMAT T

Themes Colors Fonts Effects

Page Color Bcc

Encrypt Sign

Use Vo Button

Themes Show Fields Permission

From dttest03@dnssek.info

To... dttest01@dnssek.info;

Cc...

Subject send encrypted email

If you can read this, it worked!



The image shows a Windows desktop environment. On the left is the taskbar with icons for Recycle Bin, Atmel Studio 7.0, ownCloud, Spike.exe, and Chrome App. The main area contains two windows:

- Terminal Window:** The title bar reads `/cygdrive/c/users/lamb/documents`. The content shows LDAP server logs:

```
LDAPServerWorkerThread: LDAP socket=704 86 bytes
SEQUENCE
INTEGER len=1 0C
CHOICE [3]
OCTET len=0 |
UNIVERSAL len=1 00
UNIVERSAL len=1 00
INTEGER len=1 00
INTEGER len=1 00
BOOLEAN FALSE
UNKNOWN PRIM len=11 6F 62 6A 65 63 74 43 6C 61 73 73
Class|
SEQUENCE
OCTET len=11 6F 62 6A 65 63 74 43 6C 61 73 73
OCTET len=20 64 65 66 61 75 6C 74 4E 61 6D 69 6E 67 43 6F 6E
|object
|objectClass|
|defaultNamin
|text|
gCon|
74 65 78 74
ldap: id=12 ver=3 appno=3 |||
ldap: Odd. received unbind request after start - DONE - close stream
Closing socket 704
Closing socket 624
ldap: mem:1024 max:17807
```
- Outlook Window:** The title bar reads `@dnssek.info - Outlook`. It shows a list of emails and a notification for a certificate. The notification text is: "Certificate Customer S", "Your certificate is ready for", and "To dtest03 lamb". Below the notification is a large red logo for "COMODO".

Recycle Bin

Dropbox  
(icann.org)

FILE HOME SEND / RECEIVE FOLDER VIEW

New Email New Items Clean Up Junk Delete Reply Reply All Forward Meeting More Quick Steps Move Rules Unread/Read Follow Up Search People Address Book Filter Email Send/Receive All Folders Send/Receive

- ▲ Favorites
  - Inbox **82861**
  - Sent Items
  - Deleted Items **238**
- ▶ Search Folders
- ▲ dtest01@dnssek.info
  - Inbox 1**
  - Drafts
  - Sent Items

Search Current Mailbox (Ctrl+E) | Current Mailbox

All Unread By Date Newest

▲ Today


dtest03	send encrypted email	5:09 PM
---------	----------------------	---------

▲ Two Weeks Ago

Certificate Customer Ser...	Your certificate is ready for colle...	10/20/2016
Microsoft Outlook	Microsoft Outlook Test Message	10/20/2016

Reply Reply All Forward

Fri 11/4/2016 5:09 PM

 dtest03 <dtest03@dnssek.info>

send encrypted email

To dtest01@dnssek.info

---

If you can read this, it worked!



Inbox - dtest01@dnssek.info - Outlook

FOLDER VIEW

Reply Reply All Forward Meeting More

Move to: ? To Manager Reply & Delete

Team Email Create New

Move Rules Unread/Read Follow Up

Search People Address Book Filter Email

Send/Receive All Folders Send/Receive

Respond Quick Steps Move Tags Find Send/Receive

Search Current Mailbox (Ctrl+E) Current Mailbox

All Unread By Date Newest

Today

dtest03 send encrypted email 5:09 PM

Two Weeks Ago

Certificate Customer Ser... Your certificate is ready for colle... 10/20/2016

Microsoft Outlook Microsoft Outlook Test Message 10/20/2016

Reply Reply All Forward

Fri 11/4/2016 5:09 PM

dtest03 <dtest03@dnssek.info>

send encrypted email

To dtest01@dnssek.info

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

```
lamb@DCCOM-WIN10RL /cygdrive/c/users/lamb/documents
```

```
$ 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
```

```
0597A3A2727711300D06092A864886F70D01010B050030819B310B30
```

```
09060355040613024742311B30190603550408131247726561746572
```

```
...
```

```
fPghFykI3T+kX6PngMCKW18fBbI1FouRNR2kEBroZQILRtEnSxeknT7/
```

```
iYCSBH2snjv3AGVfvsetNtciaBElx/z1r8DXA23rDBuwuj4pb1RT4UNq
```

```
xwZ3Xq1NVpnxVZEVDd5Nh3/SorOuf1N/Xbdsb+Er0X7e9BxusOv0o2B5 65Gt1g==
```

```
;; Query time: 1287 msec
```

```
;; SERVER: 8.8.8.8#53(8.8.8.8)
```

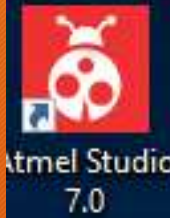
```
;; WHEN: Fri Nov 04 04:47:45 PDT 2016
```

```
;; MSG SIZE rcvd: 1768
```





Recycle Bin



Atmel Studio 7.0



ownCloud



FILE HOME

New Email New Items

Search Folders

dttest03@dnsse

**Inbox 2**

Drafts

Sent Items

Deleted Items

FILE MESSAGE INSERT OPTIONS FORMAT TEXT REVIEW

Themes Colors Fonts Effects Page Color Bcc

Encrypt Sign

Use Voting Buttons Request a Delivery Request a Read Receipt Tracking

Send

From dttest03@dnssek.info

To richard.lamb@icann.org

Cc

Subject Test encrypted email

1 2 3



Recycle Bin

Atmel Studio 7.0

ownCloud

FILE MESSAGE INSERT OPTIONS FORMAT TEXT REVIEW

Themes Colors Fonts Effects Page Color Bcc Encrypt Sign Use Voting Buttons Request Tracking

From: dtest03@dnssek.info

To: [smimea@zx.com](mailto:smimea@zx.com);

Cc:

Subject: Test unsigne unencrypted email

Inbox 2

Drafts

Sent Items

Deleted Items 2

The screenshot shows a Windows desktop with a taskbar on the left containing icons for Recycle Bin, Atmel Studio 7.0, ownCloud, Spike.exe, and Chrome App Launcher. The main window is an email client displaying an email titled "Your SMIMEA status - Message (Plain Text)". The email is from "smimea-noreply@zx.com" and is addressed to "dtest03@dnssek.info". The email content includes a status report on DNSSEC and SMIMEA records, technical details of a certificate, and a request for a SMIME signed email.

**FILE MESSAGE**

Ignore Delete Reply Reply All Forward Meeting More

Move to: ? To Manager Team Email Quick Steps

Rules OneNote Actions Move Mark Unread Follow Up Tags

Fri 11/4/2016 4:57 AM  
smimea-noreply@zx.com  
Your SMIMEA status

To: dtest03@dnssek.info

**i** We removed extra line breaks from this message.

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

SMIMEA cert info:  
dig -t TYPE53 08cd7fc1bc6868138e77a08fb4e018f2de954d2be10834dbf1cc9b9f.\_smimecert.dnssek.info.  
DANE type=030000  
[email=dtest03@dnssek.info](mailto:dtest03@dnssek.info)  
serial=4CB7682138E25324A0DB1B631A07B03F  
subject= [/emailAddress=dtest03@dnssek.info](mailto:dtest03@dnssek.info)  
SHA1 Fingerprint=0D:92:B3:13:EA:3C:02:F5:53:F3:23:15:B2:E9:B4:D8:26:2F:9D:60

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 :-)



- Recycle Bin
- tmel Studio 7.0
- ownCloud
- Spike.exe

Inbox - dttest03@dnssek.info - Outlook

FILE HOME SEND / RECEIVE FOLDER VIEW

New Email New Items Delete Reply Reply All Forward Meeting More Quick Steps Move Unread/Read Follow Up Search People Address Book Filter Email Send/Receive All Folders Send/Receive

Search Current Mailbox (Ctrl+E) | Current Mailbox

All Unread By Date Newest

Today

smimea-noreply@zx.com	Encrypted message	4:57 AM
smimea-noreply@zx.com	Your SMIMEA status Checking for DNSSEC on	4:57 AM

Two Weeks Ago

Certificate Customer Ser...  
Your certificate is ready for colle... 10/20/2016

Reply Reply All Forward

Fri 11/4/2016 4:57 AM  
smimea-noreply@zx.com  
Encrypted message

To dttest03@dnssek.info

If you can read this, congradulations. You have secure end-2-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](http://lvdt.dc.org)
- [smimea@zx.com](mailto:smimea@zx.com)