From: Dang, Quynh H. (Fed)
To: Smith-Tone, Daniel C. (Fed); (b) (6)
Subject: Re: Rainbow
Date: Sunday, June 7, 2020 9:12:38 AM

So, 39.25 smallest GeMSS128's public keys are smaller than 2^24 - 1 bytes.

For 5-cert chain, the worst case we'll have:

1) 5 certs in the chain: 5 public keys plus 5 sigs.

2) 5 STCs: 5 sigs.

3) 5 OCSP messages for the 5 certs in the chain (in #1): in the worst case: 5 sigs + 5 more certs (5 public key and 5 sigs).

4) The latter 5 certs (in #3) could have their own STCs: 5 sigs (I don't know this, I don't have data on this).

So, 10 public keys + (5 + 5 + 5 + 5 + 5 = 25) sigs and other info data which should be very small comparing to the public key.

If changing 5 to 8, we'll have 8x2 public keys + 8x5 (40) sigs.

Quynh.

From: Dang, Quynh H. (Fed) <quynh.dang@nist.gov>
Sent: Sunday, June 7, 2020 8:48 AM
To: Smith-Tone, Daniel C. (Fed) <daniel.smith@nist.gov>; Daniel Smith (b) (6)
Subject: Re: Rainbow

A cert contains a public key, a signature and some other info data (usually small size).

Quynh.

From: Dang, Quynh H. (Fed) <quynh.dang@nist.gov>
Sent: Saturday, June 6, 2020 1:31 PM
To: Smith-Tone, Daniel C. (Fed) <daniel.smith@nist.gov>; Daniel Smith (b) (6)
Subject: Re: Rainbow

Hi Daniel,

Yes, the maximum size of a certificate message is 2^24 -1 bytes.

A certificate message usually has 2 to 5 sets I think (assuming 5 is a pretty safe bet: I don't have any survey data on this). Each set contains a certificate and situationally contains 2 more signatures and 1 more certificate and some other extensions (not large data elements).

To be more sure, let's assume the max number in practice is 8 sets.

Page 65 of RFC 8446 (Section 4.4.2) even says " For maximum compatibility, all implementations SHOULD be prepared to handle potentially extraneous certificates... ."

Quynh.

From: Smith-Tone, Daniel C. (Fed) <daniel.smith@nist.gov>
Sent: Friday, June 5, 2020 4:14 PM
To: Dang, Quynh H. (Fed) <quynh.dang@nist.gov>
Subject: Rainbow

Hi, Quynh,

I recall in your part of the Rainbow presentation stating that the failure of Rainbow in the TLS experiments reported by Angela to us was due to the implementation TLS and not the specification of TLS. Do I have this correct? Right now in the Round 2 report we have a note in the Rainbow section stating that the Rainbow keys exceed the maximum message length for TLS. I want to make sure that this is an accurate statement. Do you agree with what is written there or do you think that it should be rephrased?

Cheers,
Daniel