ndn-cxx - Task #1204

Redesign of signing process / Per-instance signing keys

01/31/2014 11:15 PM - Alex Afanasyev

Status:	New	**Start date:**	
Priority:	Low	**Due date:**	
Assignee:		**% Done:**	0%
Category:	Security	**Estimated time:**	0.00 hour
Target version:			

Description

Signing process should not directly use TPM-based signing in KeyChain to sign all Data and Interests. Instead, there should be an API to generate a key pair and a (properly signed) certificate for the running instance of the application.

This task also includes figuring out the way to store/exchange the per-instance certificate. For example, should it be published or be available only during application instance active time?

History

#1 - 04/17/2014 11:23 PM - Junxiao Shi

- Description updated

Certificates must be published. Otherwise, Data cannot be verified once the certificate is gone.

Publishing per-instance certificates is expensive, especially for short-lived producers.
If ndn-tlv-poke is called once per minutes, it's 1440 certificates per day.

Per-instance signing are suitable for a few apps that (1) are long-lived producers (2) Data are not useful beyond producer lifetime.
It should not be the default signing method in the library.

#2 - 05/12/2014 06:46 PM - Alex Afanasyev

For applications such as ndn-tlv-ping (real-time-like apps when data is not longer useful after application stops), publishing can be accomplished with the result of task #1480

For other types of Data, I agree that we need to define a way (and where) to publish certificates.

#3 - 06/30/2014 12:16 AM - Junxiao Shi

- Category set to Security

#4 - 11/18/2014 09:59 PM - Junxiao Shi

One solution to the certificate publishing problem is #1529.

However, as pointed out in note-1, this is unsuitable for short-lived producers.