ndn-cxx - Feature #3816

KeyRollover for high-rate data

10/17/2016 01:14 PM - Peter Gusev

Status:	New	**Start date:**	10/17/2016
Priority:	Normal	**Due date:**	
Assignee:		**% Done:**	0%
Category:	Security	**Estimated time:**	0.00 hour
Target version:			

Description

Need a mechanism for keyrollover for high-rate data (50fps and up) where producer can let consumers fetch newly generated certificate before this certificate is used to sign the
data.

Why it's needed: If producer will change certificate on-the-fly, consumer will trigger fetching new certificate for real-time data signed by this certificate, which is time-sensitive and certificate may not arrive in time for consumer to verify received packets. Thus, consumer should fetch new certificate prior to it being used by the publisher.

Original e-mail by peter@remap.ucla.edu:

> We talked with Zhehao today about key rollover and he mentioned that there was a proposal from Yingdi. However, I couldn't find it. Does anyone know where to find it?
> Any links on the materials covering the issue would be appreciated as well.
>
> Currently, in ndncon I didn't plan for writing any special roll-over mechanism/module and wanted to keep things simple (maybe not in a very elegant way - that's what triggered our discussion about rollover with Zhehao today).
>
> My idea right now is to have ndncon producer to generate new instance certificate every hour. This certificate is installed in the instance keychain, but is not set as a default certificate yet. Media stream packets are always signed with the default certificate. Once new certificate is generated, it is used for signing low-rate data generated by the discovery library. That way, consumers will be able to receive discovery data signed with the new certificate, fetch it according to the certificate chain, verify and have it cached locally. After some delay (60 seconds for instance) producer sets newly generated certificate as a default for the instance keychain and media data packets now will get signed with the new certificate. This won't trigger fetching certificate on consumer sides as they already have this certificate fetched when they received discovery data earlier. That way, verification won't trigger delays for the time-sensistive media streaming data.
>
> I'm reaching out for your thoughts on this approach. How does this conflict with the key roll-over concept and whether we should to proceed with this approach (for now/for good)?

History

#1 - 10/20/2016 01:15 PM - Peter Gusev

In order to proceed with development and based on Lixia's reply, I'll implement proposed algorithm for triggering key rollover using low-rate data.

> Alex, Yingdi, Zhiyi and I just had a discussion about your email tonight.
> 1/ Yingdi cannot recall he ever made any key rollover proposal. I copied Zhehao here, if he can help recall something.
> 2/ your proposed idea below looks fine to us, so yes please proceed.

#2 - 07/07/2017 12:36 AM - Junxiao Shi

- Category set to Security