UCLA ENGINEERING
Henry Samueli School of Engineering and Applied Science
Birthplace of the Internet

Deployment and Usage of NDNCERT

Zhiyi Zhang (UCLA), Alexander Afanasyev (Florida International University), Lixia Zhang (UCLA)

Internet Research Laboratory

Motivation

The Named Data Networking (NDN) [4] : all retrieved data packets must be signed. Requiring **simple, secure, and user-friendly** cryptographic key/cert management.

NDN Trust Management system (NDNCERT) [5] provides flexible mechanisms to **delegate trust between certificates**

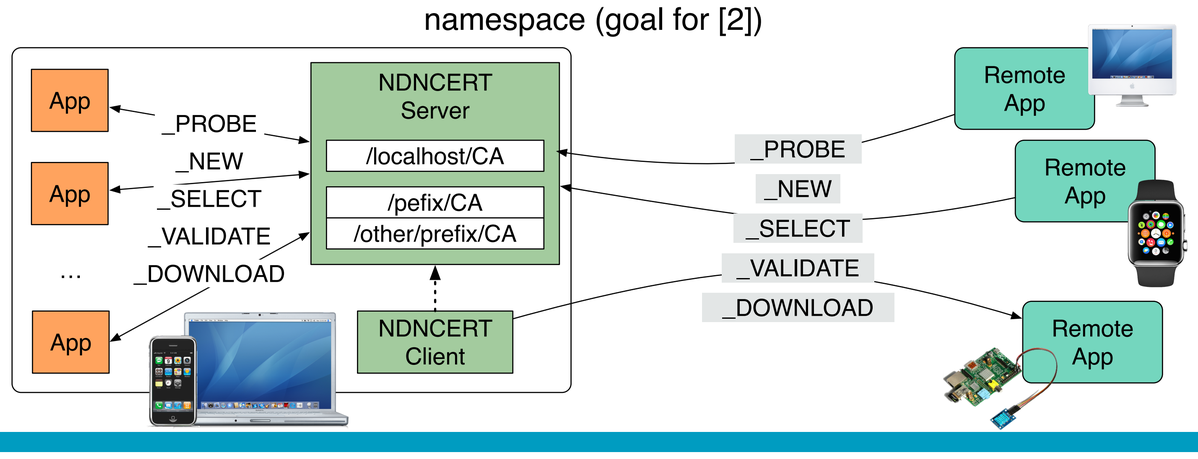
- **Within a single device** (managing permissions for local applications on a node to operate under a given namespace)
- **Across devices/entities**.

The poster introduces the deployment of NDNCERT over NDN testbed and shows how to use the command line tools or android app to get yourself an NDN certificate.

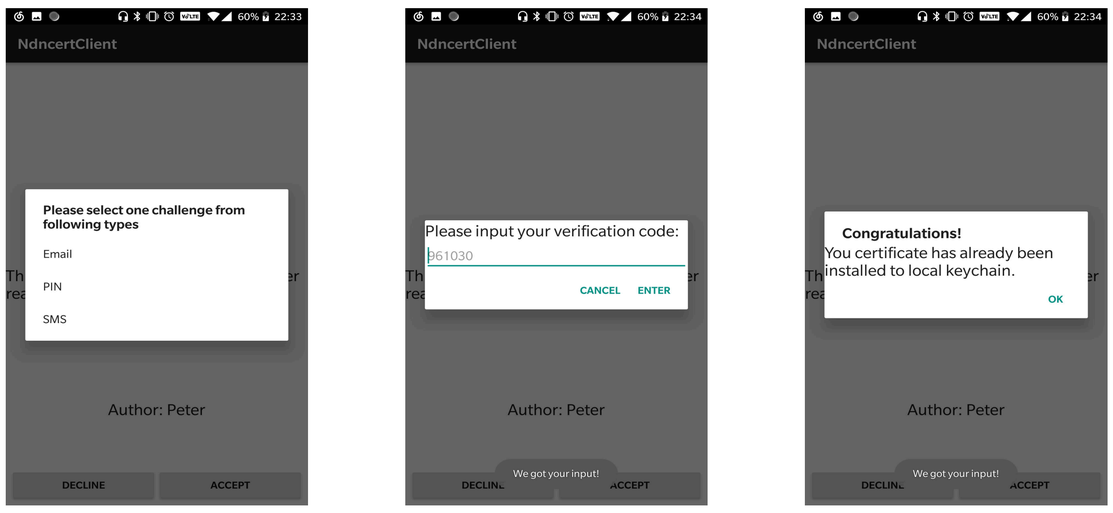
NDNCERT Overview

Automated intra-node and inter-node trust management over NDN

With obtained or self-signed (for local trust) each node can become authority for its namespace (goal for [2])



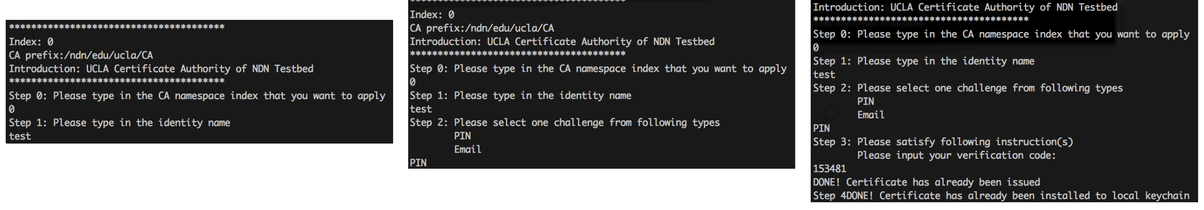
Android User Interface



With NDNCERT agent implementation over Android, mobile phone users can obtain NDN certificate via our Android app.

By simply selecting the type of the out-of-band challenge and finishing the identity verification according to certificate authority's requirement, one can obtain an NDN certificate for their own NDN identity name.

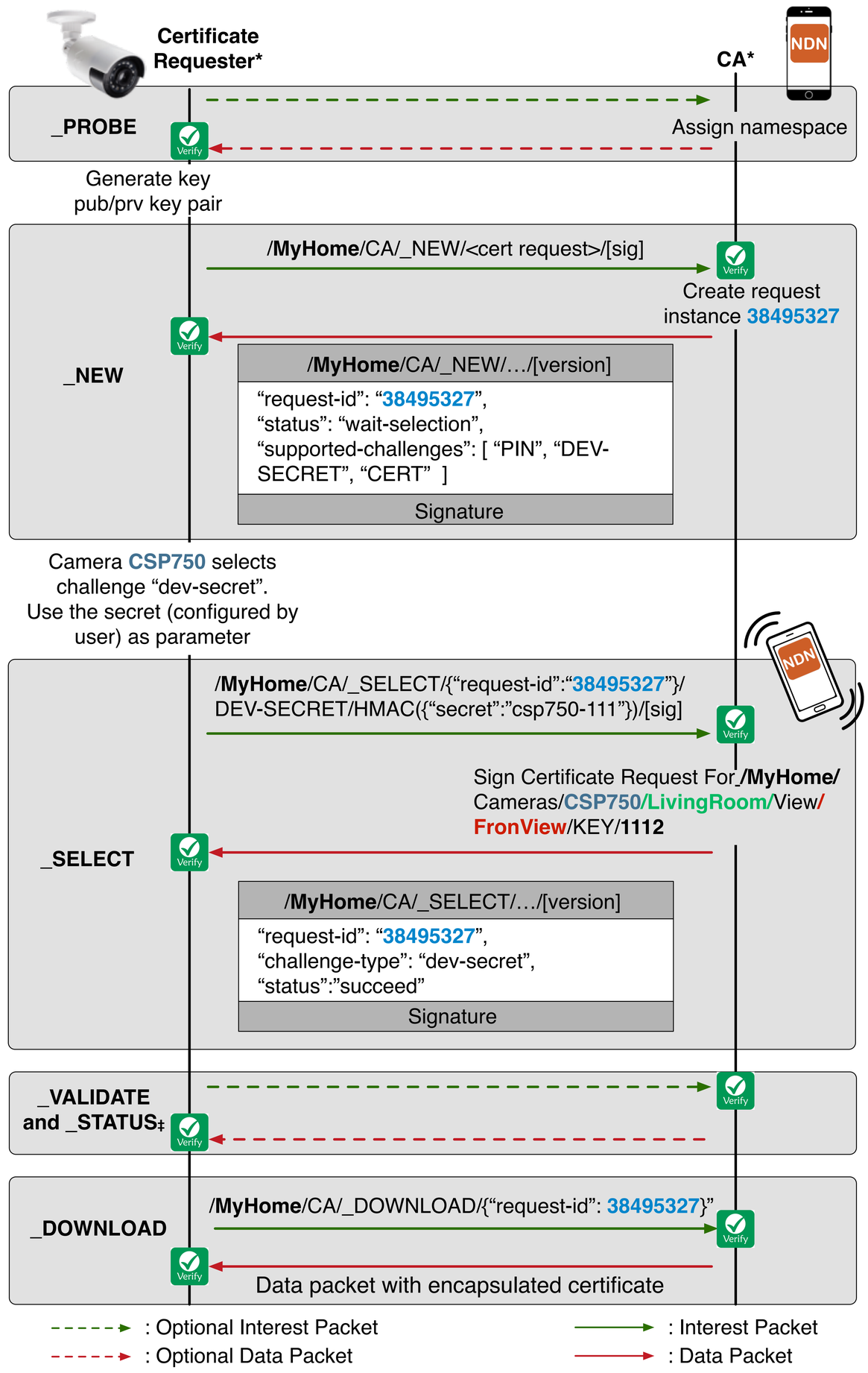
Linux/MacOS Command Line User Interface



With NDNCERT agent implementation over Linux and MacOS, users can obtain NDN certificate via command line tools.

By simply selecting the type of the out-of-band challenge and finishing the identity verification according to certificate authority's requirement, one can obtain an NDN certificate for their own NDN identity name.

Example of NDNCERT protocol

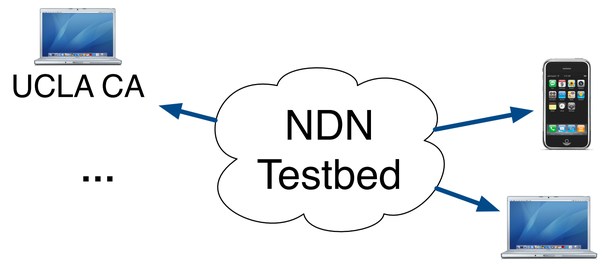


* All signatures of interest/data packet will be verified by CA and requester.
‡ Requester sends _VALIDATE if _SELECT alone cannot finish the challenge. Requester sends _STATUS if certificate is not immediately issued.

Deployment of NDNCERT

NDNCERT CA server has been deployed on NDN testbed. For now, NDNCERT CA runs on UCLA site and is able to issue certificates on behalf of NDN testbed.

By creating a face towards NDN testbed and adding the proper route, users can use command line tools or android app to get certificate, while applications can invoke NDNCERT library.



Codebases

NDNCERT Library and Tools: https://github.com/named-data/ndncert

NDNCERT Specifications: https://github.com/named-data/ndncert/wiki

NDNCERT Android App: https://github.com/DataCorrupted/android-identity-manager

This material is based upon work supported by the National Science Foundation under contract No. CNS-1345318 and CNS-1629922