Transitioning Verisign's TLDs to Elliptic Curve DNSSEC

Duane Wessels

COM/NET Uptime

(2014 Verision, Inc. Al Rights Reserved

182,170 182,653

162,748

162,748 162,541

140,040 130,778

DNS-OARC 41, September 6, 2023



Growth in COM/NET Signed Domain Names

Domain Names with DS Records





Growth in COM/NET Signed Domain Names

Domain Names with DS Records





Growth in COM/NET Signed Domain Names

- About 0.1% per year growth^{*} 2012—2020
- About 1.1% per year growth^{*} 2020—present
- We anticipate continued growth in the number of signed second-level domains

*growth based on total domains



Benefits of ECDSA

- Smaller signature sizes
 - 64 bytes for ECDSA vs 160 bytes for 1280-bit RSA
 - Benefits both message size and memory usage
- Improved cryptographic strength
 - ECDSA Curve P-256 is generally considered equivalent to 3072bit RSA



Changing DNSSEC Algorithms

- Currently RSA/SHA-256 (8):
 - 2048-bit KSK
 - 1280-bit ZSK
- Rolling to ECDSA Curve P-256 with SHA-256 (13) with conservative, double-signature approach:
 - add algorithm 13 ZSK signatures along side algorithm 8 signatures (25% per day)
 - 2. add algorithm 13 DNSKEY records
 - add algorithm 13 DS record; remove algorithm 8 DS record
 - 4. remove algorithm 8 DNSKEY records
 - 5. remove algorithm 8 ZSK signatures (25% per day)



Schedule

| Zone | Start | Rollover | End |
|------|--------|--------------|---------|
| EDU | Sept 6 | Sept 12-15 | Sept 22 |
| NET | Oct 25 | Oct 31-Nov 3 | Nov 10 |
| COM | Nov 29 | Dec 5-8 | Dec 15 |

- Start: Algorithm 13 signatures first published
- Rollover: Root zone publishes DS record for algorithm 13
- End: Algorithm 8 signatures no longer published
- Note: dates are subject to change
- Schedule for remaining TLDs still to be determined





VERISIGN[®]

© 2023 VeriSign, Inc. All rights reserved. VERISIGN and other trademarks, service marks, and designs are registered or unregistered trademarks of VeriSign, Inc. and its subsidiaries in the United States and in foreign countries. All other trademarks are property of their respective owners.