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

NDNCERT: Usable Trust Management for Named Data Networking

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

Internet Research Laboratory

Motivation

Named Data Networking (NDN) [4] : all retrieved data packets must be signed

Requiring **simple, secure, and user-friendly** cryptographic key/cert management.

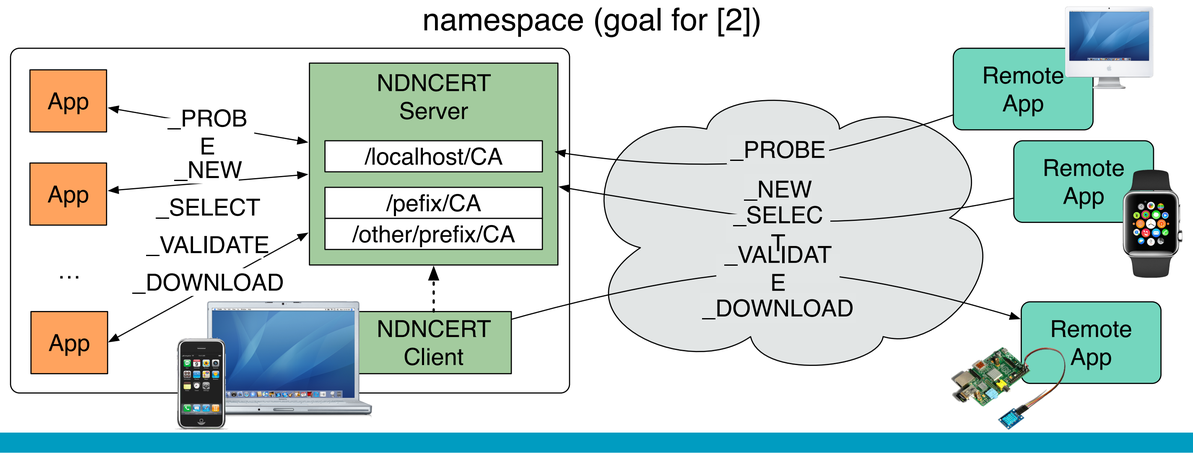
NDN Trust Management system (NDNCERT) [5] provides flexible mechanisms to **delegate trust between certificates**

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

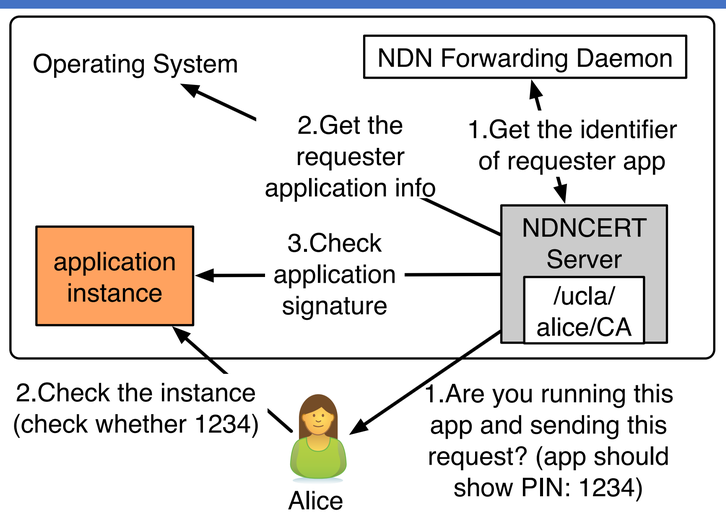
NDNCERT Overview

Automated intra-node and inter-node trust management inspired by ACME [1]

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



Intra-node NDNCERT



The two-way challenge for the intra-node NDNCERT

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

Modular NDNCERT Challenges

NDNCERT provides **modular security challenges**, enabling customized challenges to be added to meet different needs

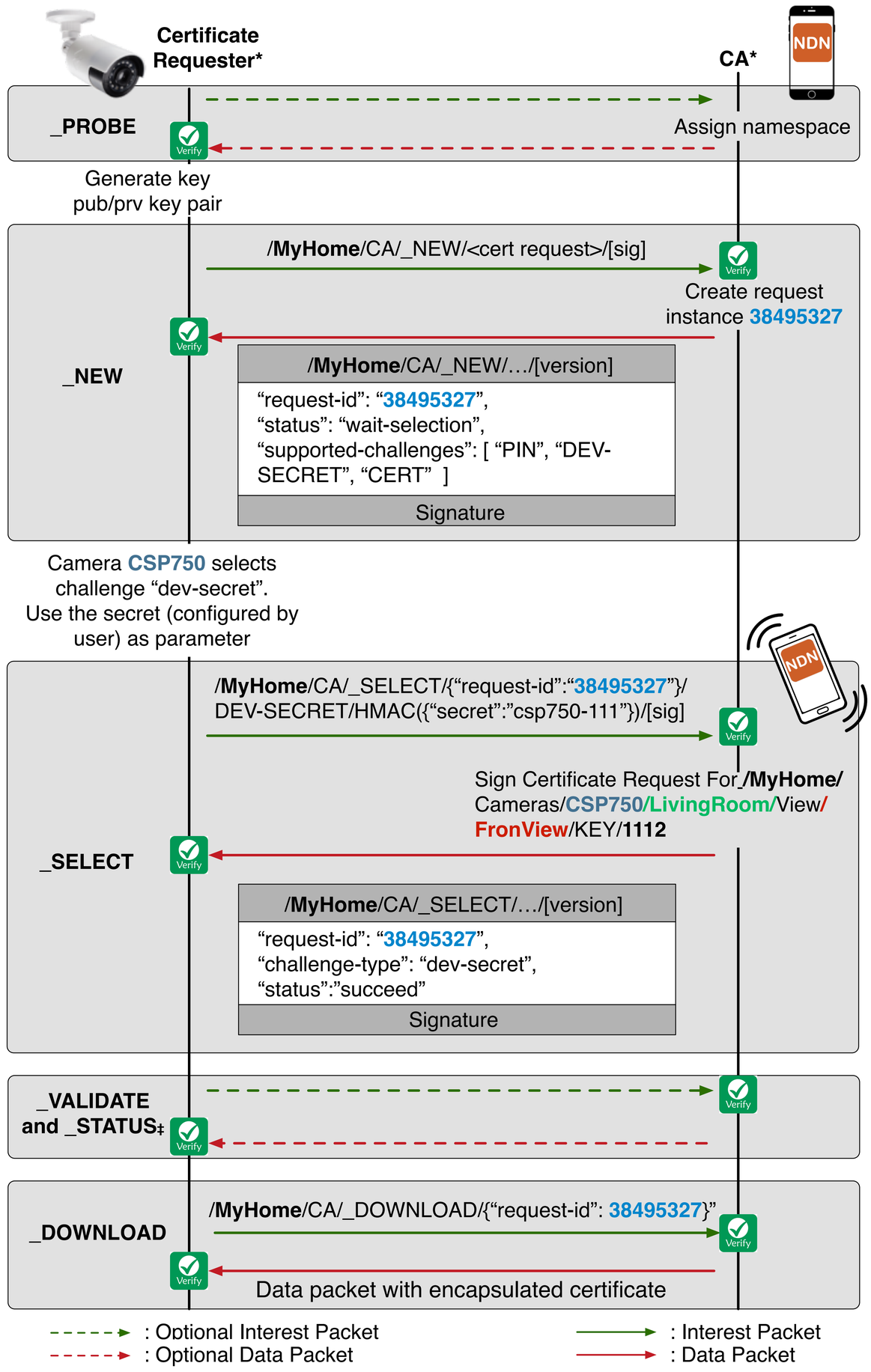
Currently implemented challenges

- **PIN code challenge**: Out-of-band access to a secret PIN code (CA-generated)
- **Device secret**: Out-of-band access to a shared secret (requester generated, such as scanning QR code before running the protocol)
- **Credential-based**: Proof-of-control of a certificate issued by another authority(ies)
- **Email-based**: (legacy) Proof-of-control of an email account

References

[1] R. Barnes and others. 2017. Automatic Certicate Management Environment (ACME). Internet Draft, draft-ietf-acme-acme-06. (2017).
[2] Ronald L Rivest and Butler Lampson. 1996. SDSI-a simple distributed security infrastructure.
[3] Yingdi Yu, Alexander Afanasyev, David Clark, kc clay, Van Jacobson, and Lixia Zhang. 2015. Schematizing Trust in Named Data Networking. In Proc. of ACM ICN.
[4] Lixia Zhang, Alexander Afanasyev, and others. 2014. Named data networking. ACM SIGCOMM Comp. Comm. Review (2014).
[5] Zhiyi Zhang, Yingdi Yu, Alex Afanasyev, and Lixia Zhang. 2017. NDN Certicate Management Protocol (NDNCERT). Technical Report NDN-0054. NDN.

Example of Protocol Exchanges



* 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.

Conclusion & Future Work

NDNCERT: flexible, easy, and user-friendly trust management

- Delegate trust between certificates
- Any node becomes a CA
- Modular authentication challenge design
- Intra-node and inter-node trust

Future work

- Integrate NDNCERT into NDN Control Center, NDN Android and trust schema [3]
- Investigating more authentication challenges for IoT environments

Codebases

NDNCERT: https://github.com/named-data/ndncert
NDN Control Center: https://named-data.net/codebase/applications/ndn-control-center/
NDN on Android: https://github.com/named-data-mobile/NFD-android

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