NDN Certificate Management with NDNCERT

Zhiyi Zhang (UCLA)
NDN Certificate

◊ An NDN Data packet
◊ Content := public key bits
◊ Signed by the cert issuer

• Certificate helps others to cryptographically identify you and your data
• Certificate proves the ownership of an NDN namespace

Manually configure certificate is error prone and of low efficiency. An ease-of-use and automatic certificate management system is required.
Certificate Issuer and Requester

- An NDN entity can be a cert requester and a cert issuer at the same time
NDNCERT

◊ NDNCERT command line tools
  o Client
  o Server Daemon

◊ NDNCERT Library for applications to become a cert issuer/requester
  o Client APIs
  o Server APIs
NDNCERT Protocol

Certificate Requester

Start a management process

Certificate Issuer

_NEW

_OR

_RENEW

_OR

_REVOKE

Collect available challenges
NDNCERT Protocol

Select a challenge

_SELECT

Prepare the challenge

_VALIDATE

Check the challenge progress

zero or more round trips to finish the challenge
NDNCERT Protocol

Requester can send _STATUS to check issue status

_DOWNLOAD
Intra-node Certificate Management

Make sure request came from the right application instance

- App was developed by the trusted developer and the code could has not been tampered with
- App instance is run by trusted user

1. Are you running this app and sending this request? (app should show PIN: 1234)
2. Check the instance (check whether 1234)
3. Check application signature
1. Get the identifier of requester app
2. Get the requester application info
NDN Forwarding Daemon
NDNCERT Server
/ucla/alice/CA
Alice
application instance
Operating System
NDN Forwarding Daemon
Example 01: Try NDNCERT Client Command Line Tool

You can use obtain an NDN certificate issued by NDN Testbed UCLA site via NDNCERT command line tool

Prerequisites

♢ Your NFD is running

♢ A route from your NFD to NDN Testbed has been established

♢ The trust anchor has been downloaded:

```bash
curl -o /usr/local/etc/ndncert/client.conf https://zhiyi-zhang.com/ucla-client.txt
```

More Details: https://github.com/named-data/ndncert/wiki/NDNCERT-Instructions
Example 01: Try NDNCERT Client Command Line Tool

Index: 0
CA prefix:/ndn/edu/ucla/CA
Introduction: UCLA Certificate Authority of NDN Testbed

Step 0: Please type in the CA namespace index that you want to apply
0
Step 1: Please type in the identity name
test
Step 2: Please select one challenge from following types
  PIN
  Email
  PIN
Step 3: Please satisfy following instruction(s)
  Please input your verification code:
  153481
DONE! Certificate has already been issued
Step 4 DONE! Certificate has already been installed to local keychain
Example 02: Try NDNCERT Server Command Line Tool

Prerequisites

♢ Your NFD is running
♢ Your requesters have routes towards your server NFD
♢ Your certificate is ready

Steps

♢ Prepare the NDNCERT CA configuration file and the anchor certificate
♢ Run ndncert-ca-server

More details: https://github.com/named-data/ndncert/wiki/NDNCERT-CA-Instructions
Live Demo

◊ Get a NDN testbed certificate now
  o if Junxiao Shi (NIST) hasn’t crashed my server yet
A certificate is not the end

◊ Make certificate available to other users
◊ Try -r for your ndncert issuer daemon
  o Port the certificate Data packet into the repository (either remote or local repo)
client.sendProbe(ca, "...",[...

sendNew(ca, certIdentity,
[...

sendSelect(ca, certIdentity,
[...

sendValidate(ca, ...,
[...

requestStatus / requestDownload
});

...);

},

...);

}
Examples and Documentation of NDNCERT

◊ NDNCERT command line tools source code
  o https://github.com/named-data/ndncert/tree/master/tools

◊ NDNCERT protocol specifications

◊ NDNCERT client and server configuration file samples
  o https://github.com/named-data/ndncert/wiki/Ca-Configuration-Sample
  o https://github.com/named-data/ndncert/wiki/Client-Configuration-Sample
NDNCERT Next Steps

◊ Simpler API to be used in applications (for intra-node certs)
◊ Integration with NDN Control Center
◊ Integration with NDN Android