# *Security Progress in ICE-AR*

ICN-WEN ANNUAL MEETING

JUNE 20 2018

# Outline

- Introduction
- Schematized Trust Progress
- Access Control in the Context/Deep Context Parlance
- Some other contributions
- Next Year

# Outline

- Introduction
- Schematized Trust Progress
- Access Control in the Context/Deep Context Parlance
- Some other contributions
- Next Year

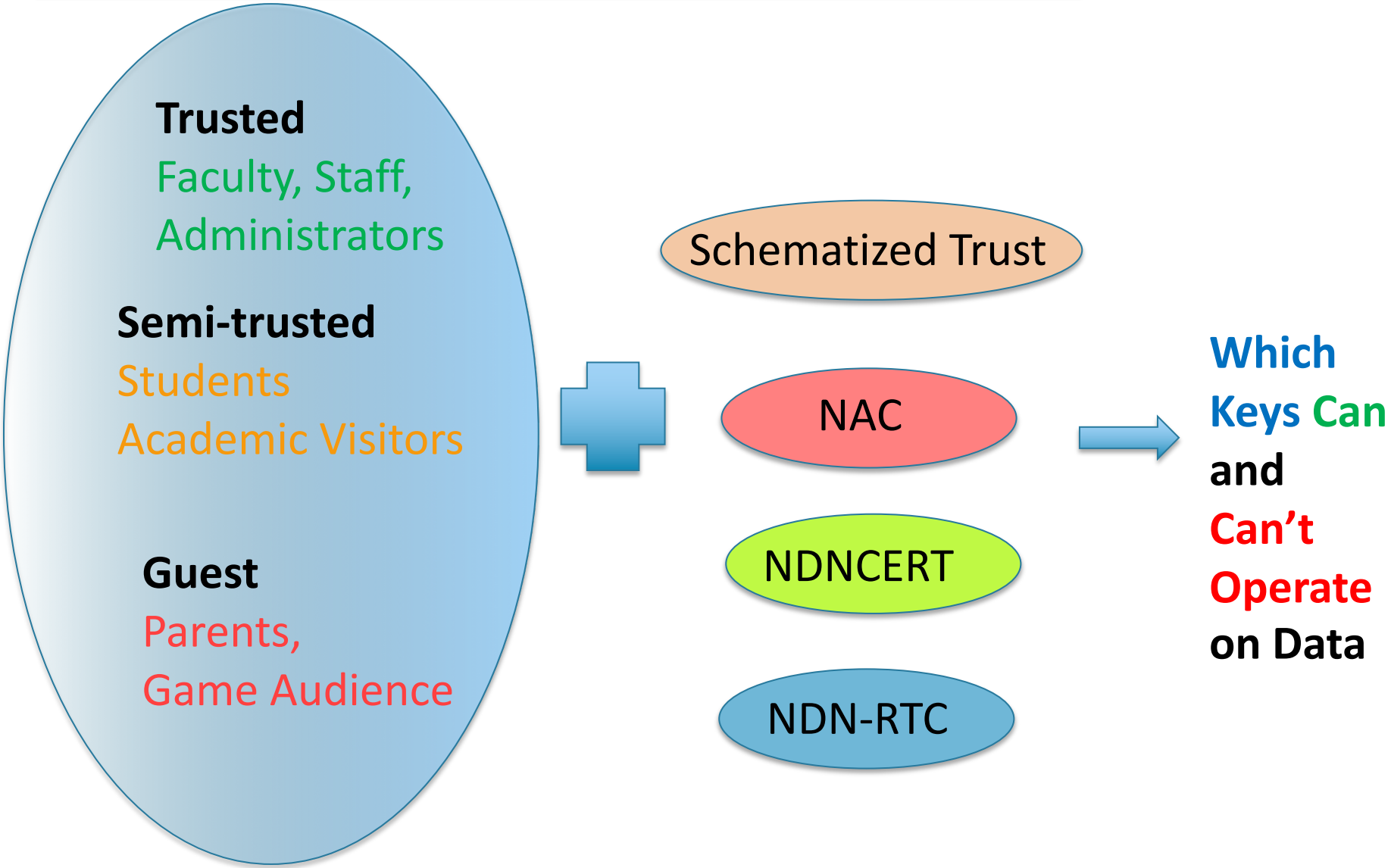
# Introduction

- Scope of ICN-WEN
  - Creating a trust framework for use by the diversity of users in the campus setting
    - Trusted, Semitrusted, Untrusted (Guest)
  - Exploring mechanisms for access control for the AR/VR case
    - How to share content between MD and EN?
      - Context and Deep Context
    - Efficiently leverage NDN's trust and access control.
  - Explore security enhancements and test their impact.

# Outline

- Introduction
- Schematized Trust Progress
- Access Control in the Context/Deep Context Parlance
- Some other contributions
- Next Year

# Users and Trust in the Campus Scenario.



# How to use schematized trust?

A trust schema set up for our application

**Trust Anchors (TAs)**

Well-known; trusted; end nodes have TAs' certificate for validation

**End Nod**

Mobile Dev
Edge Node

Obtain thei
a TA by ext
(Namespace
access)

/ucla/ca

/ucla/cs/ca

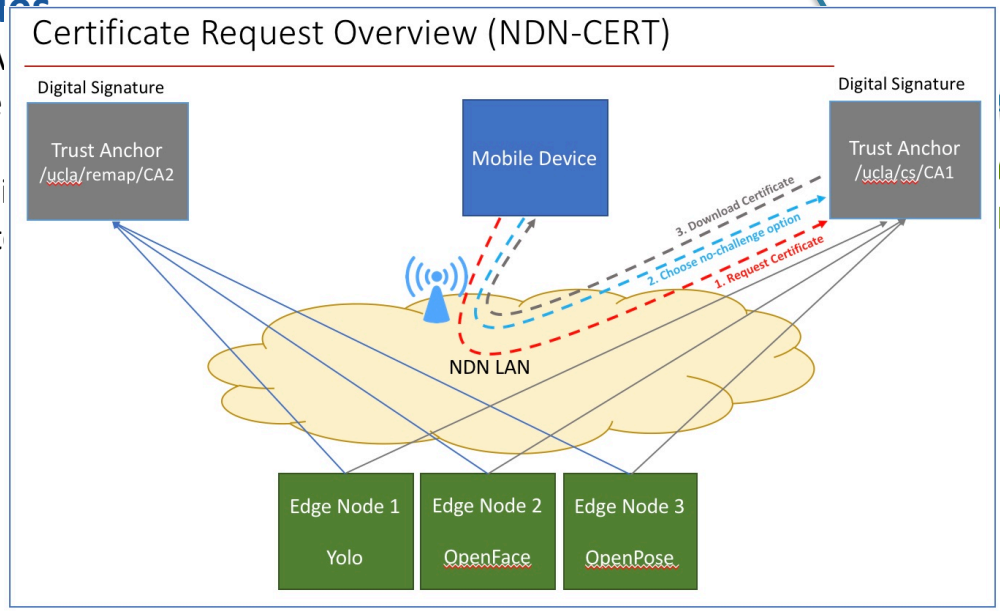
/ucla/remap/ca

/ucla/remap/guest/$MD_2$

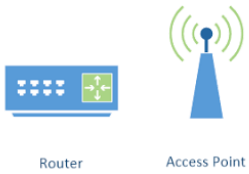
/$EN_1$

map/$EN_1$

ng trust

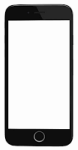


# Identity and Certificate plurality.




**/ice-ar/nmsu/cs,ece/SH/AP11**

**Identity:** **/ndn/edu/nmsu/cs/fac/jaymisra**

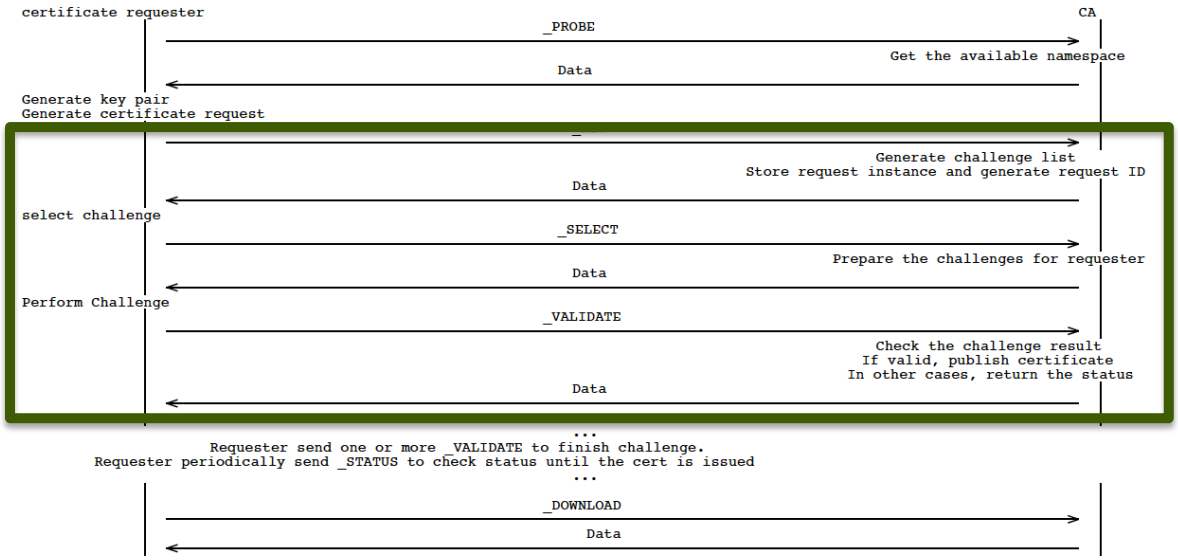


**Location:** **/ice-ar/nmsu/cs,ece/SH/AP11/MD1**

Name (hence identity) and certificate can be different!
Devices can get different certificates based on locations or services.

Signature of content vs. signature of location.
Challenges of user privacy vs location privacy.

# Using NDN-Cert to obtain certificate for a given namespace from a CA.




Certificate Request Overview in NDN Cert

Works with trusted users.

What is the “challenge” for a guest?

**Things to do:**

Automate the process to remove manual user input

Design a mechanism for the guest to work

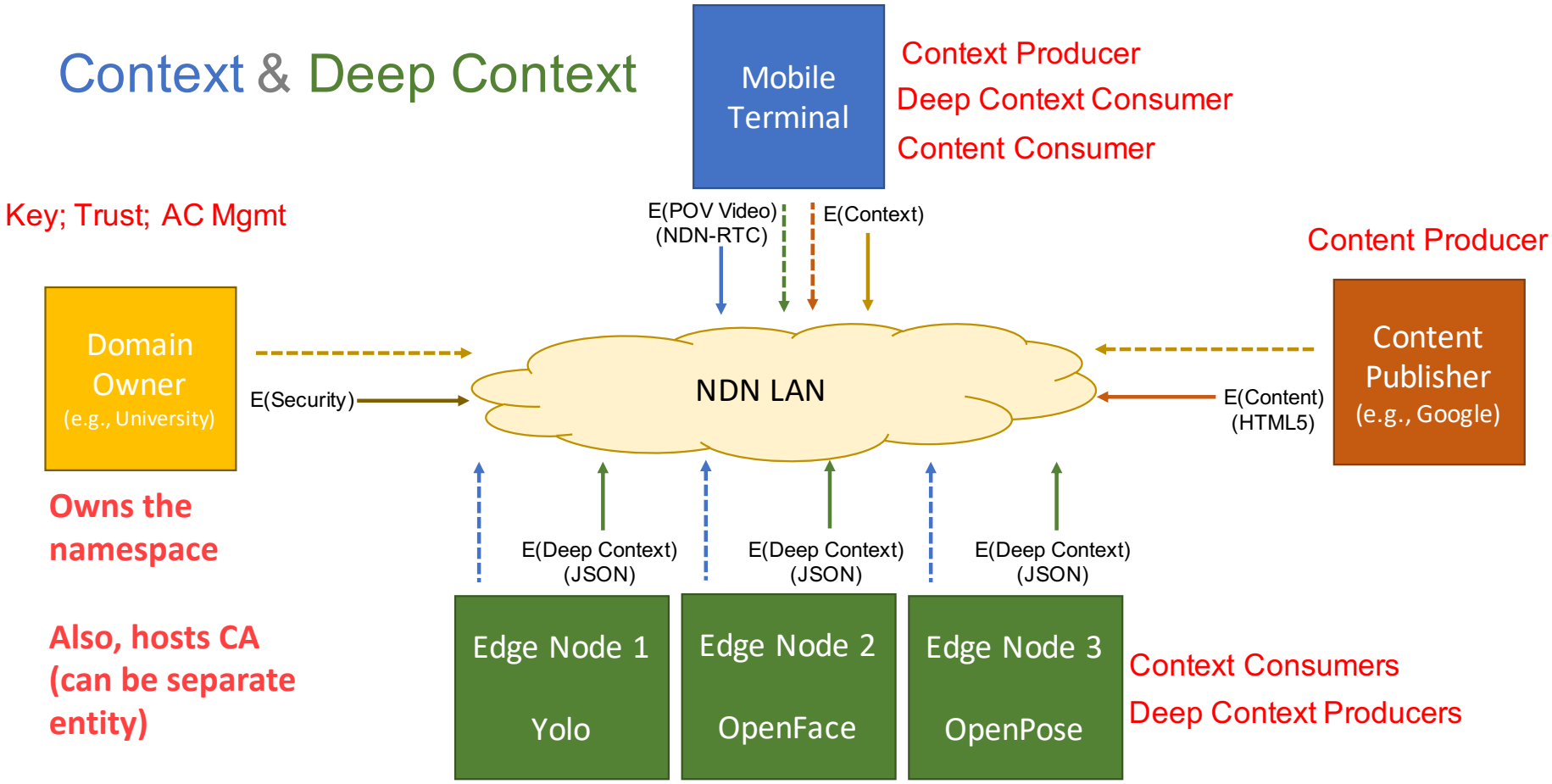
Identify a generic challenge mechanism for the users.

Integrate with Name-based access control.

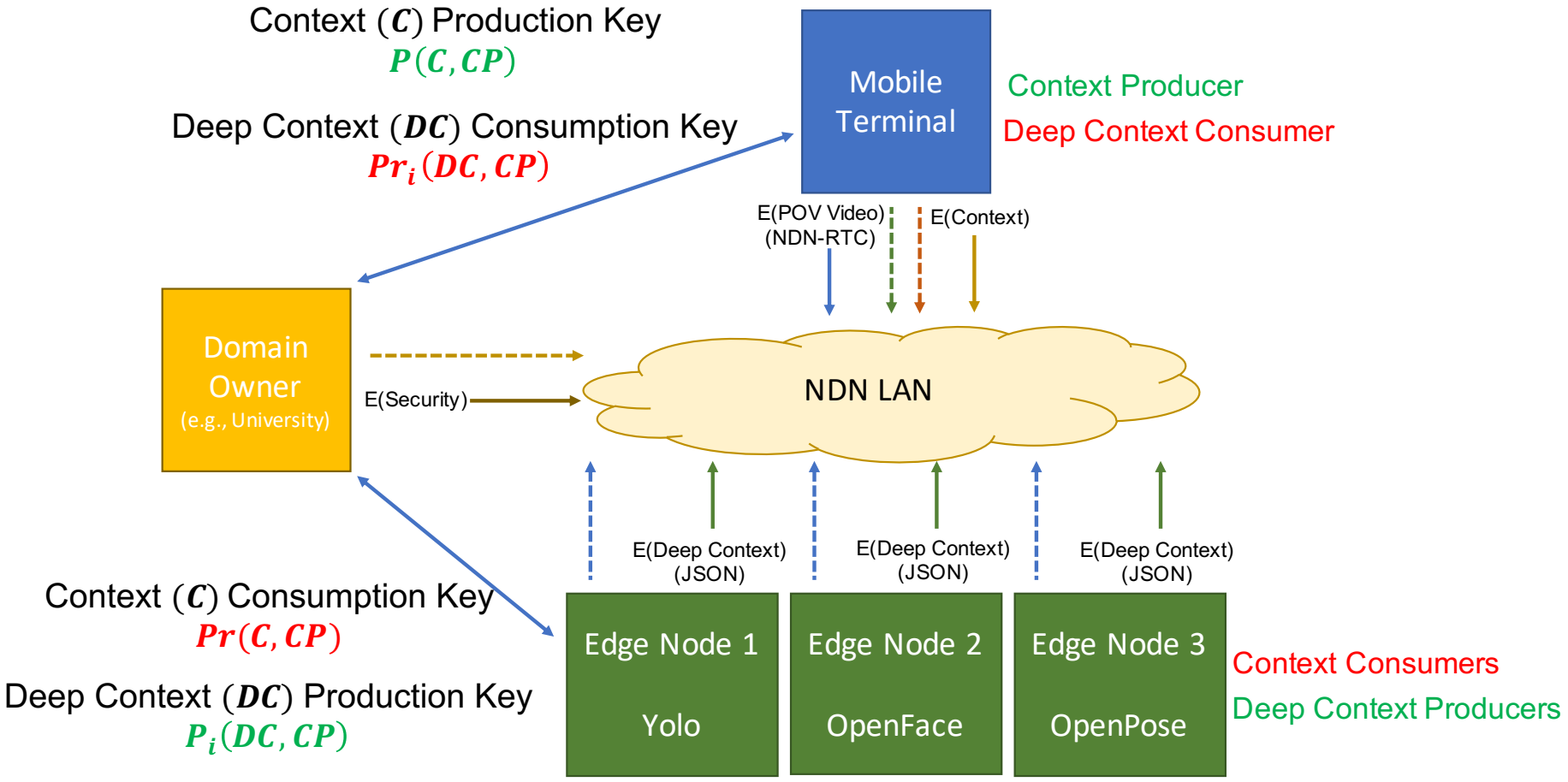
# Outline

- Introduction
- Schematized Trust Progress
- Access Control in the Context/Deep Context Parlance
- Some other contributions
- Next Year

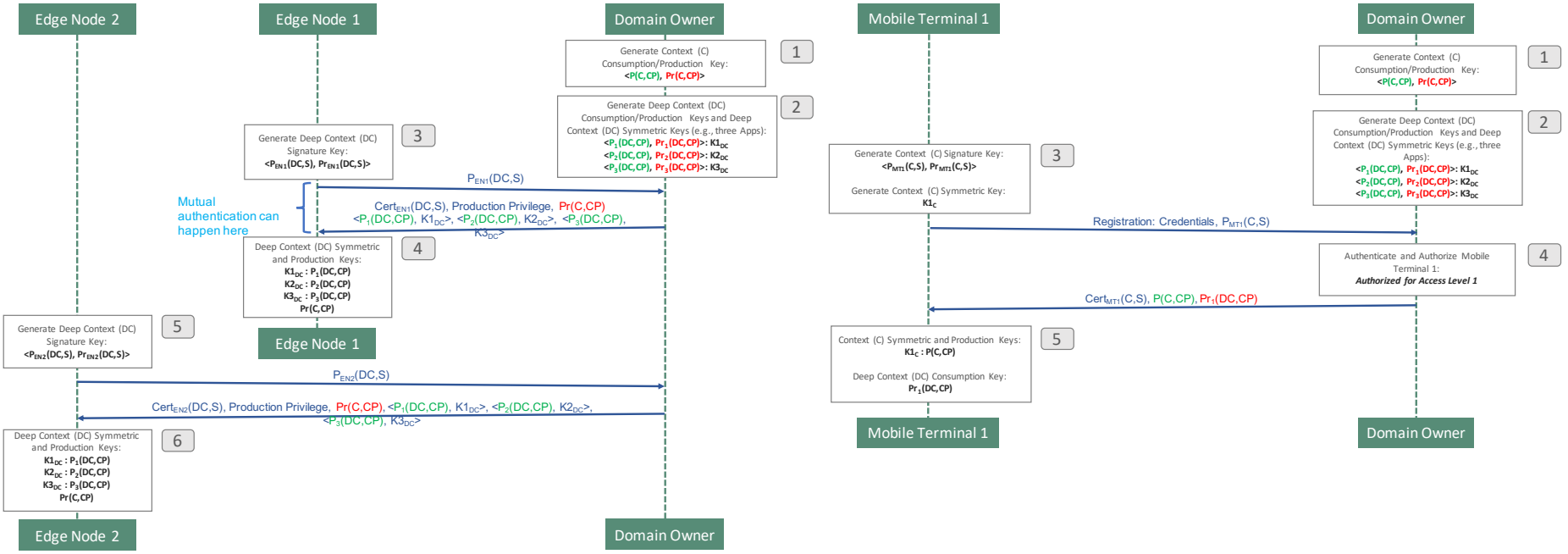
# Access Control: Context + Deep Context



# Set-up for Access Control



# Working on Protocol Design for AC

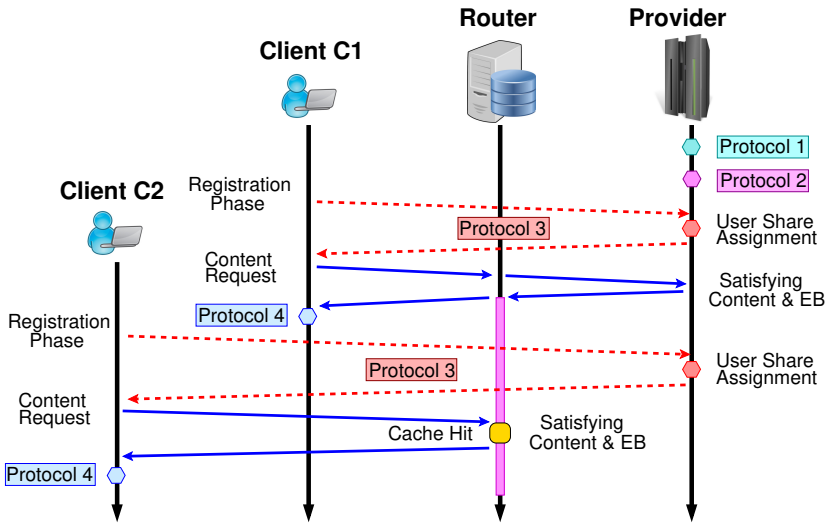


# Outline

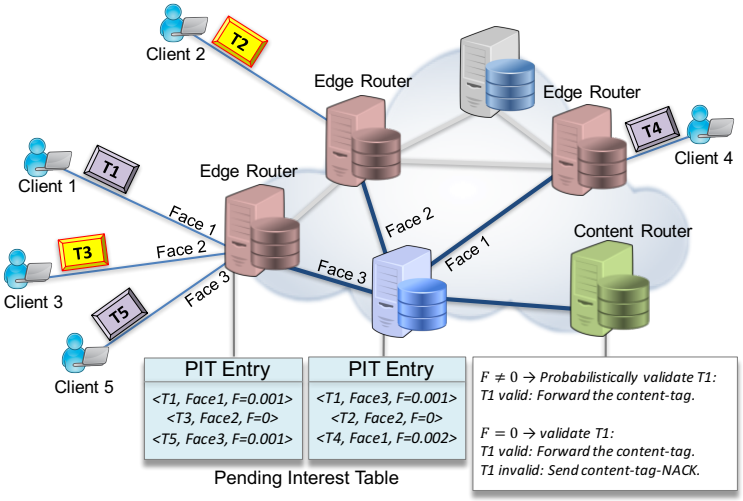
- Introduction
- Schematized Trust Progress
- Access Control in the Context/Deep Context Parlance
- Some other contributions
- Next Year

# Some other contributions

- Access Control edge and beyond



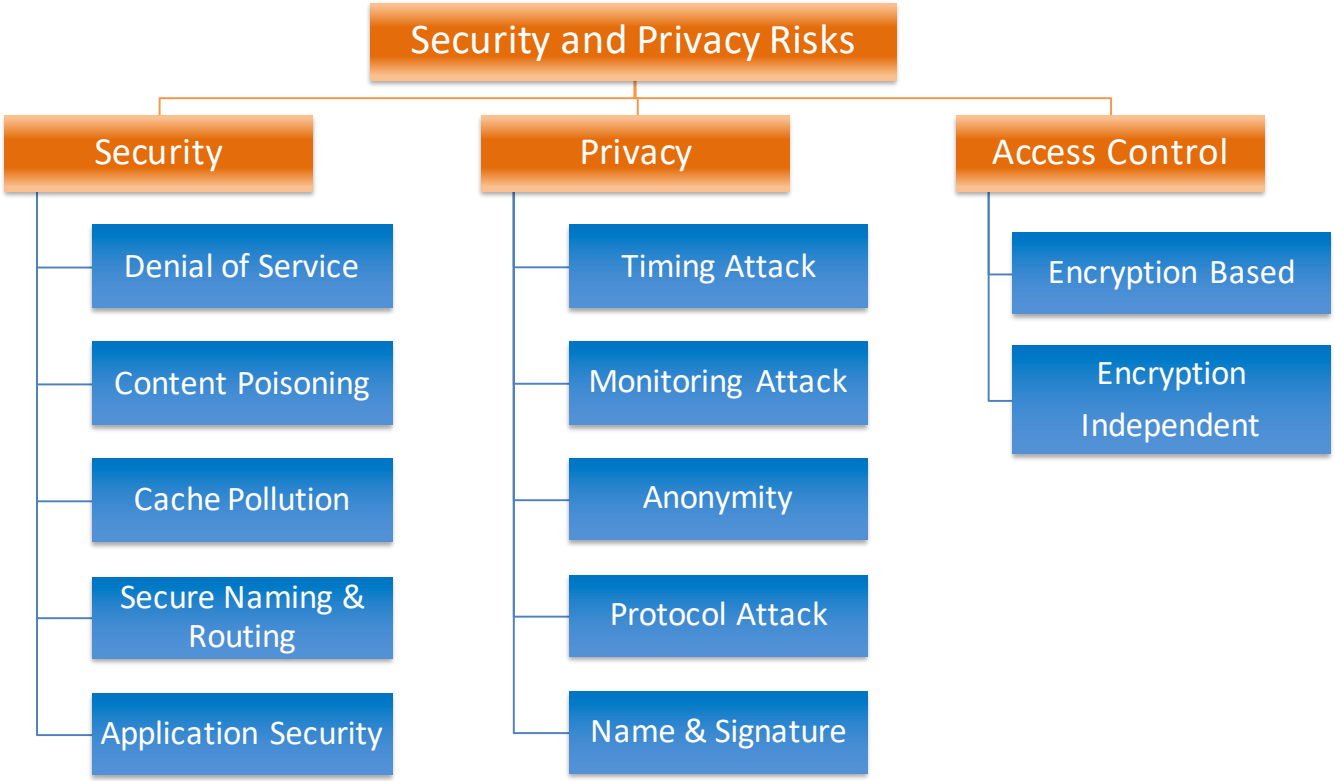

Broadcast Encryption based access control @ edge (TDSC'18)




Tag based access control @ edge (ICDCS'18)

# Some other contributions

- Security, Privacy, and Access Control Survey



# Next Year

- Integrate Security into the application
  - Plan to do first integration and testing in summer and early fall.
  - Refine design for meeting application needs
    - Latency
    - Different tolerance to security
- Implement Variable security
- Explore Edge computing security in the NDN context

# Looking Beyond: Community Security Challenges.

- Application driven not application specific.
  - Domain-specific and task specific security
- Security in the application-driven context.
  - Security on a sliding scale
  - Binary Trust does not work!
    - Especially true in a dynamic or disaster environment
- Privacy-efficiency tradeoff.
  - Better approach than just saying
    - You want privacy? Then, there is no efficiency.
    - You want efficiency? Then, there can be no privacy.
  - Multi-stakeholder, multi-tenant, multi-user setting
    - Data
    - Computation
    - Meta-data and Post-processed data

Thank You!