Named Data Networking (Part 2)

Intel/NSF ICN-WEN Kickoff Workshop Tutorial

June 21, 2017, Hilsboro, OR

NAMED DATA NETWORKING

Alex Afanasyev and others
University of California, Los Angeles

Named Data Networking Communication Model

Interest packets

Name

Optional fields

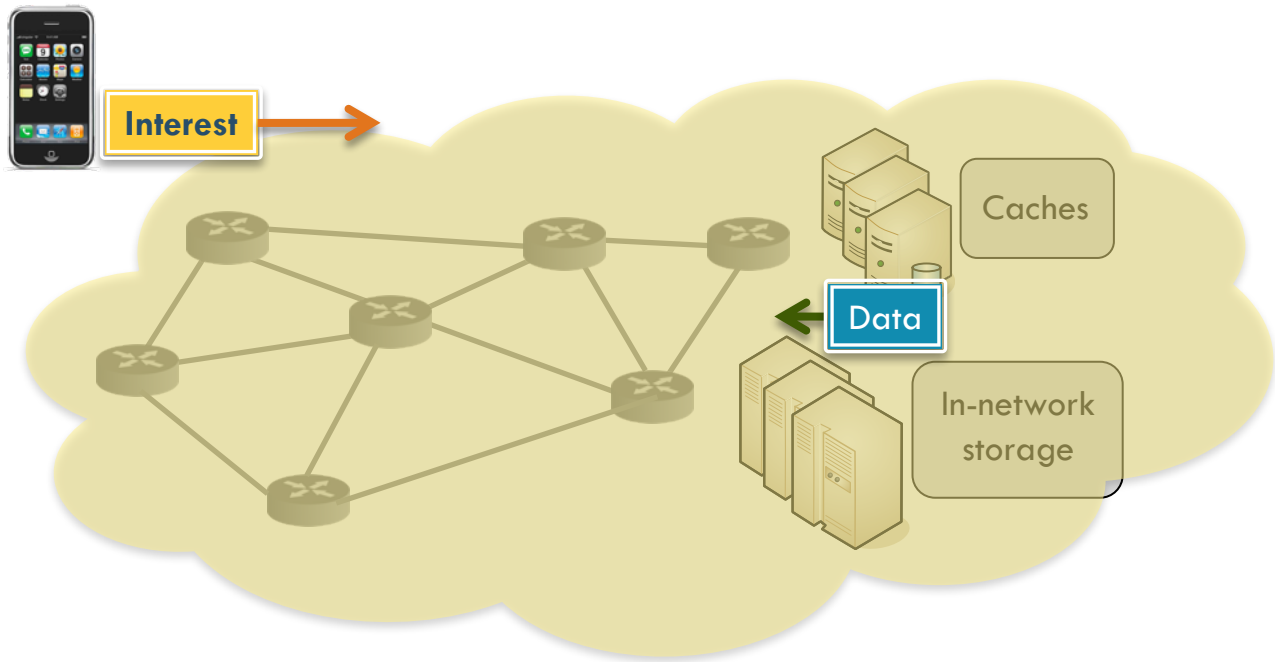
Data packets

Name

Content

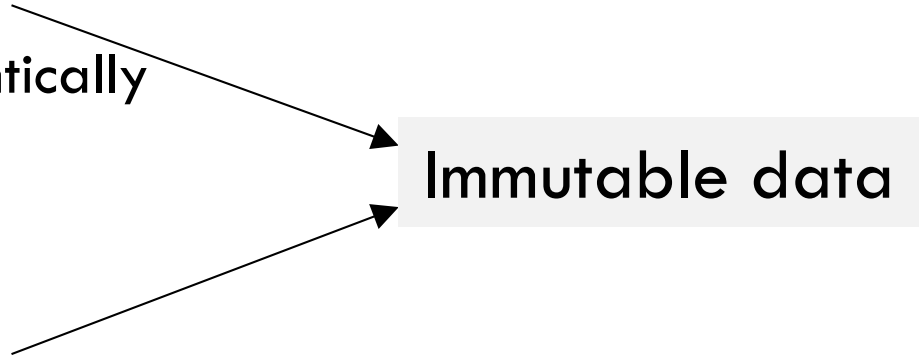
Signature

Building security principles into the networking architecture

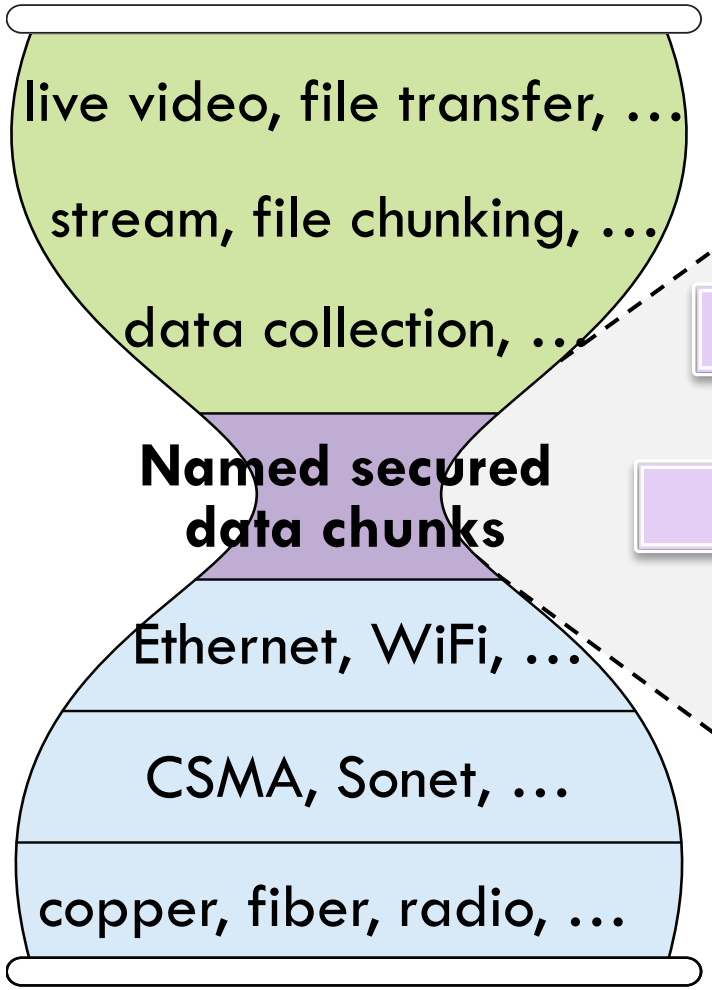


NDN: Just Three Simple Ideas

1. Per Interest, per hop forwarding state
   - → Creating closed feedback loop
     - Measure performance, detect failures
   - → Enabling multi-path forwarding
     - Add a strategy module to assist the forwarding decisions
2. Hierarchical naming of data
   - → Fetching data by application-defined, semantically meaningful names
3. Securing every data packet
   - → Removing dependency on transport security



Application-Defined, Semantically Meaningful Names for All Data Packets



Raw frames of video feed — **/UCLA/Campus/RoyceHall** /ARFeed/**FrontView**/mp4/_frame=12/ _chunk=20

Commands to a projector — /**_thisRoom**/Projector/SHOW/…

Video frame analysis — /**FUN:**/SLAM/(/…/ARFeed/…) /…

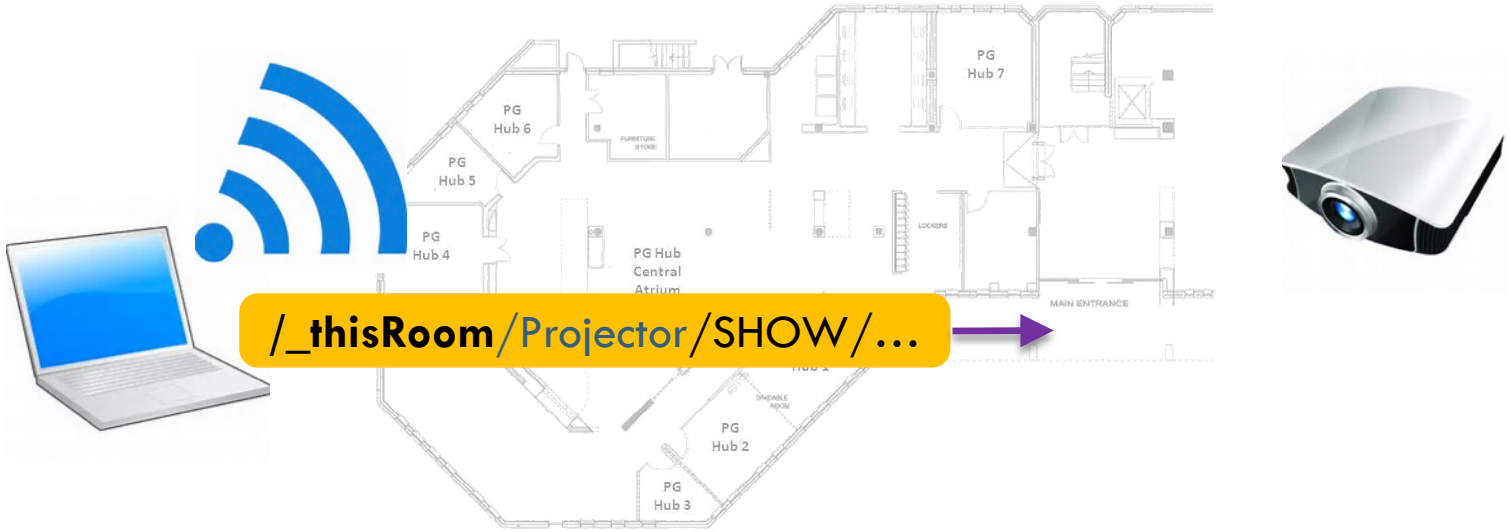
Parking lot information — /**UCLA**/Parking/**LOT8**/Info/…

Cryptographic keys — /**UCLA**/Faculty/HSEAS/CS /Alex/**BoelterHall**/KEY/_id=42

Fetching Data by Application Names enables

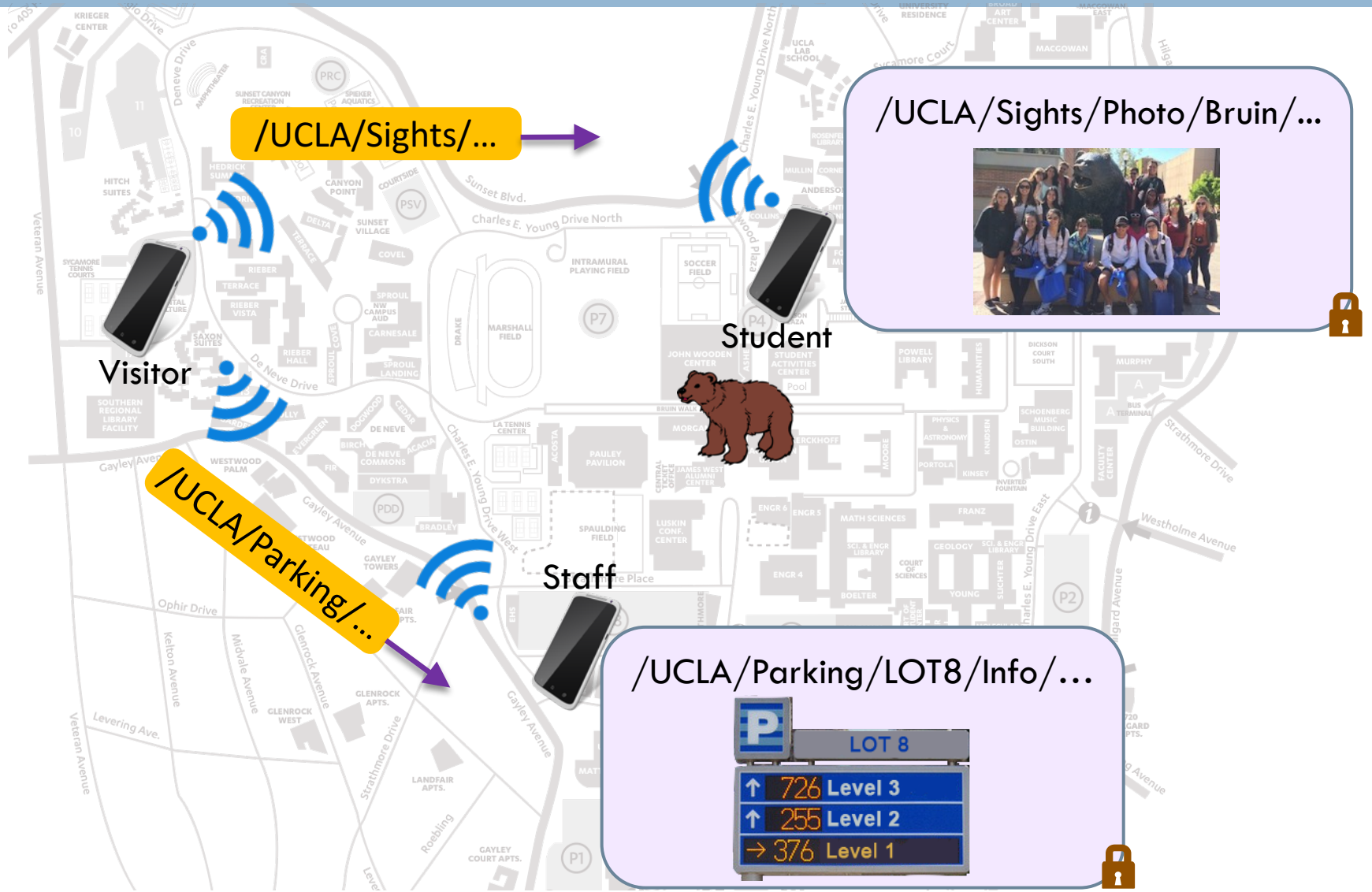
- Zero configuration and auto-discovery
- Seamless ad hoc communication
- Integration of computation, storage, networking
- Ability to use multiple interfaces at once
- And more

Zero Configuration and Auto Discovery



- Utilizing well defined naming conventions
  - "/**_thisRoom**": Interest carrying this prefix travels within local one room environment (e.g., one hop)
    - local: WiFi, Ethernet, etc; no long distance like LTE
  - "/Projector": identifies type of the device for which the interest is intended
    - Once projector located, may have further exchange on model/parameter details

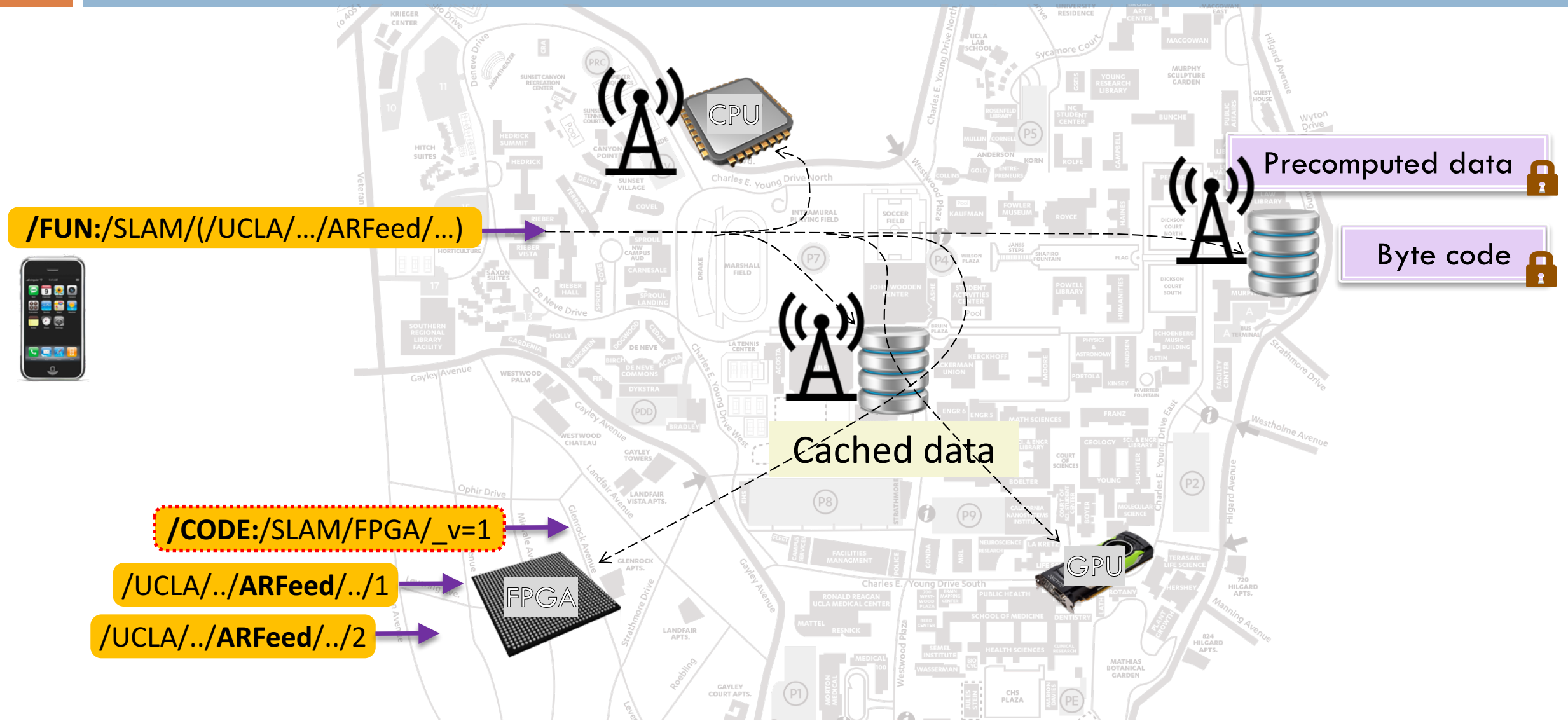
Seamless Ad Hoc Communication



Wi Fi DIRECT

Bluetooth

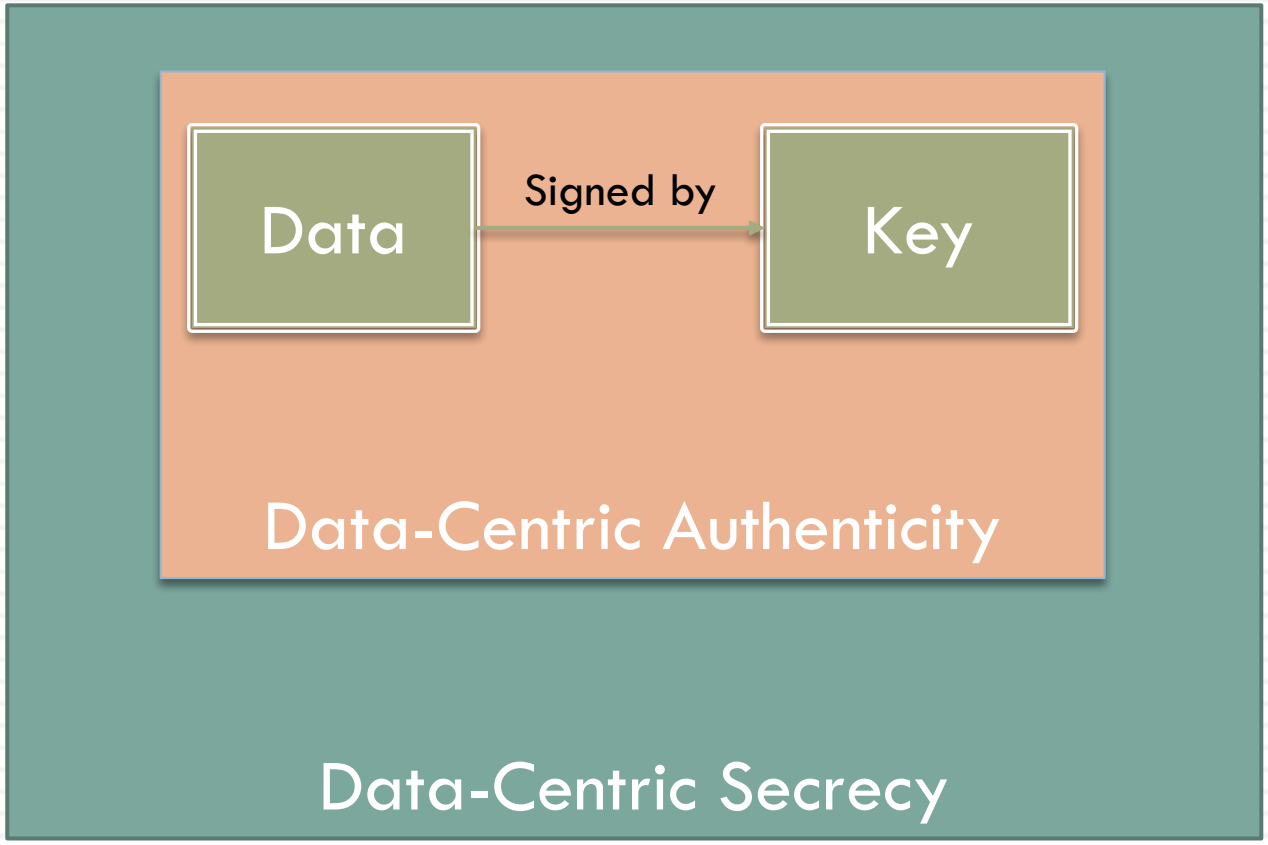
Integration of Networking, Storage & Computation



Use of Multiple Interfaces at Once

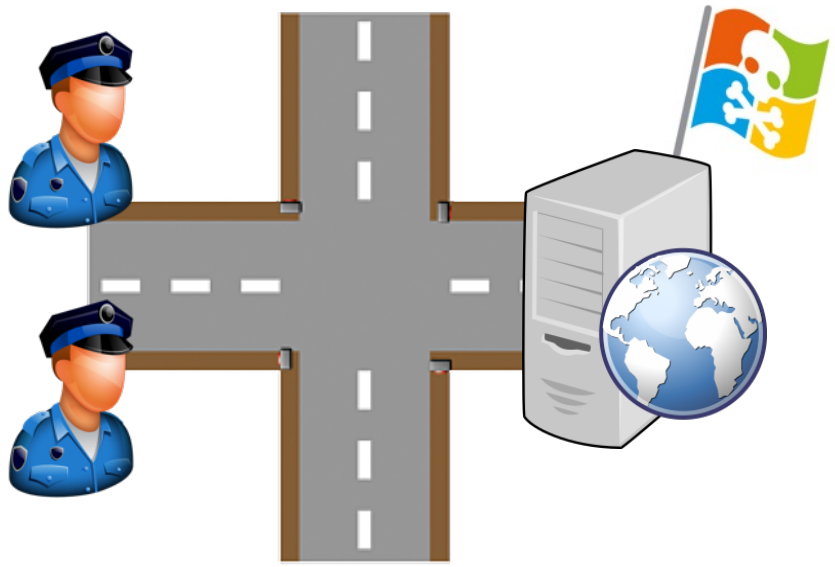
Data request by its name is independent of the link or location

Data-Centric Security of NDN

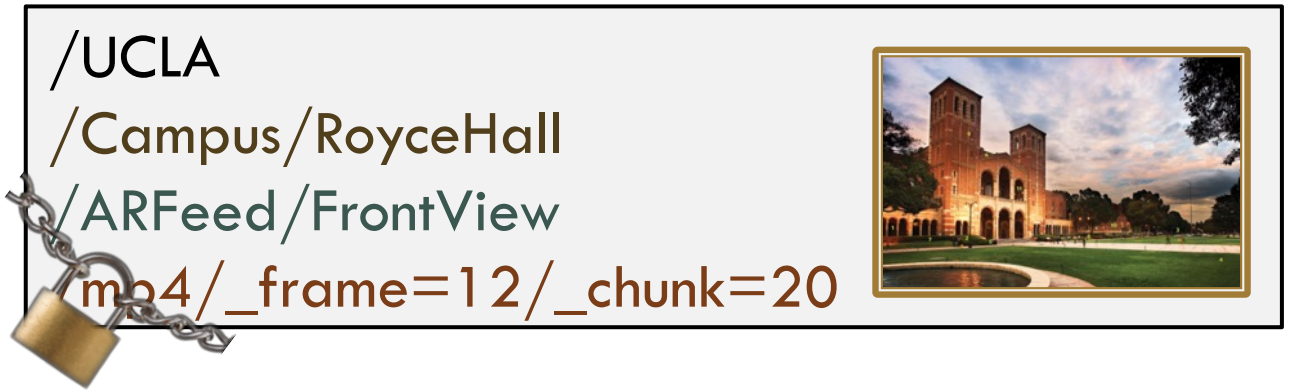


Built-In For Every Data Packet

- 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**



Authentication of NDN Data

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

Signed by

/UCLA
…/KEY

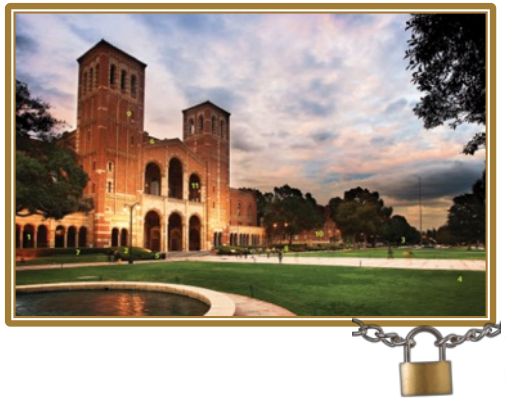
Signed by

KeyLocator: /UCLA/…/KEY

KeyLocator: /UCLA/…/KEY

Key Privilege Separation

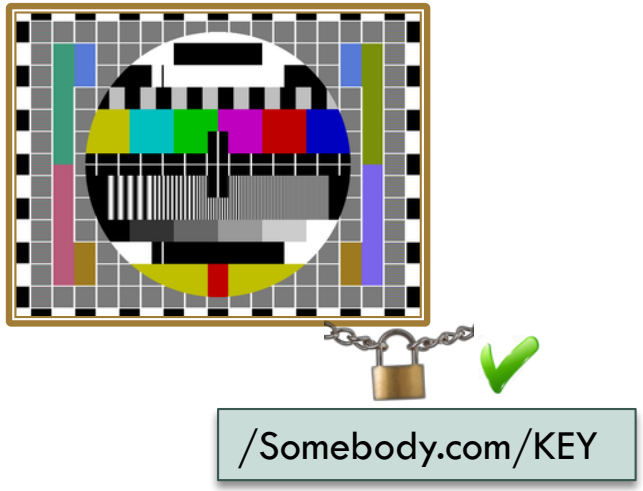
/UCLA/Campus/RoyceHall/ARFeed/FrontView
/mp4/_frame=12/_chunk=20



/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

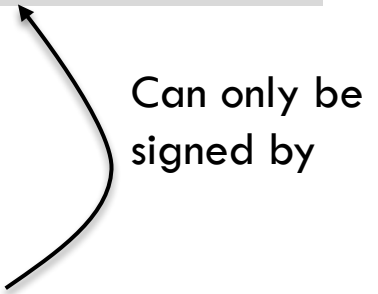


/Somebody.com/KEY

A forged frame

Name-Based Limit of Key Power

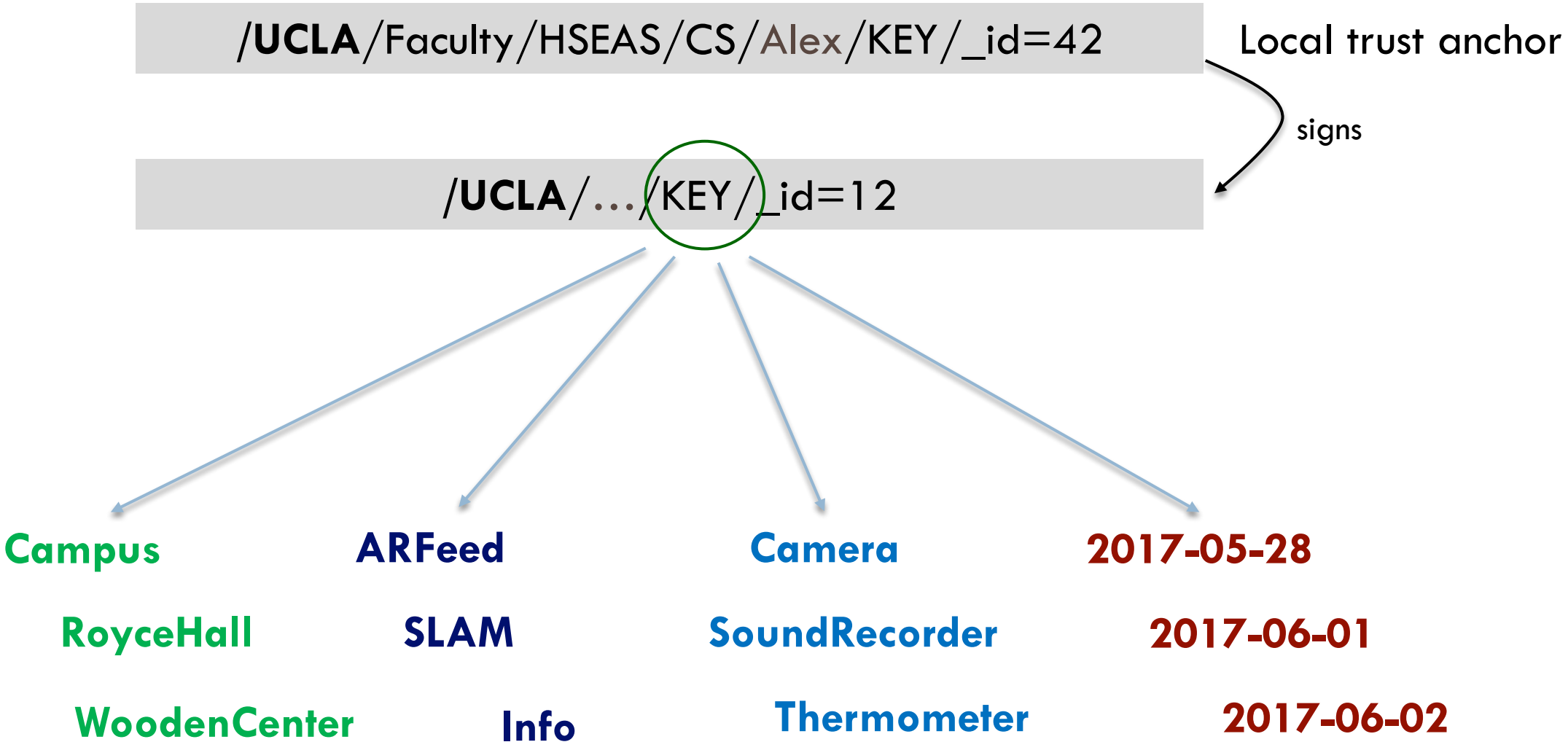
/**UCLA**/Campus/RoyceHall/**ARFeed**/…/mp4/_f=…/_s=…



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

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

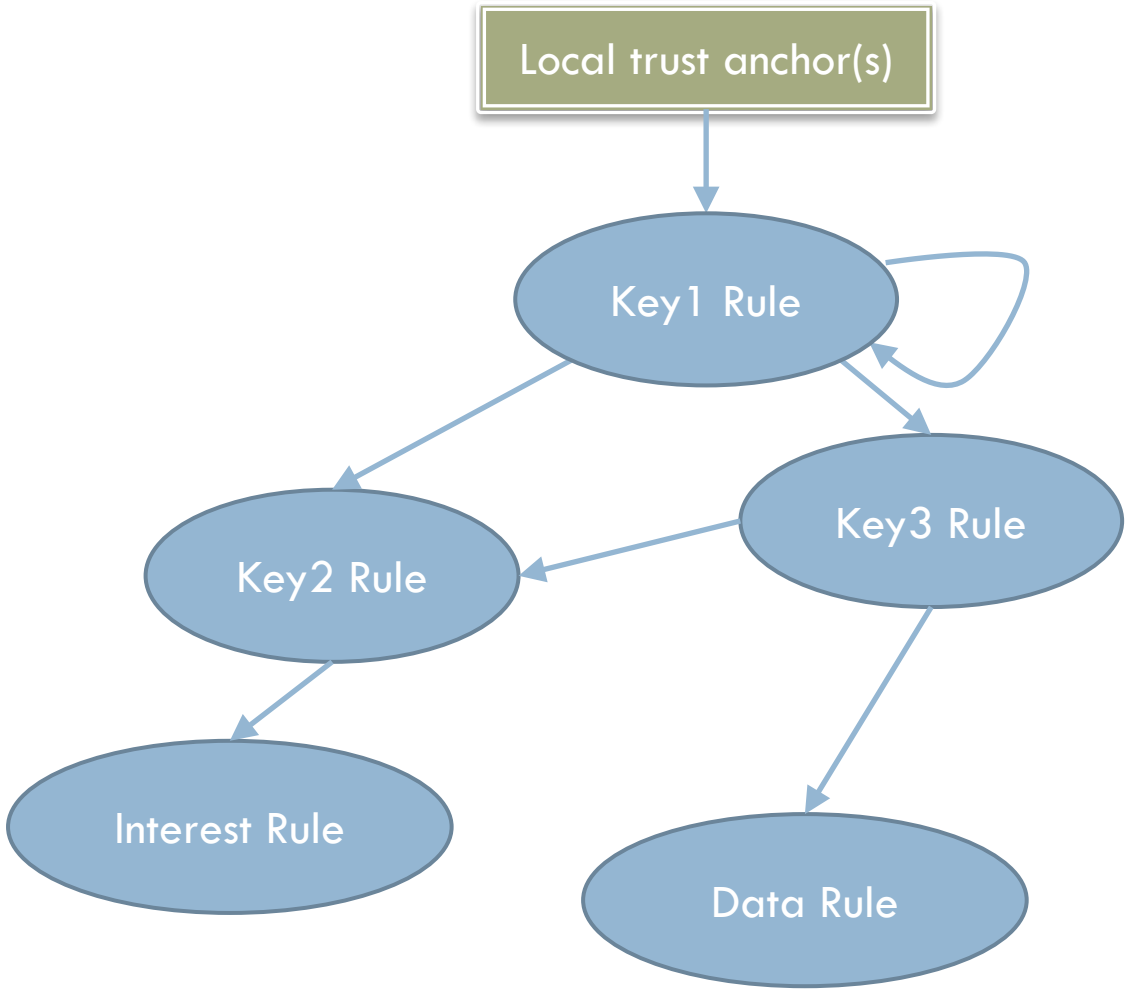
Flexible Restrictions through Namespace Design



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]

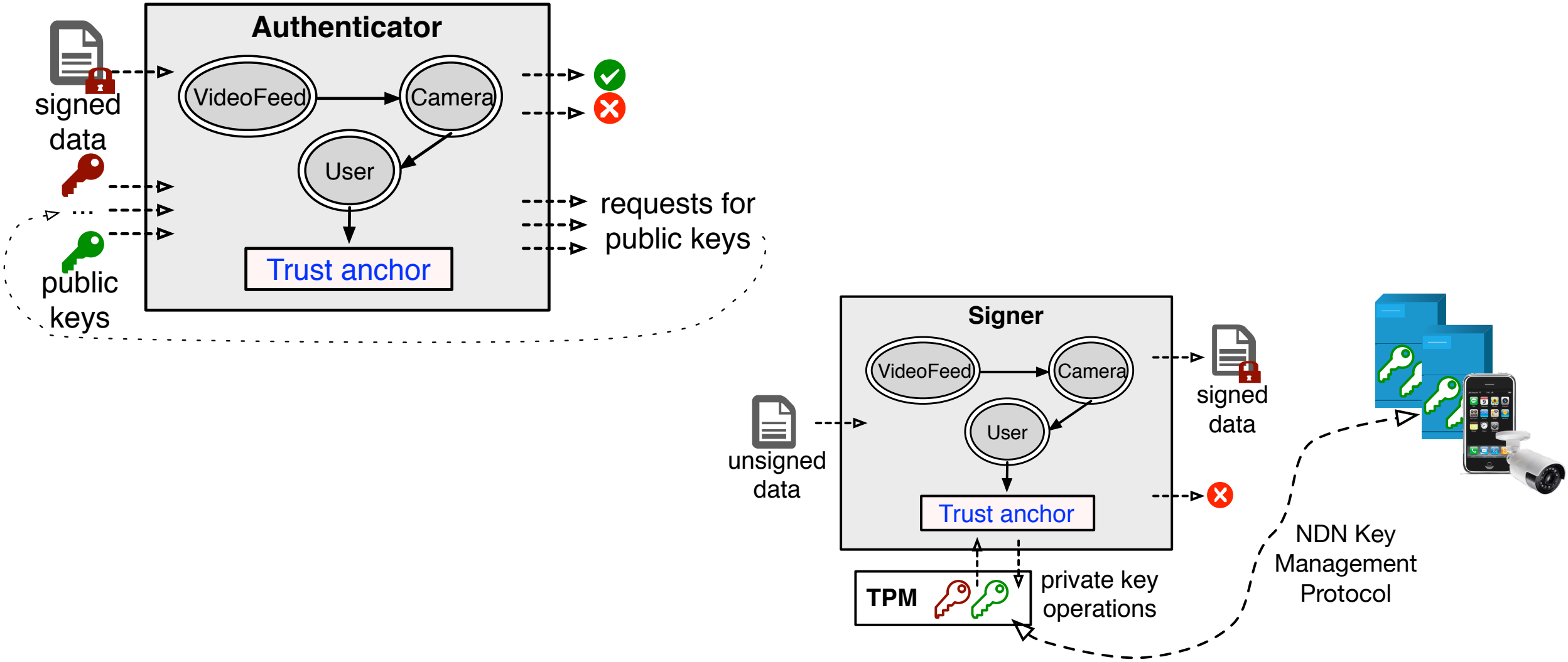
LocalAnchor(Prefix)

General Trust Model

/UCLA/KEY/_id=1

Trust Model Specialization for UCLA campus

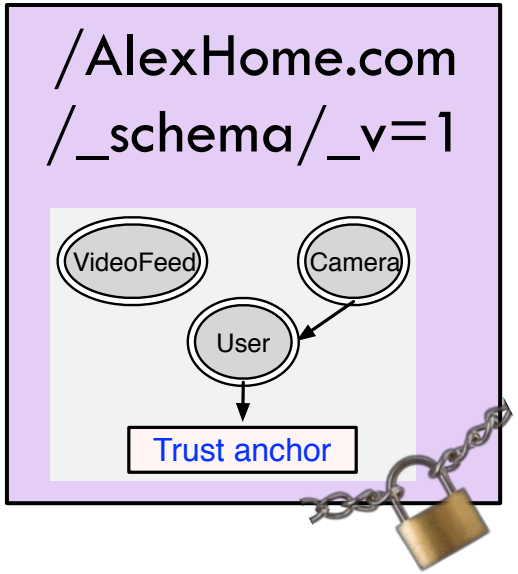
Trust Schema as an Automation Tool



Trust Schema as a Bag of Bits

- Can be distributed and updated using NDN mechanisms
- Secured as any other data packet

- Power of trust schema data
  - My phone can reliably validate the received video feed data
  - Camera can properly sign video feed data
  - Camera can validate commands from my phone
  - Routers can validate data and authorize requests



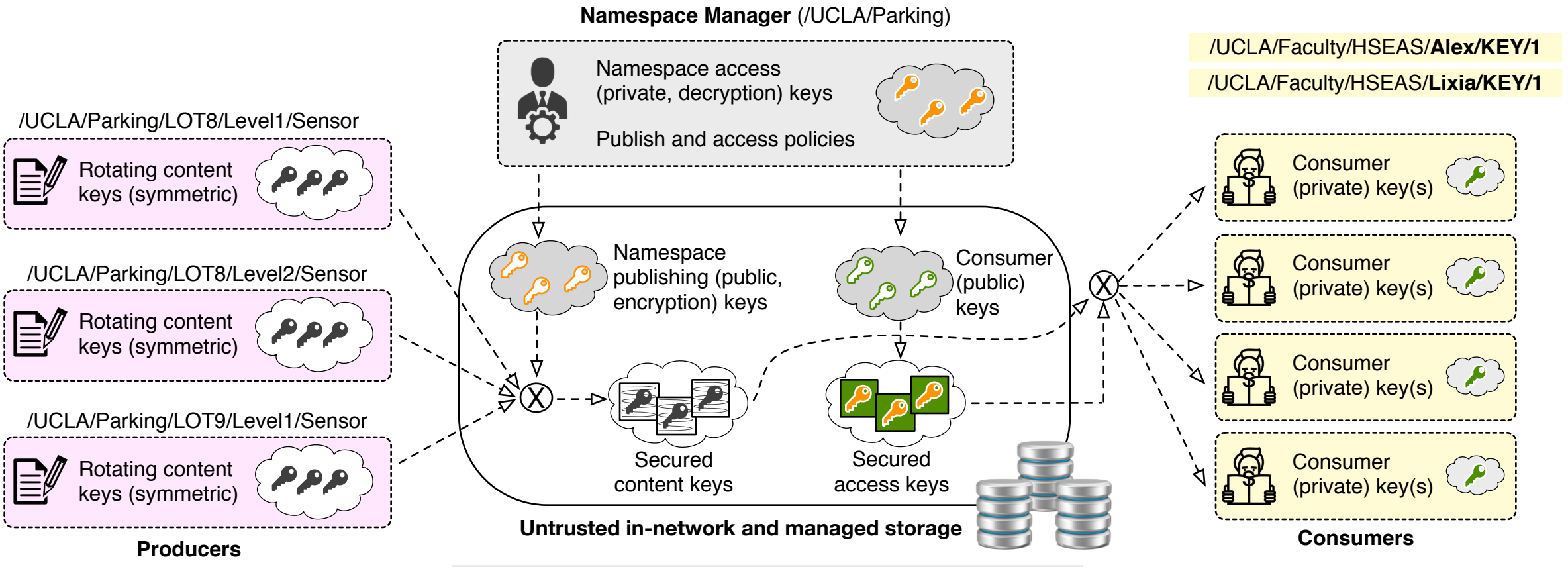
Data-Centric Secrecy

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

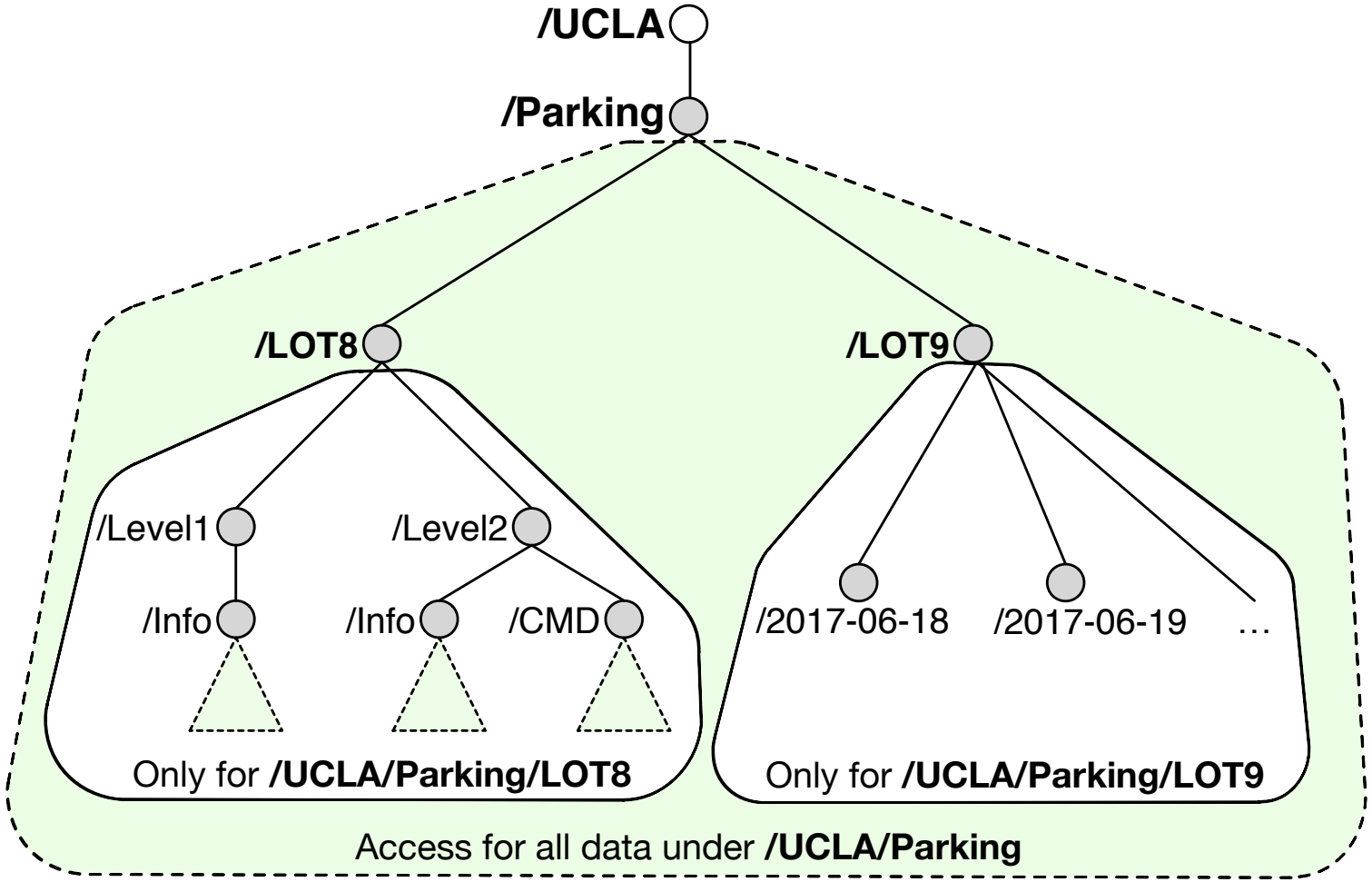
Name-Based Access Control



Control Granularity

- Naming conventions to leverage hierarchical scopes for read and write access

- Based on data type
  - LOT8 vs LOT9
  - Level1 vs Level2
- Based on data attributes
  - Time
  - Location



Takeaway Points

- NDN: a great 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