MILCOM 2017

MILITARY COMMUNICATIONS AND INNOVATION - PRIORITIES FOR THE MODERN WARFIGHT

Named Data Networking of Secure Things

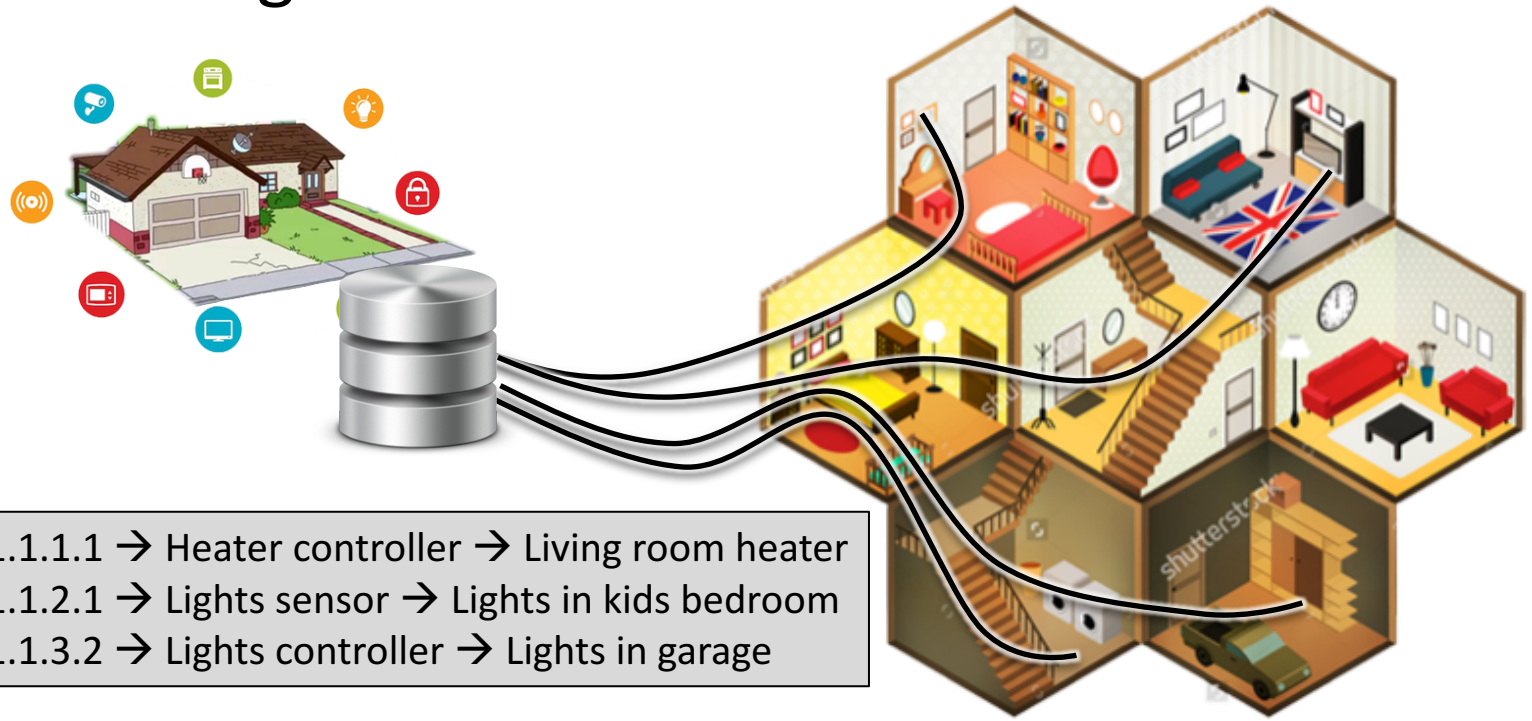
Alex Afanasyev

Florida International University

BALTIMORE, MD • OCTOBER 23–25, 2017

Today's IoT over TCP/IP

- Point-to-point communication model
- Cloud dependency
- With focus on devices that are associated with a "things", not "things" themselves

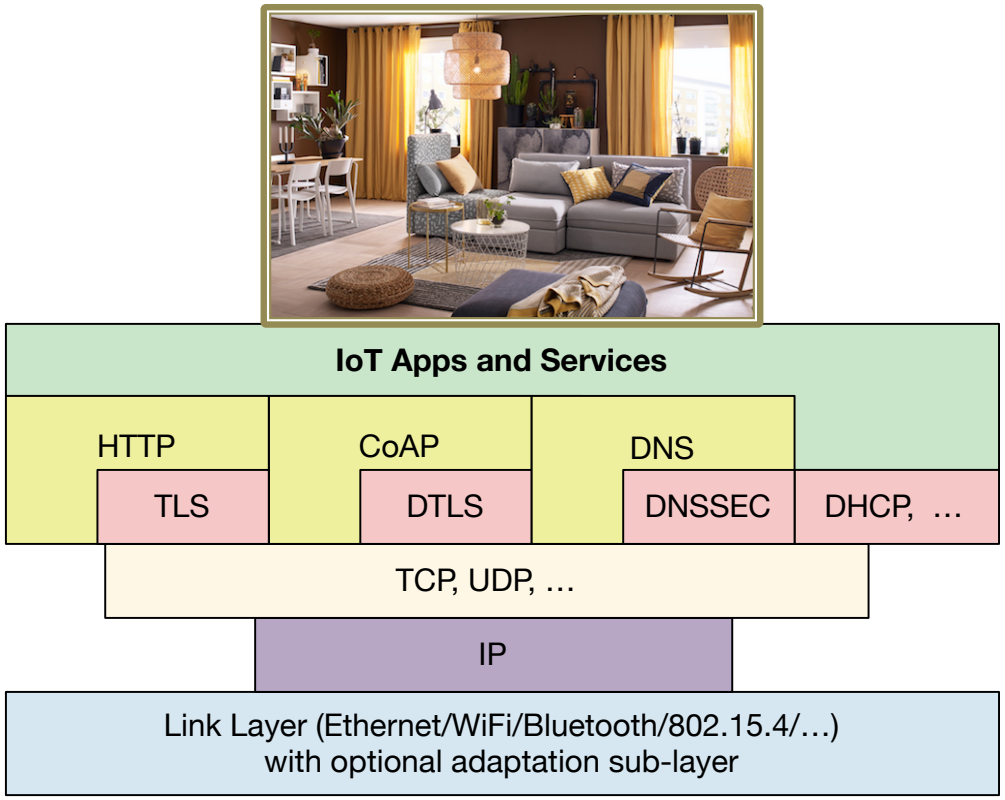


1.1.1.1 → Heater controller → Living room heater
1.1.2.1 → Lights sensor → Lights in kids bedroom
1.1.3.2 → Lights controller → Lights in garage

amazon web services
Microsoft Azure
androidthings
Google Cloud Platform
Weave
iCloud
SAMSUNG SmartThings™

Complexity and Semantic Mismatch for IP/IoT

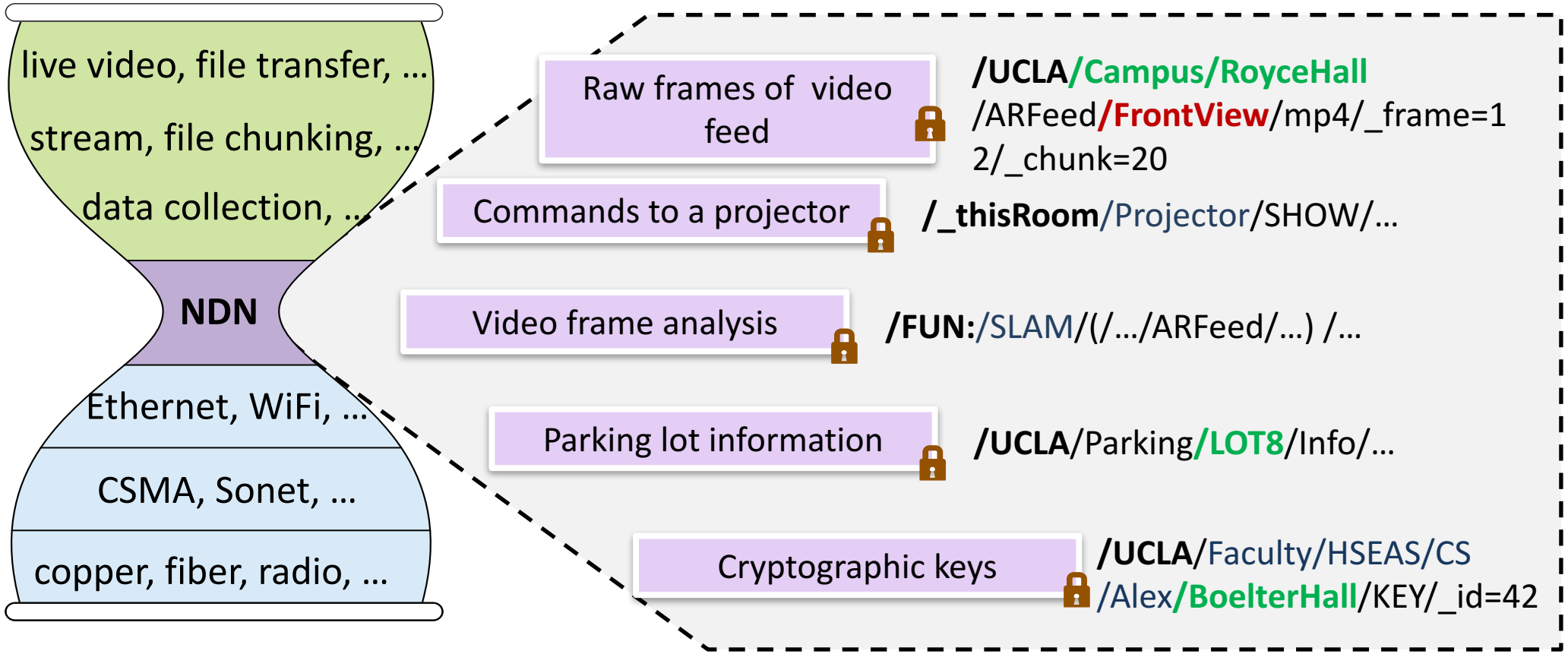
- **App: "Living room frontal view feed"**
- Network:
  - Request stream (HTTP/CoAP)
  - Connect to camera (TCP/IP)
- +
  - Lookup mapping "Living room" -> camera URI
  - Connect to AlexHome.com (cloud?) service
  - DNS lookup IP of AlexHome.com service
  - DHCP to assign IP addresses to all devices



NDN Alignment with IoT Applications

- Name the “things” and operations on “things”
  - “temperature in the room”, “humidity on the second floor”
  - “blood pressure”, “body temperature”
  - “max/min/avg pH of soil in specific point of US soil grid”
- Secure data directly
- Request-response semantics with name-based forwarding and in-network cache
  - Make use of ad hoc and broadcast-style communications
  - Make use of any intermittent connectivity
  - Independence of communication technology

Application-Defined, Semantically Meaningful Names for All Data Packets



Bootstrapping, discovery, and auto-config

- No IP address allocations / management needed

Built-in identity

- nature of IoT device
- config interface

../lights/ON **../lights/OFF**

/local/discovery/lighting/serial=123456

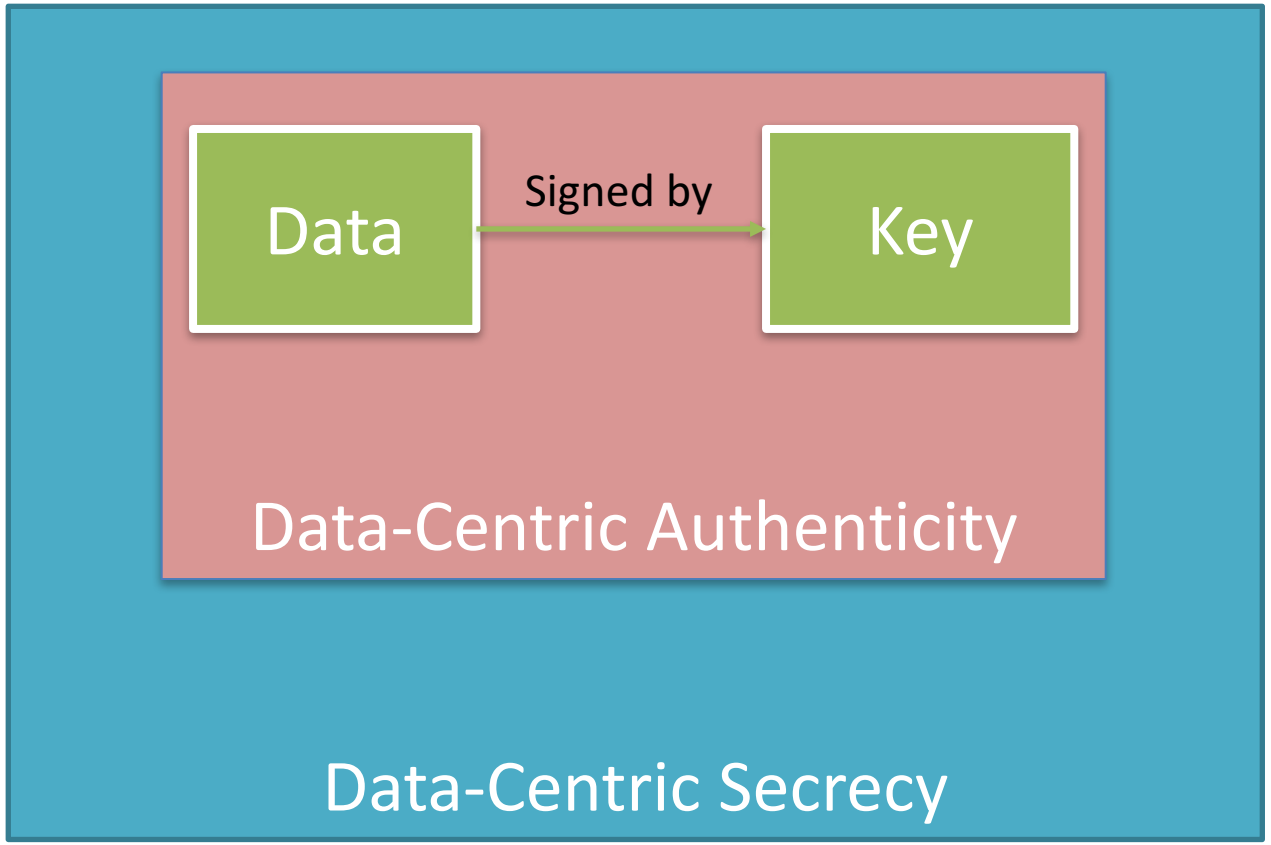
Enabling Trust

- out-of-band PIN
- a pre-scanned barcode

/MyHome/Bedroom/lights/...

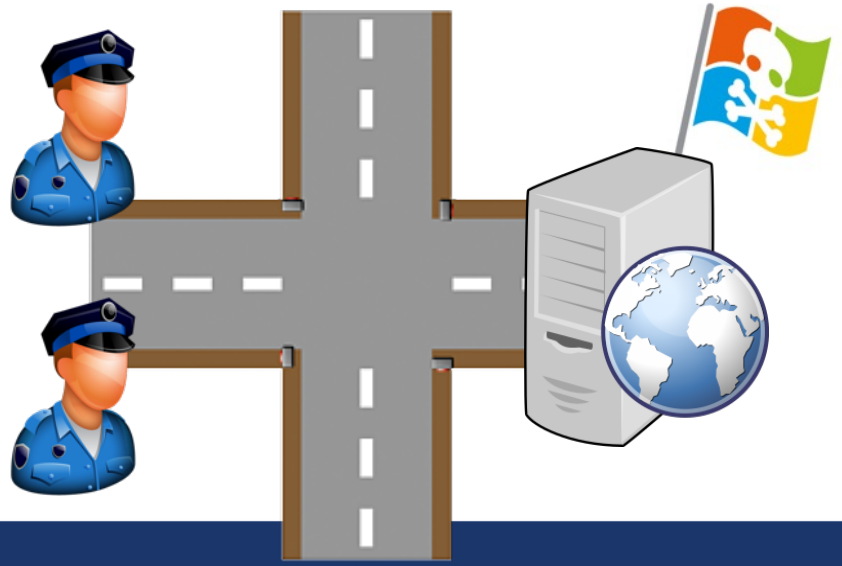
Operate

Data-Centric Security of NDN



Data-Centric Security of NDN: Built-In For Every Data Packet

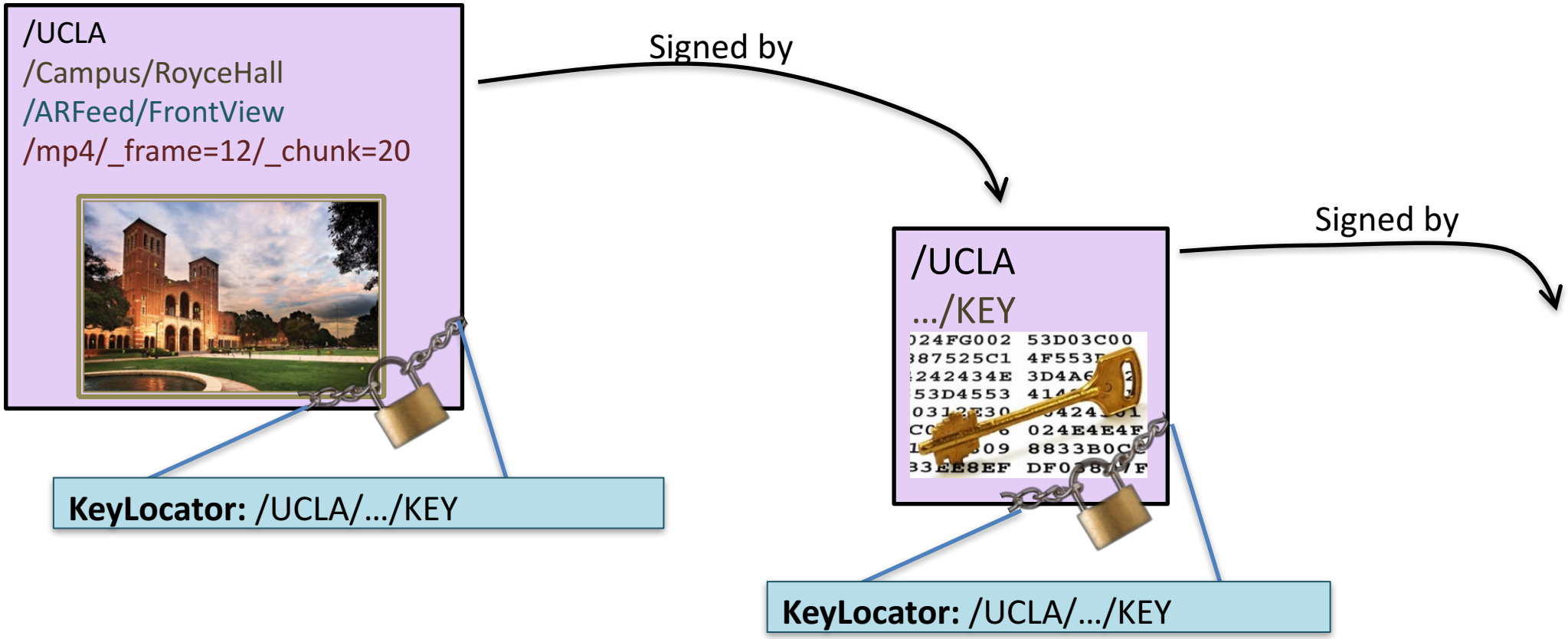
- In the Internet you secure your path..
- ..but the server may still be hacked!



- In NDN you sign the data with a digital signature..
- ..so the users know when they get bad data!
- Data secured in motion and at rest

/UCLA
/Campus/RoyceHall
/ARFeed/FrontView
/mp4/_frame=12/_chunk=20

Authentication of NDN Data



Key Privilege Separation

/UCLA/Campus/RoyceHall/ARFeed/FrontView
/mp4/_frame=12/_chunk=20

/UCLA/Camera/…/Campus
/RoyceHall/Camera/KEY

A frame from a camera installed in the Royce Hall

/UCLA/Campus/RoyceHall/ARFeed/FrontView
/mp4/_frame=12/_chunk=20

/Somebody.com/KEY

A forged frame

Name-Based Confinement of Key's Power

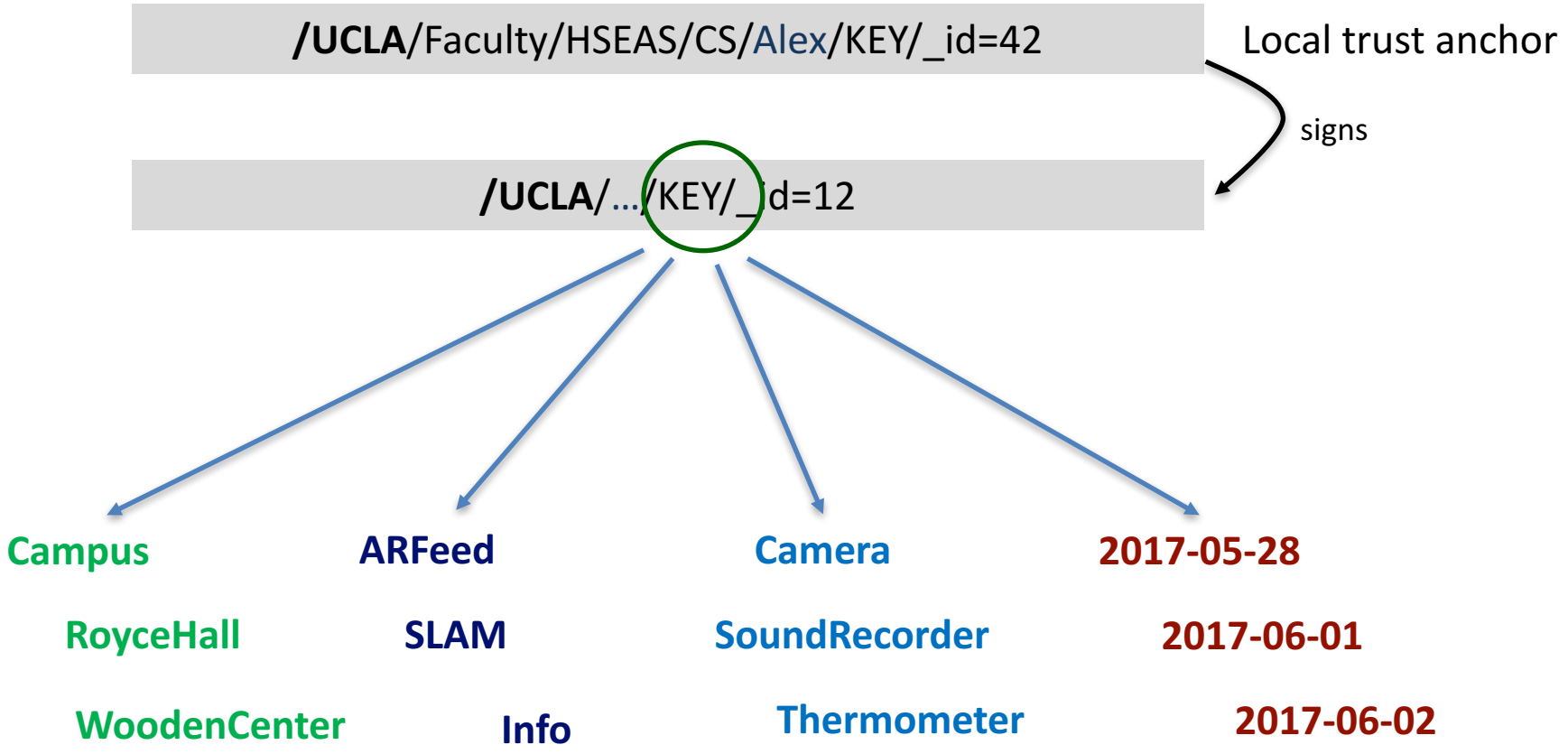
/UCLA/Campus/RoyceHall**/ARFeed**/…/mp4/_f=…/_s=…

Can only be signed by

/UCLA/Cameras/_id=…/RoyceHall/…/KEY/_id=…

ARFeed data to be valid, must be signed with a "Camera" key under the same name hierarchy

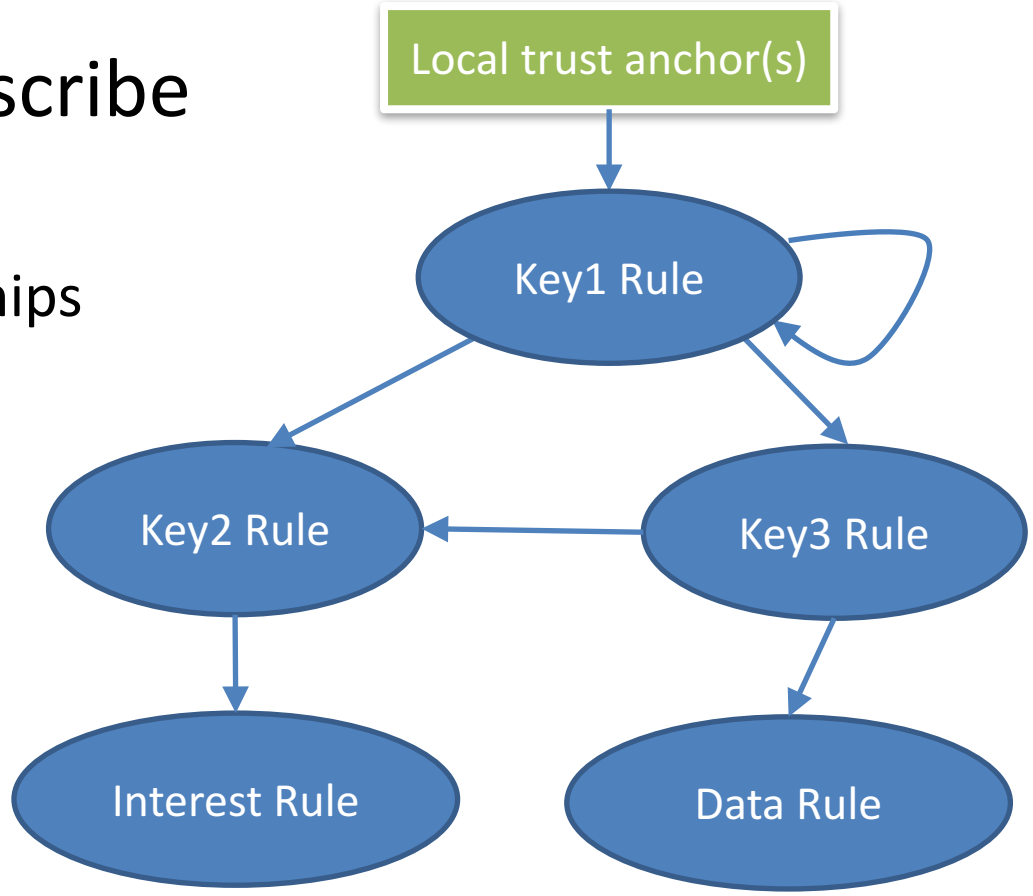
Flexible Confinement through Namespace Design



Trust Schema: Name-Based Definition of Trust Model

- A formal language to formally describe trust model
  - Schematize data and key name relationships

```
<>
<CONST>
token*
token?
[func]
(:group:token)
```



An Example of Trust Schema for Smart Campus

(:Prefix:<>*)(:Location:<>?)<ARFeed>**[View]**<mp4><frame><chunk>

Camera(Prefix, Location, View)

(:Prefix:<>*)<Cameras>[cam-id]**(:Location:<>?)**<View>**[View]**<KEY>[key-id]

Faculty(Prefix, Location)

(:Prefix:<>*)<Faculty>[user]**(:Location:<>?)**<KEY>[key-id]

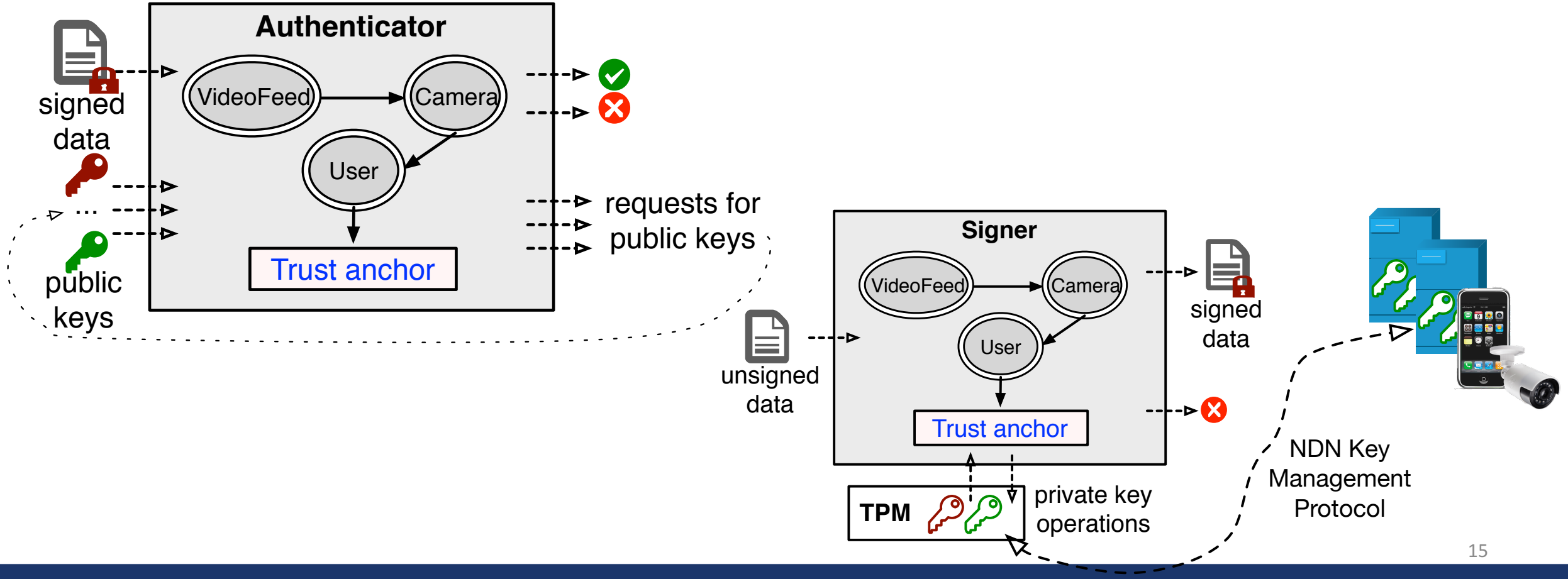
LocalAnchor(Prefix)

General Trust Model

/UCLA/KEY/_id=1

Trust Model Specialization for UCLA campus

Trust Schema as an Automation Tool

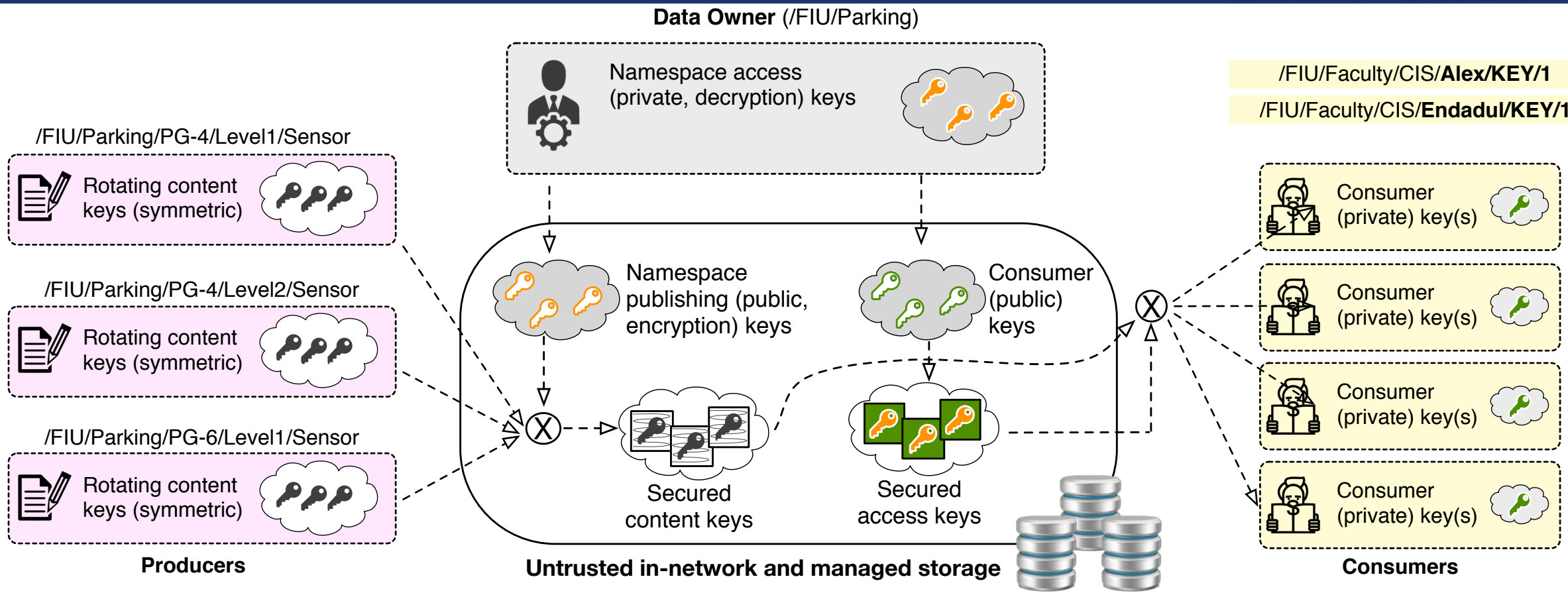


- Data-Centric Secrecy
- Name-Based Confidentiality and Access Control

Confidentiality and Access Control Requirements

- Data-centricity
  - Confidential “end-to-end” (app-to-app), in motion or at rest
- Flexible controls
  - Granting access to publish/read at fine granularities
  - Changeable policies at any time
- Asynchrony
  - No tight coupling between distributed data production and access granting
- Scalability
  - Manageable number of encryption/decryption keys
- Multi-party
  - Seamless coordination of control among distributed data producers and consumers

Name-Based Access Control (NAC)



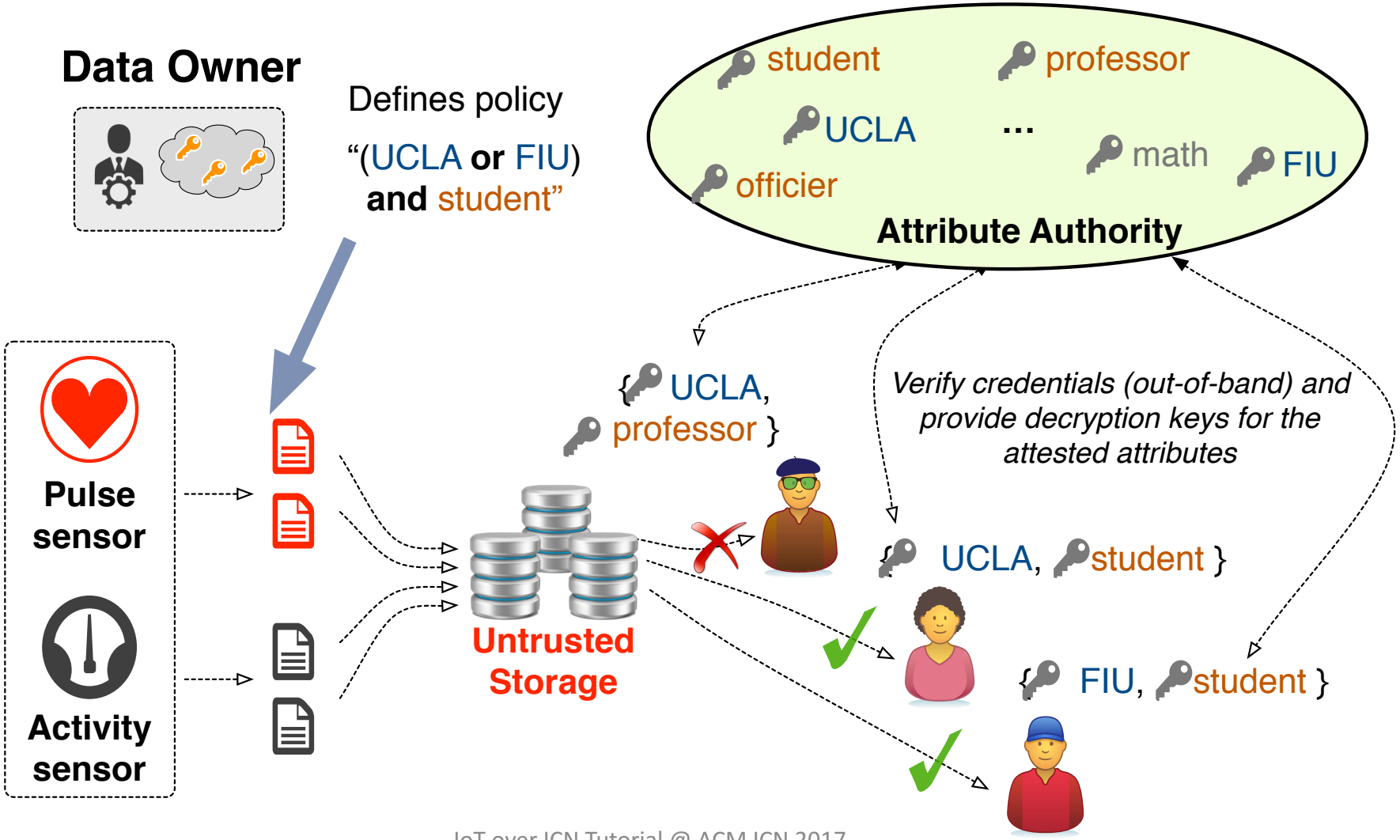
/FIU/Parking/PG-4/Level1/Sensor/**CKEY/1**

/FIU/Parking/PG-6/Level2/Sensor/**CKEY/42**

/FIU/Parking/PG-4/Level1/Sensor/**CKEY/1**
/ENCRYPTED-BY/FIU/Parking

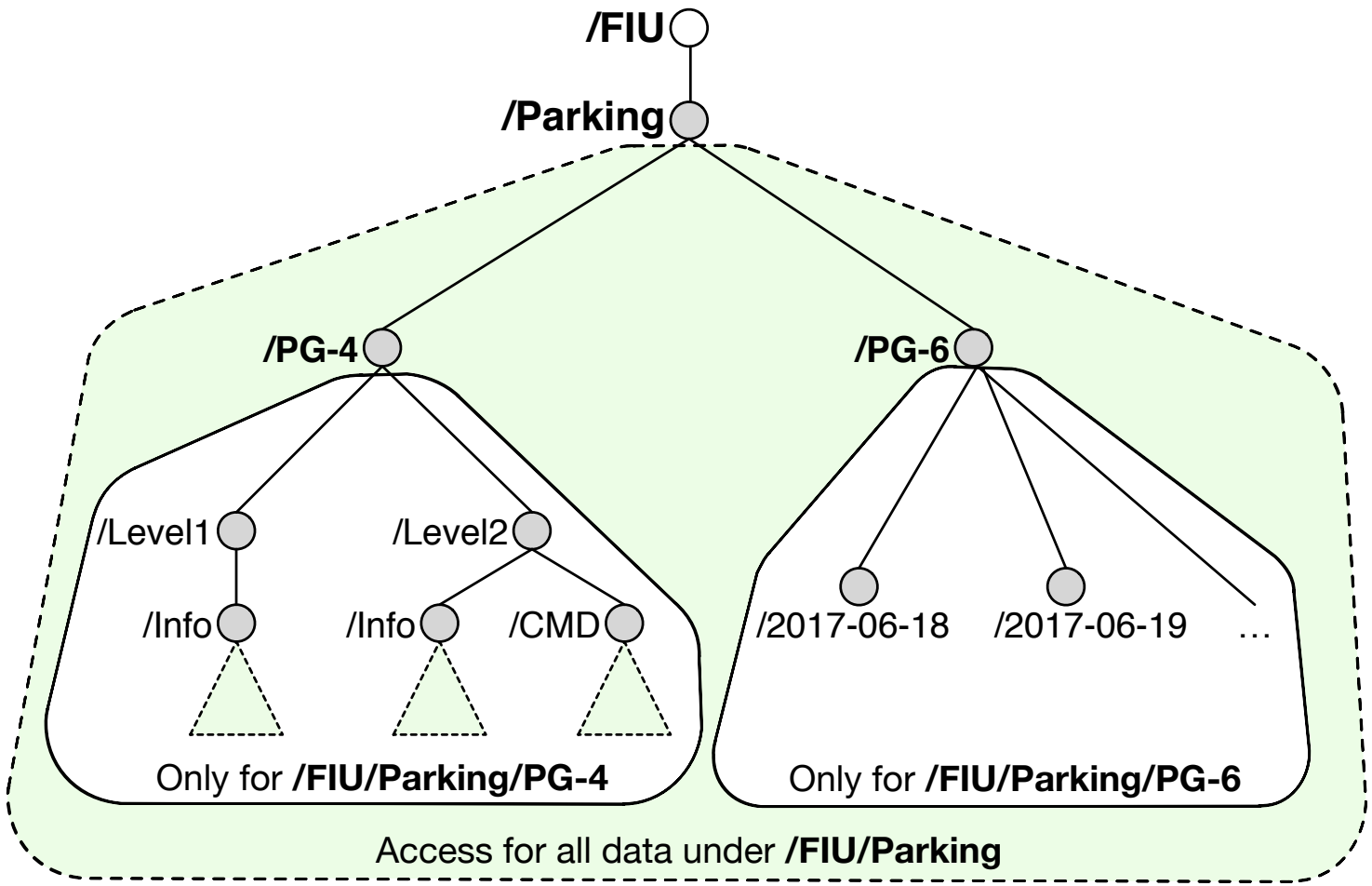
/FIU/Parking/**DKEY/1**
/ENCRYPTED-BY/FIU/Faculty/CIS/**Alex**

NAC with Attribute-Based Encryption



Control Granularity

- Naming conventions to leverage hierarchical scopes for read and write access
- Based on data type
  - PG-4 vs PG-6
  - Level1 vs Level2
- Based on data attributes
  - Time
  - Location



Takeaway Points

- NDN: an enabler for boosting secure, reliable, yet simple edge networking
- Key idea: letting network and applications share the same namespace
  - Enabling ad hoc, DTN communication via established namespace
  - Integrating networking, storage, processing via named data
  - Directly securing data
  - Leveraging names of data and keys
    - To define trust schema for distributed authentication and authorization
    - To define groups and access permissions in distributed (decentralized) way