NDN Security

ACM ICN 2018 Tutorial
Boston, MA, September 21, 2018

NDN Certificate Management with NDNCERT

Zhiyi Zhang (UCLA)

NDN Certificate

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

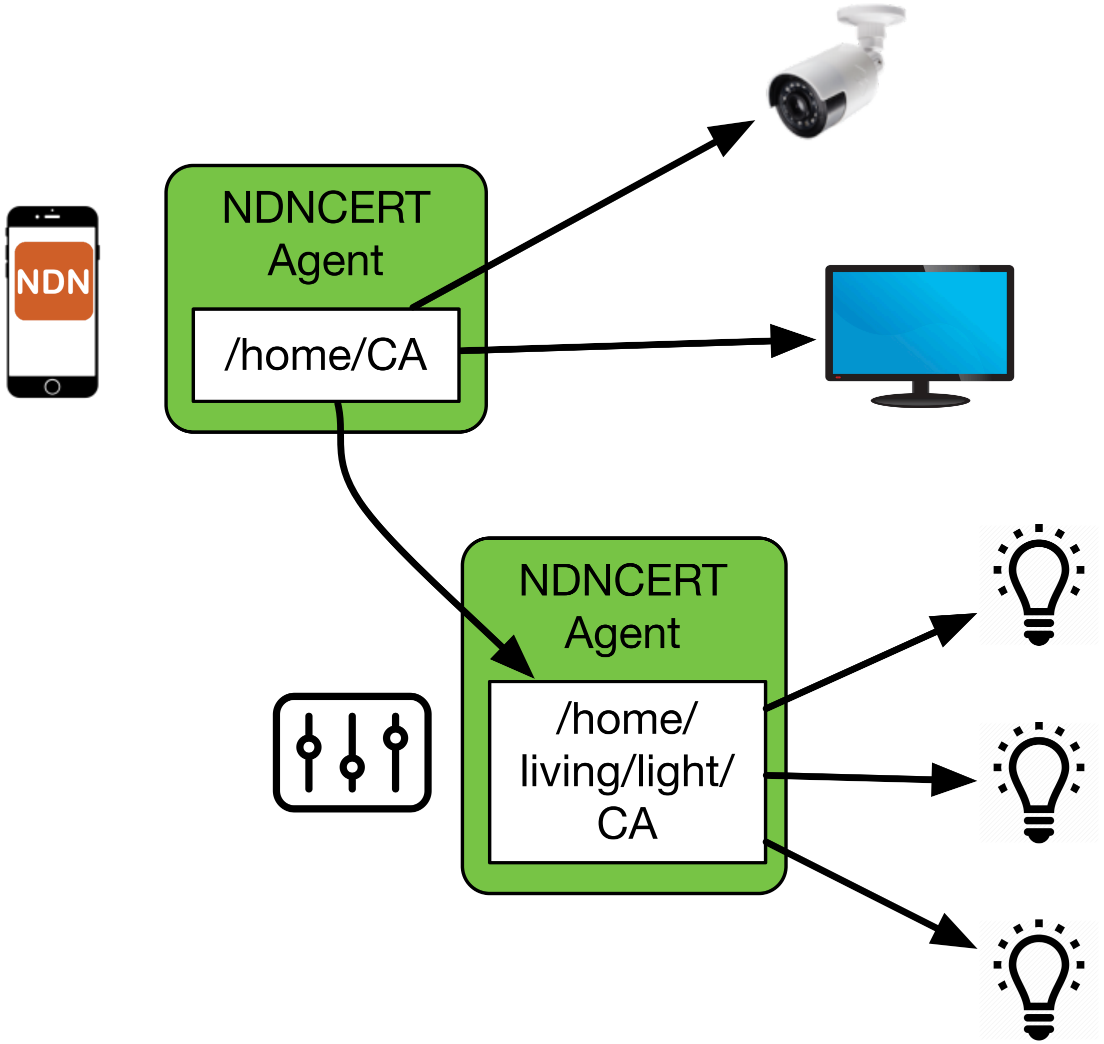
- Certificate helps others to cryptographically identify you and your data
- Certificate proves the ownership of an NDN namespace

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

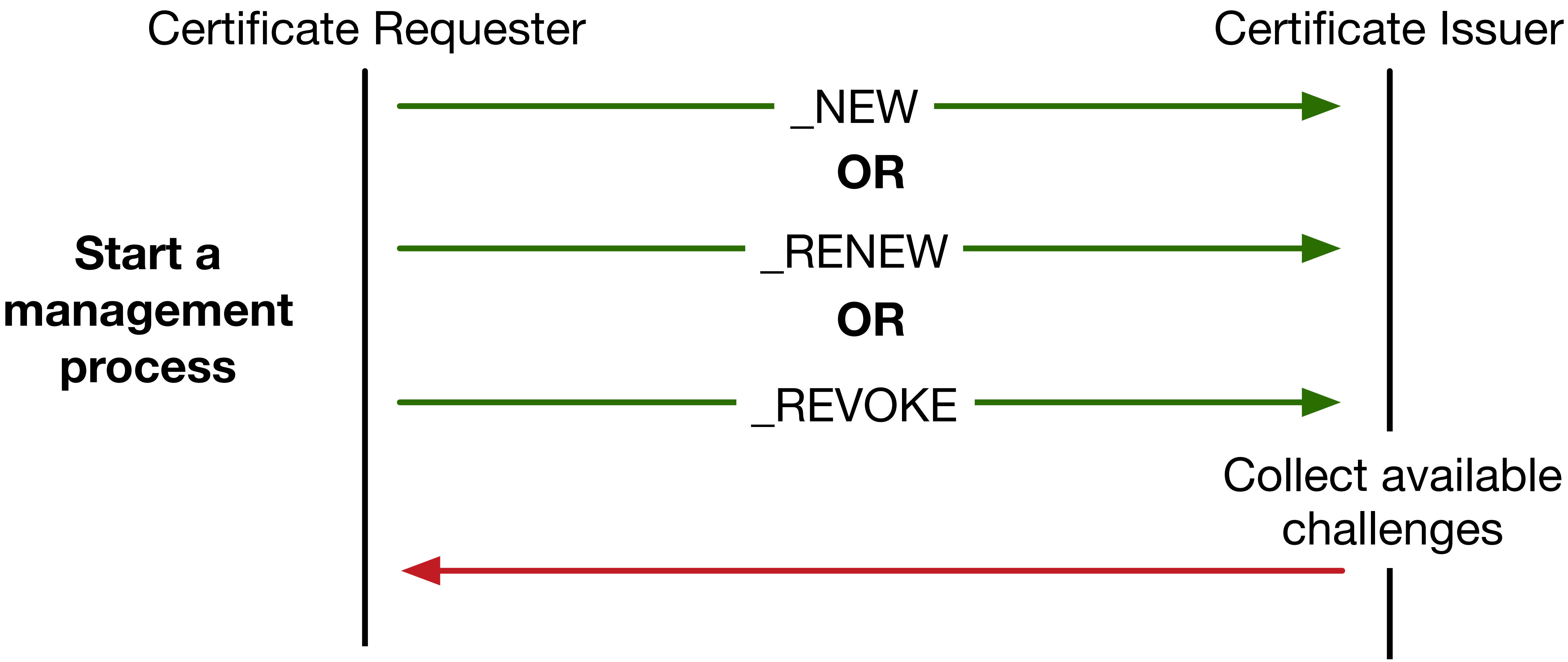
- An NDN entity can be a cert requester and a cert issuer at the same time



NDNCERT

- NDNCERT command line tools
  - Client
  - Server Daemon
- NDNCERT Library for applications to become a cert issuer/requester
  - Client APIs
  - Server APIs

NDNCERT Protocol



Certificate Requester

Certificate Issuer

Start a management process

_NEW

OR

_RENEW

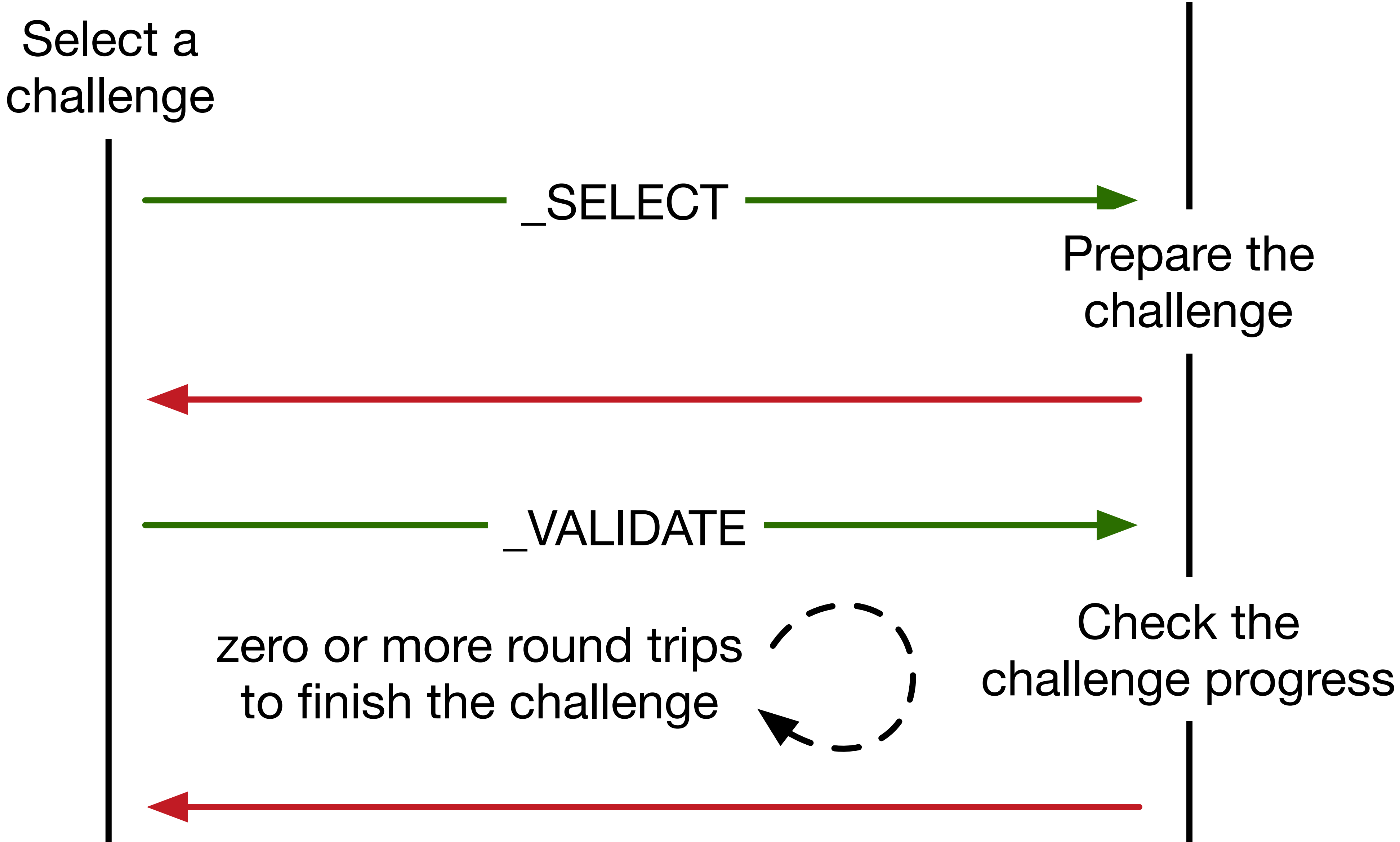
OR

_REVOKE

Collect available challenges

NDNCERT Protocol

Security Challenge Phase



Select a challenge

_SELECT

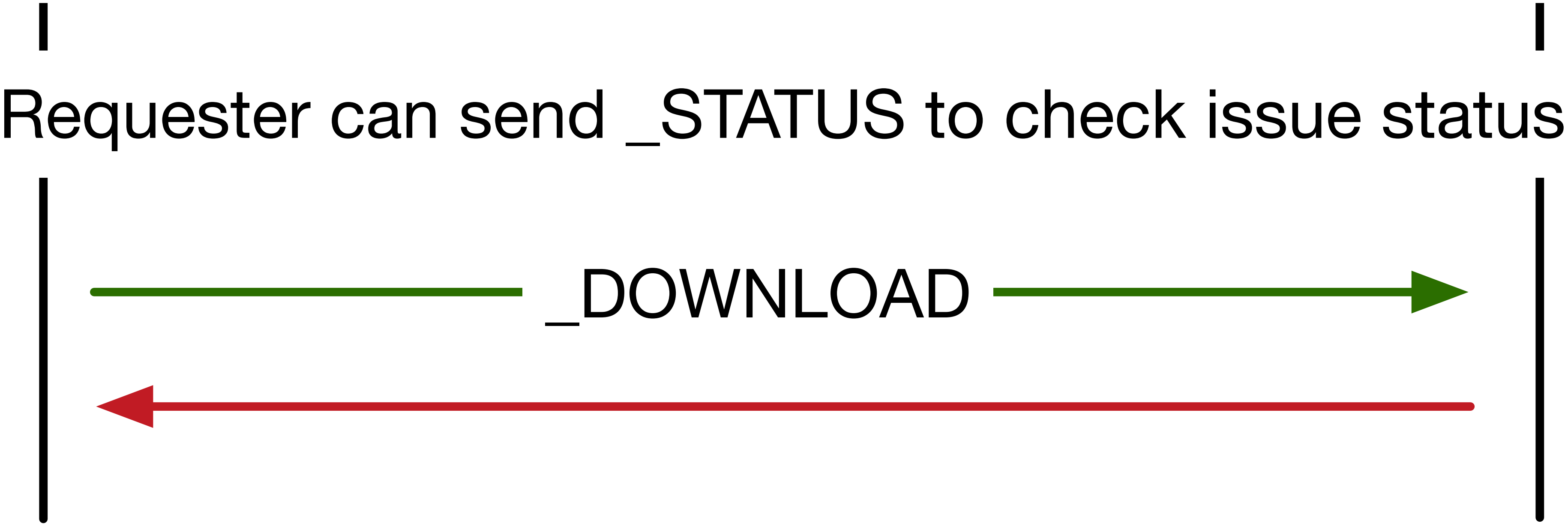
Prepare the challenge

_VALIDATE

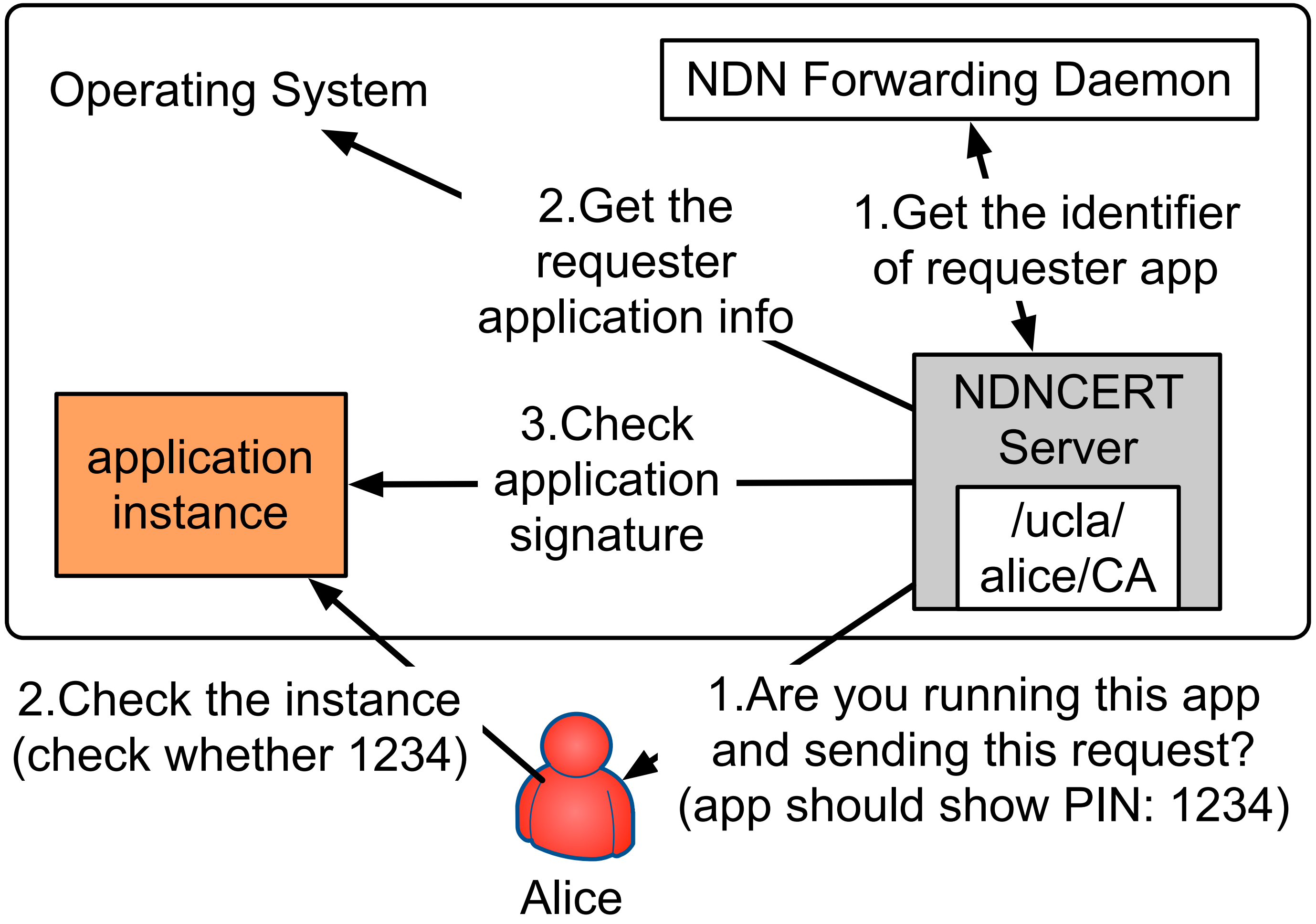
zero or more round trips to finish the challenge

Check the challenge progress

NDNCERT Protocol



Intra-node Certificate Management


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

- 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

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

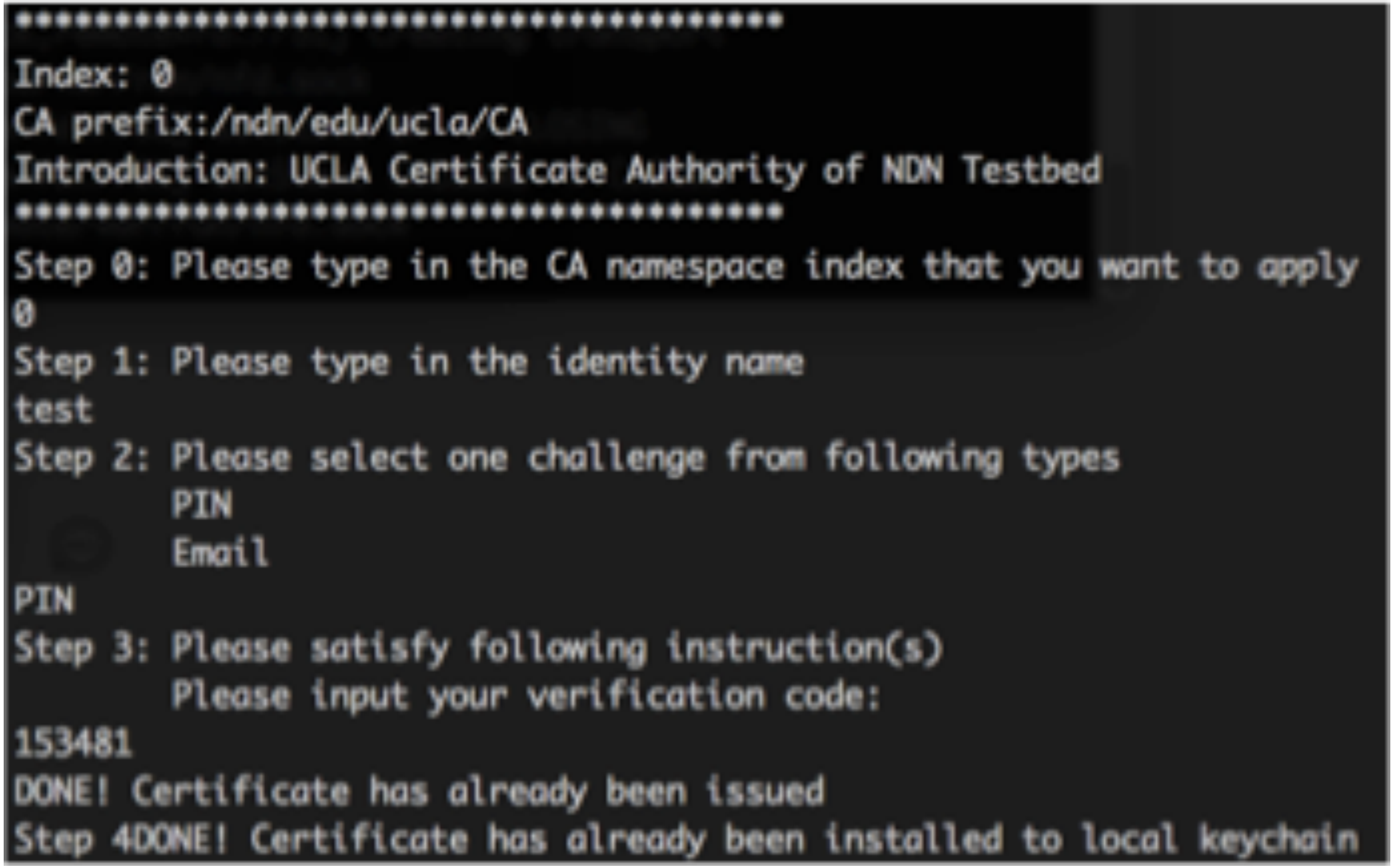
Prerequisites

- ◊ Your NFD is running
- ◊ A route from your NFD to NDN Testbed has been established
- ◊ The trust anchor has been downloaded:

```
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 4DONE! 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

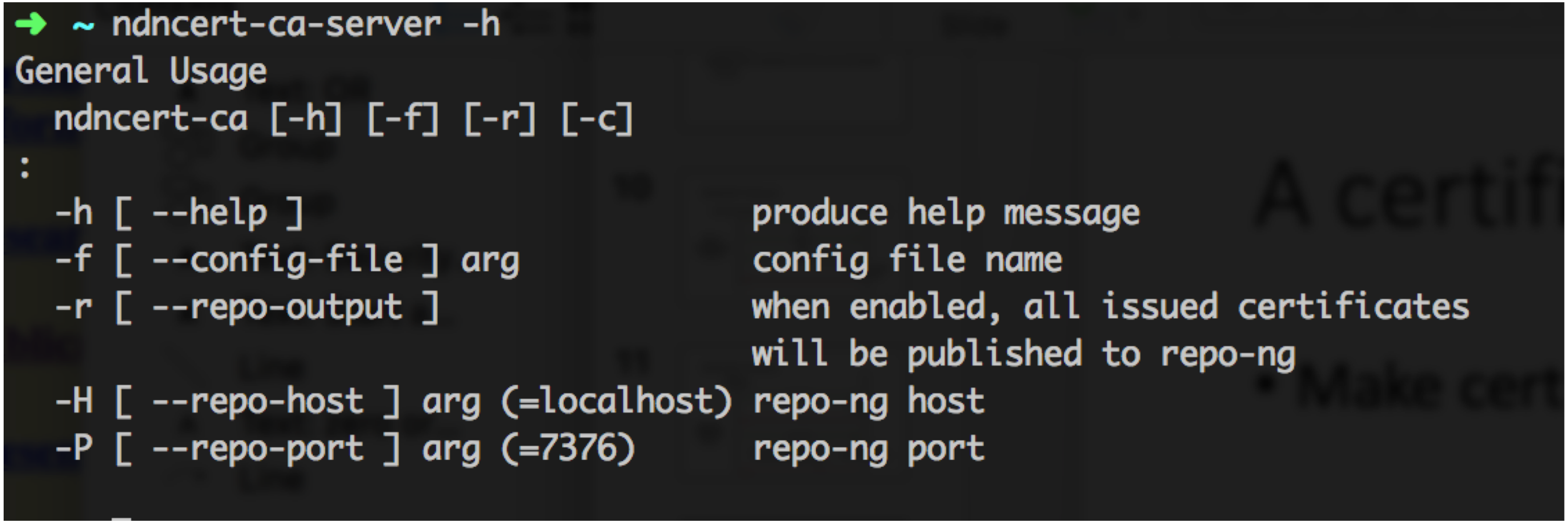
- Get a NDN testbed certificate now
  - if Junxiao Shi (NIST) hasn’t crashed my server yet

A certificate is not the end

◊ Make certificate available to other users

◊ Try -r for your ndncert issuer daemon

- Port the certificate Data packet into the repository (either remote or local repo)



```
➜  ~ ndncert-ca-server -h
General Usage
  ndncert-ca [-h] [-f] [-r] [-c]
:
  -h [ --help ]                       produce help message
  -f [ --config-file ] arg            config file name
  -r [ --repo-output ]                when enabled, all issued certificates
                                      will be published to repo-ng
  -H [ --repo-host ] arg (=localhost) repo-ng host
  -P [ --repo-port ] arg (=7376)      repo-ng port
```

NDNCERT Library For Applications

```
client.sendProbe(ca, "...",
                 [] (...) {
                   sendNew(ca, certIdentity,
                           [] (...) {
                             sendSelect(ca, certIdentity,
                                        [] (...) {
                                          sendValidate(ca, ...,
                                                       [] (...) {
                                                         requestStatus / requestDownload
                                                       });
                                        }
                                        ...);
                           },
                           ...);
                 }
                 , ...);
```

Examples and Documentation of NDNCERT

- NDNCERT command line tools source code
  - https://github.com/named-data/ndncert/tree/master/tools
- NDNCERT protocol specifications
  - https://github.com/named-data/ndncert/wiki/NDN-Certificate-Management-Protocol
- NDNCERT client and server configuration file samples
  - https://github.com/named-data/ndncert/wiki/Ca-Configuration-Sample
  - 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