DNSSEC Encryption Algorithm Agility

ICANN 56 DNSSEC Workshop
June 27, 2016
Helsinki, Finland

Dan York, Internet Society
DNSSEC Algorithms

• Used to generate keys for signing
  • DNSKEY

• Used in DNSSEC signatures
  • RRSIG

• Used for DS record for chain of trust
  • DS

• Used in validation of DNSSEC records
IANA Registry of DNSSEC Algorithm Numbers

<table>
<thead>
<tr>
<th>Number</th>
<th>Description</th>
<th>Mnemonic</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>Reserved</td>
<td></td>
</tr>
<tr>
<td>1</td>
<td>RSA/MD5 (deprecated)</td>
<td>RSAMD5</td>
</tr>
<tr>
<td>2</td>
<td>Diffie-Hellman</td>
<td>DH</td>
</tr>
<tr>
<td>3</td>
<td>DSA/SHA1</td>
<td>DSA</td>
</tr>
<tr>
<td>4</td>
<td>Reserved</td>
<td></td>
</tr>
<tr>
<td>5</td>
<td>RSA/SHA-1</td>
<td>RSASHA1</td>
</tr>
<tr>
<td>6</td>
<td>DSA-NSEC3-SHA1</td>
<td>DSA-NSEC3-SHA1</td>
</tr>
<tr>
<td>7</td>
<td>RSASHA1-NSEC3-SHA1</td>
<td>RSASHA1-NSEC3-SHA1</td>
</tr>
<tr>
<td>8</td>
<td>RSA/SHA-256</td>
<td>RSASHA256</td>
</tr>
<tr>
<td>9</td>
<td>Reserved</td>
<td></td>
</tr>
<tr>
<td>10</td>
<td>RSA/SHA-512</td>
<td>RSASHA512</td>
</tr>
<tr>
<td>11</td>
<td>Reserved</td>
<td></td>
</tr>
<tr>
<td>12</td>
<td>GOST R 34.10-2001</td>
<td>ECC-GOST</td>
</tr>
<tr>
<td>13</td>
<td>ECDSA Curve P-256 wSHA-256</td>
<td>ECDSAP256SHA256</td>
</tr>
<tr>
<td>14</td>
<td>ECDSA Curve P-384 wSHA-384</td>
<td>ECDSAP384SHA384</td>
</tr>
<tr>
<td>15-122</td>
<td>Unassigned</td>
<td></td>
</tr>
<tr>
<td>123-251</td>
<td>Reserved</td>
<td></td>
</tr>
<tr>
<td>252</td>
<td>Reserved for Indirect Keys</td>
<td>INDIRECT</td>
</tr>
<tr>
<td>253</td>
<td>private algorithm</td>
<td>PRIVATEDNS</td>
</tr>
<tr>
<td>254</td>
<td>private algorithm OID</td>
<td>PRIVATEOID</td>
</tr>
<tr>
<td>255</td>
<td>Reserved</td>
<td></td>
</tr>
</tbody>
</table>
Elliptic Curve DNSSEC Algorithms

- ECDSA – RFC 6605 – April 2012

Under development:

- Ed25519:
  - draft-ietf-curdle-dnskey-ed25519

- Ed448
  - draft-sury-dnskey-ed448

(See “New Curves in DNSSEC” from ICANN 55)
Why Do We Care About Newer Algorithms?

- **Faster!**
  - Signing
  - Validation

- **Smaller keys and signatures**
  - Packet size (and avoiding fragmentation)
  - Minimizing potential reflection/DDoS attacks

- **Better cryptography**
  - Move away from 1024-bit RSA
Aspects of Deploying New Algorithms

• Validation
• Signing / DNS Hosting Operators
• Registries
• Registrars
• Developers

(See ICANN 55 Marrakech DNSSEC Workshop archives for more information.)
Discussions To Date

• Mar 2016 - ICANN 55 DNSSEC Workshop, Marrakech
• Apr 2016 – DNS-OARC Workshop, Buenos Aires
• Apr 2016 – IETF 95, Buenos Aires – Discussion in CURDLE and DNSOP working groups
• May 2016 – RIPE 72 session, Copenhagen
• Jun 2016 – ICANN 56 DNSSEC Workshop, Helsinki

• Internet-Draft
  • draft-york-dnsop-deploying-dnssec-crypto-algs
What Have We Learned?

• A conversation with Ondřej Surý
Next Steps

• Help people understand value and need to support new algorithms

• Document these steps in a form that can be distributed (ex. Internet-draft)

• ?

• Need to start NOW as it will take several years to deploy...
Thank You!