DNSSEC Enables Secure Mail

Jaap Akkerhuis (proxying)
Secure Mail Project

- The Players
  - Fraunhofer IAO
  - ISC
  - Microsoft
  - NCCCE
  - NIST
  - NLnet Labs
  - Secure64
The (Open Standard) Parts

- SMIME
- TLS
- DNSSEC
- CERTS
  - Self signed
  - Well Known Certs
  - Private Certs

} Dane
The MUA Parts

- Microsoft Office
- Thunderbird
- Also with Apple Key Chain Utility
The MTA Parts

• Postfix
• Dovecot
• Exchange
The DNS Parts (I)

- ISC
- BIND
- Microsoft
- Active Directory and DNS Server
The DNS Parts (2)

- NLnet Labs
  - nsd4, Unbound, OpenDNSSEC
- Secure64
  - DNS Signer, DNS Cache, DNS Manager, Apple Keychain Utility
The Product

• NIST Publication: Practice Guide SP 1800-6

• A HowTo

• Tested example configurations

• There will be a Public Comment Period

• Breaking news: Report published

• https://nccoe.nist.gov/projects/building_blocks/secured_email
Environment

DNS-Based Email Security Test Set-up
Main Scenarios

- Transport security
- TLSA DNSSEC
- End-to-End Security
- S/MIME Signed mail
- Encrypted
## Well defined tests

<table>
<thead>
<tr>
<th>Sequence</th>
<th>NCCoE Lab</th>
<th>Legitimate Remote Site</th>
<th>Certificate on Receiver Side</th>
<th>Legitimate Remote Site</th>
<th>Certificate on Receiver Side</th>
</tr>
</thead>
<tbody>
<tr>
<td>Event</td>
<td>MUA</td>
<td>MTA</td>
<td>DNS Service</td>
<td>Secure 64</td>
<td></td>
</tr>
<tr>
<td>13</td>
<td>Outlook</td>
<td>Exchange</td>
<td>Active Directory</td>
<td>Thunderbird on MacBook, Postfix/ Dovecot, DNS Authority/ Cache/ Signer issued (CU=2)</td>
<td>Local CA (CU=1)</td>
</tr>
<tr>
<td>14</td>
<td>Thunderbird</td>
<td>Postfix/ Dovecot</td>
<td>NSD4/ Unbound/ OpenDNSSEC</td>
<td>Same as 13</td>
<td>Local CA issued (CU=1)</td>
</tr>
<tr>
<td>15</td>
<td>Thunderbird on MacBook</td>
<td>Postfix/ Dovecot</td>
<td>DNS Authority/ Cache/Signer</td>
<td>Same as 13</td>
<td>Local CA issued (CU=1)</td>
</tr>
<tr>
<td>16</td>
<td>Outlook</td>
<td>Exchange</td>
<td>Active Directory</td>
<td>Same as 13</td>
<td>Self-Signed Cert (CU=3)</td>
</tr>
<tr>
<td>17</td>
<td>Thunderbird</td>
<td>Postfix/ Dovecot</td>
<td>NSD4/ Unbound/ Open DNSSEC</td>
<td>Same as 13</td>
<td>Self-Signed Cert (CU=3)</td>
</tr>
<tr>
<td>18</td>
<td>Thunderbird</td>
<td>Postfix/ Dovecot</td>
<td>BIND</td>
<td>Same as 13</td>
<td>Self-Signed Cert (CU=3)</td>
</tr>
</tbody>
</table>
Results

- No surprises here
- Tests met expectations
- Analyses of tampering attempts from logfiles
Role of DNSSEC

• Enables verification of trust in the applications
Questions