XX December 2019

To: pqc-comments@nist.gov, pqc-forum@list.nist.gov

Subject: SAC10X: SSAC Comment to NIST on Quantum Cryptography Algorithms

The Internet Corporation for Assigned Names and Numbers (ICANN) Security and Stability Advisory Committee (SSAC) submits the following comments in response to the National Institute of Standards (NIST) request for feedback on its post-quantum cryptography second-round candidate algorithms.[1]

Our comments concern the role that new cryptographic algorithms would have in the implementation of DNSSEC. In general, implementing quantum-resistant cryptography in DNSSEC should be straightforward. However, an issue that we foresee, given that there are some architectural size limits in the DNS, is that some of the candidate algorithms may not be supportable in the DNS.

The Internet's Domain Name System (DNS) is fundamentally a hierarchy of named records. Server operators can sign the records using DNSSEC, and clients can verify the signatures. The hierarchy is divided into subtrees known as zones, with links from each zone to the next.

For example, for the name WWW.EXAMPLE.COM, a resolver would first look up the name in the root zone, which returns NS records pointing at the authoritative servers for the COM zone. A second lookup to one of those servers returns NS records pointing at the servers for the EXAMPLE.COM zone, and a third lookup returns the data for WWW.EXAMPLE.COM.

Each zone is typically signed with a single key, although there may be multiple keys during key rotation. Also, it is common to have a longer key known as a key signing key (KSK) that signs the key known as the zone signing key (ZSK), and the KSK can also be rotated. All of a zone's keys are stored in DNSKEY records at the apex of the zone. In a signed zone, there are also RRSIG records that contain the signatures of the records for each name with timestamps indicating how long the signatures are valid.

For example, below are text versions of the DNSKEY records and corresponding RRSIG records for Comcast's DNS zone, with a 2K[2] RSA key signing key, a 1K RSA zone signing key, and two

[1] See https://csrc.nist.gov/Projects/post-quantum-cryptography/round-2-submissions
[2] 2K in this context refers to 2 kilobits, or 2048 bits of data.

RRSIGs, one using the ZSK and one using the KSK. The actual DNS records use a binary format. The long strings below are base64 text encodings of the actual binary keys and signatures.

```
comcast.net.   3570 IN   DNSKEY    257 3 5
AwEAAcdTwXuKIERUoEaOHCEafPCgHW8Dq8OftDPD1sZCwCUH7VjfSXQpgvkYUG+6
FN9INP2uHybzRe/m4EG8HD8zkKtaIBzrYZIcbchuXKZ5biwkj1hIMTGlDG0jD0j3
rjiJkk3dDkygKvV8FswEJo9X7+CWbtf4WKgXqnd/2JcsliDK4XujFsw27eWpXlHZ
t5SuQb0N1jmMazESXwYJYtGXce5vi4pBhlE9OUgCQlkxPxedvaelT5hKxYP3lIH4
vjBrKMzQE7OzoB4lOsJVhbvDF1VZUzC6n42w8WWvjBDY3TilOvsC9Je7DOD3yQlg
cmiQ80PM4zknfQJ76APxYrrowTE= ;{id = 40909 (ksk), size = 2048b}

comcast.net.   3570 IN   DNSKEY    256 3 5
AwEAAbEO9O0+NybzFSgdaG+ExZkMKYpZc9w5VdEJ9vUABIjFftKjd/l8Mo53OIrU
7XC81WTsSI8RQqaQqccbWDoP3afbdLR0xJw6auIEsDo6kJ7ZaSoFCAeSlMTPvdHA
lcFbHL1zF4/HzaaoOL3psKfeMe2/2j7saEOKQlxIPa5R5mgx ;{id = 26550
(zsk), size = 1024b}

comcast.net.   3570 IN   RRSIG     DNSKEY 5 2 3600
20200303144152 20191104104152 40909 comcast.net.
KtujJLry+kzibzToXFED8KpVr9dw+NC8RwlaZ+dDUHuqsVu7NGmyAjC4wtzNBwbp
FdAE56+ohEoEprgImcRS3Ok5FQxnBeGGQzWyxCO15XkEQgEnxzXnNDfrw1MMpynq
EmFiIPdXSWeVaZgzlfQAGK8WS3BWhAosqv1b7Ne3ytZS6e7MrhnbpCnFlt2DZnzL
OMPohtuXgRelrmhKx/5ixdWuLjDFPHBCZRcM4mkLWHPln/AD+C5vWagI3R4M3tUa
POM4k9txLmlKnV8Z7AwCB+LkOQh/nfE9TOnYbsczthGxY19mddnk+2tZCKJusfO4
0MzAcjqeI94jX0/9KekuuA==

comcast.net.   3570 IN   RRSIG     DNSKEY 5 2 3600
20191118174152 20191111143652 26550 comcast.net.
MJBTBBgFSvmKGNBb8n4mWjsDZUayK1dTZcLF7qkqTXuVNp6+xi2WQSr0rm3bsncx
pkEmz3rvokAceVbrcmxE9tN2Ca3fx5iw1Q87EdgsFPrvga9YrdUop5PuGdJttESv
FldjLnnYqPl/rB2C1ckJJUjONXy5bqdBJpZffzyitW8=
```

The DNSKEY records are fetched and cached the first time a resolver asks for records in a zone. The RRSIG records are returned with every answer for any query from a signed zone.

In general, implementing quantum-resistant cryptography in DNSSEC should be straightforward. The key and signature records have fields that signal what signing algorithm is in use, and new algorithms are added over time. The problem is that there are some architectural size limits in the DNS. A DNS message with a total length up to about 4K bytes can be sent using the UDP transport protocol, while larger messages can use TCP at some loss in efficiency. There is an absolute architectural limit of 64K on a TCP DNS packet, which includes all of the records and some protocol overhead. With 1K and 2K RSA keys and signatures, the DNS packet is usually under 2K bytes , and even with multiple keys and signatures during key rotation it’s typically under 4K. Existing DNSSEC algorithms can handle keys up to 4K bits which would roughly

double the packet size, and it would be straightforward to go to an 8K or 10K bit key, which might bring the packet size to 16K.

The SSAC is concerned that some of the candidate algorithms have very large keys, 10K to 200K or more, or very large signatures, exceeding 20K bits. With very large keys DNSSEC wouldn't work reliably, since some combinations of multiple KSKs and ZSKs and associated signatures wouldn't fit in a 64K packet. Large signatures wouldn't pose a correctness problem, but would be a performance problem since they would increase the size of every DNS response message. Zones are typically signed once and then signatures verified on every response, so signing performance is less of an issue than validation performance.

The SSAC thanks you for the opportunity to comment on proposed quantum cryptography algorithms, and ask that you take these issues involving encryption and the DNS into account in your evaluations.

Thank you,

Rod Rasmussen
Chair, ICANN Security and Stability Advisory Committee

About the SSAC: The Security and Stability Advisory Committee advises the ICANN community and Board on matters relating to the security and integrity of the Internet's naming and address allocation systems. This includes operational matters (e.g., matters pertaining to the correct and reliable operation of the root name system), administrative matters (e.g., matters pertaining to address allocation and Internet number assignment), and registration matters (e.g., matters pertaining to registry and registrar services such as WHOIS). SSAC engages in ongoing threat assessment and risk analysis of the Internet naming and address allocation services to assess where the principal threats to stability and security lie, and advises the ICANN community accordingly.