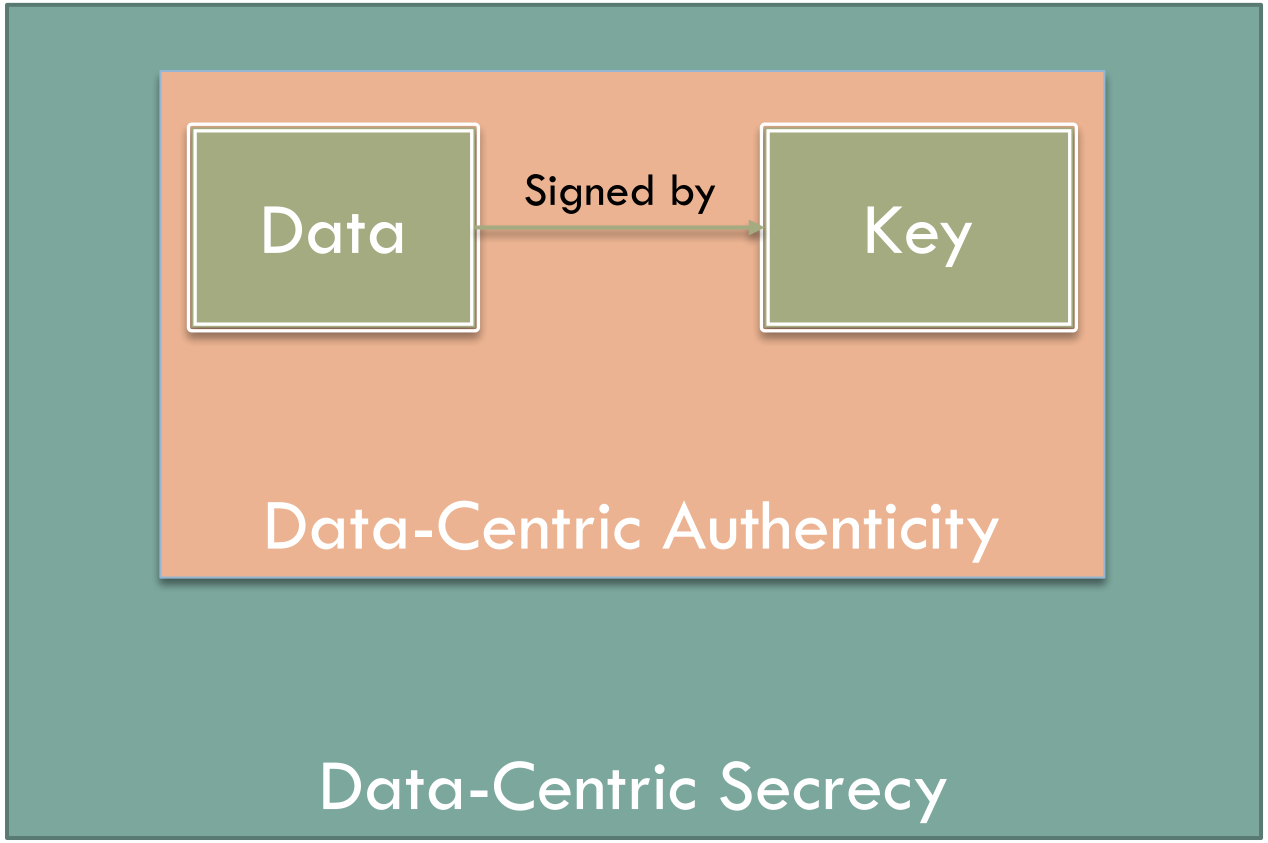
Named Data Networking of Things: **Trust Management for Autonomous Data-Centric Security**

NAMED DATA NETWORKING

Alex Afanasyev, Wentao Shang, Yingdi Yu, Jeff Burke, Lixia Zhang, and others
UCLA

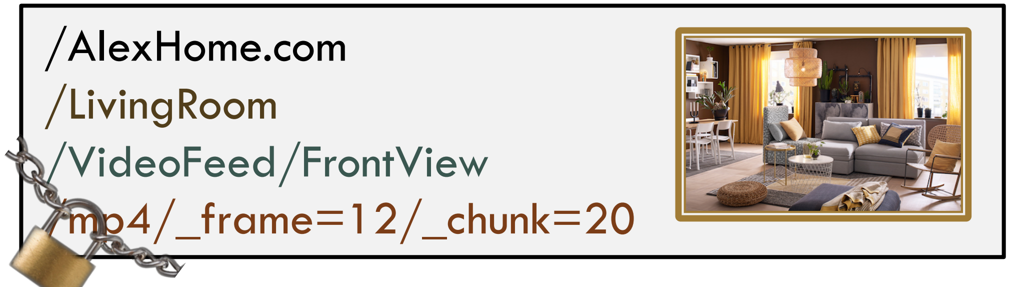
Data-Centric Security in NDN



Availability
Authenticity
Confidentiality

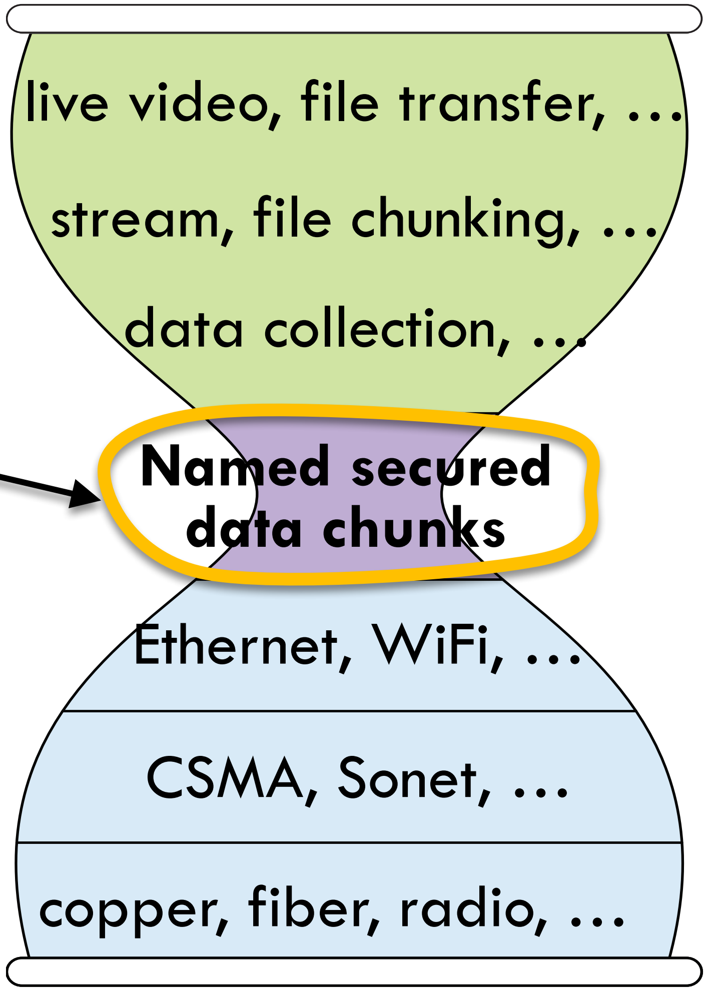
Named Data Networking: Built-in Security

- □ Hierarchically structured names, shared between application and network layers
- □ Security
  - Built-in into the networking layer



/AlexHome.com
/LivingRoom
/VideoFeed/FrontView
/mp4/_frame=12/_chunk=20

- □ Focus on application data
  - **Data secured in motion and at rest**
- □ Universal mechanism
  - Same security mechanisms for networking, transport, and application layers



live video, file transfer, …

stream, file chunking, …

data collection, …

Named secured data chunks

Ethernet, WiFi, …

CSMA, Sonet, …

copper, fiber, radio, …

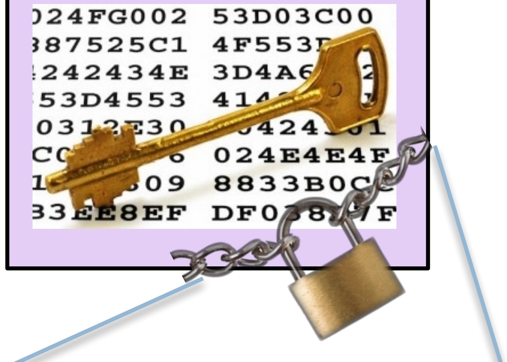
How NDN's Data-Centric Authenticity Works?

/AlexHome.com
/LivingRoom
/VideoFeed/FrontView
/mp4/_frame=12/_chunk=20

Signed by

KeyLocator: /AlexHome.com/…/KEY

/AlexHome.com
…/KEY



Signed by

KeyLocator: /AlexHome.com/…/KEY

Not Just One Key

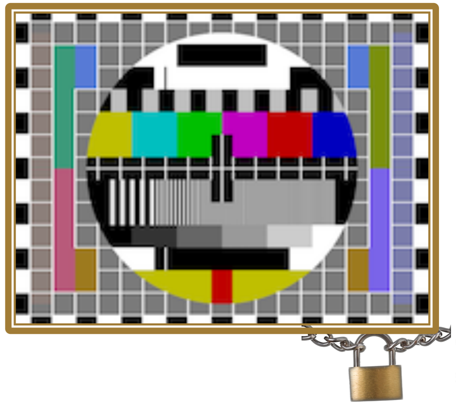
/**AlexHome.com**/**LivingRoom**/VideoFeed
/**FrontView**/mp4/_frame=12/_chunk=20

✓

/AlexHome.com/Camera/KEY

✓ A frame from a camera I have installed in my living room

/**AlexHome.com**/**LivingRoom**/VideoFeed
/**FrontView**/mp4/_frame=42/_chunk=1

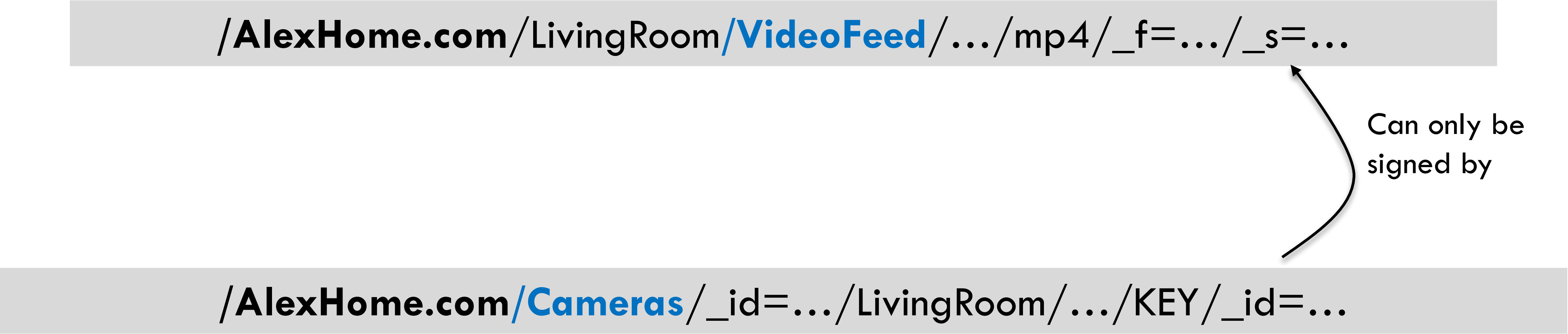


✓

/AlexHome.com/TV/KEY

TV incorrectly trying to publish living room feed ✗

Restricting Power of Keys



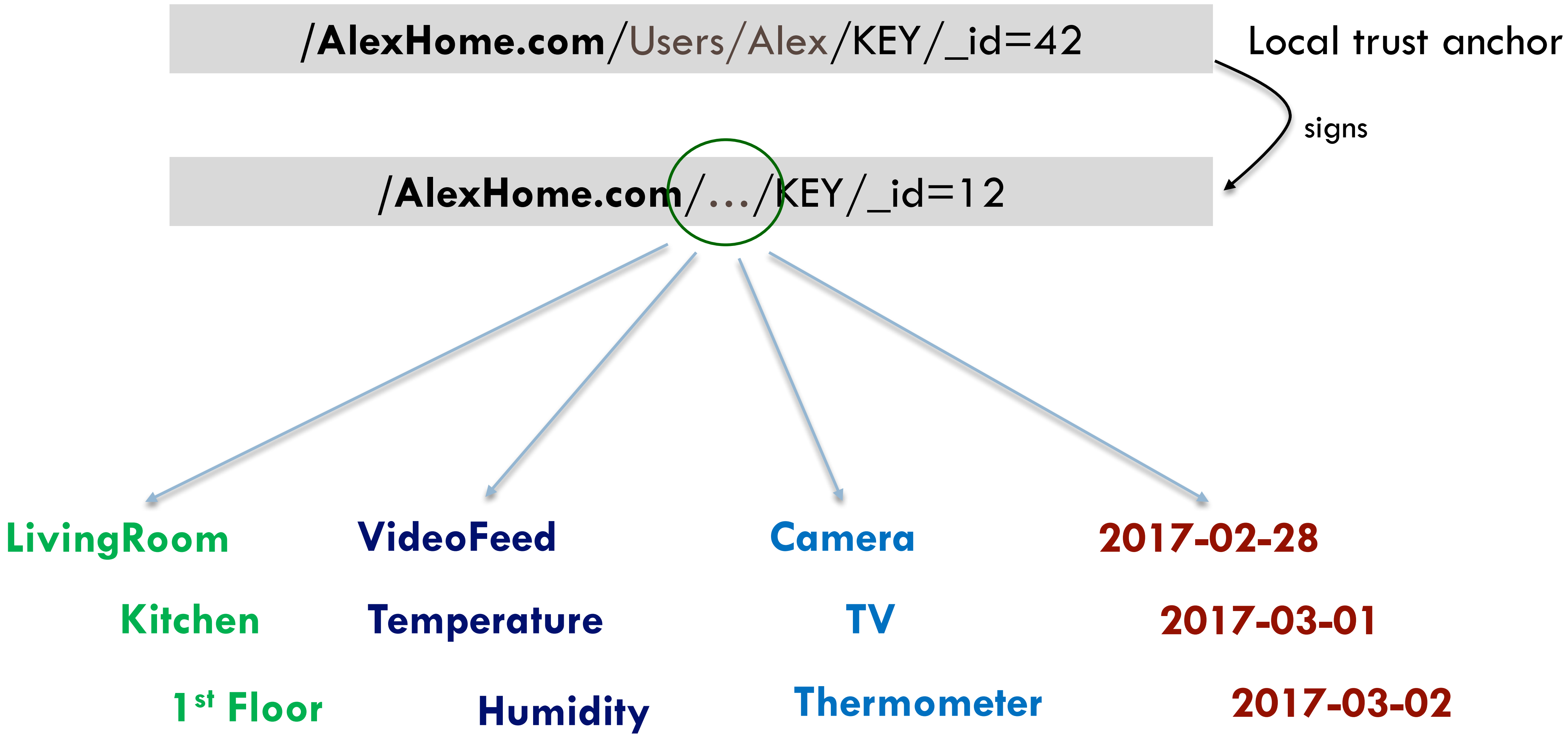
/**AlexHome.com**/LivingRoom/**VideoFeed**/…/mp4/_f=…/_s=…

Can only be signed by

/**AlexHome.com**/**Cameras**/_id=…/LivingRoom/…/KEY/_id=…

VideoFeed data to be valid, must be signed with a “Camera” key under the same name hierarchy

Defining Limits via Namespace Design



/**AlexHome.com**/Users/Alex/KEY/_id=42

Local trust anchor

signs

/**AlexHome.com**/…/KEY/_id=12

LivingRoom

Kitchen

1st Floor

VideoFeed

Temperature

Humidity

Camera

TV

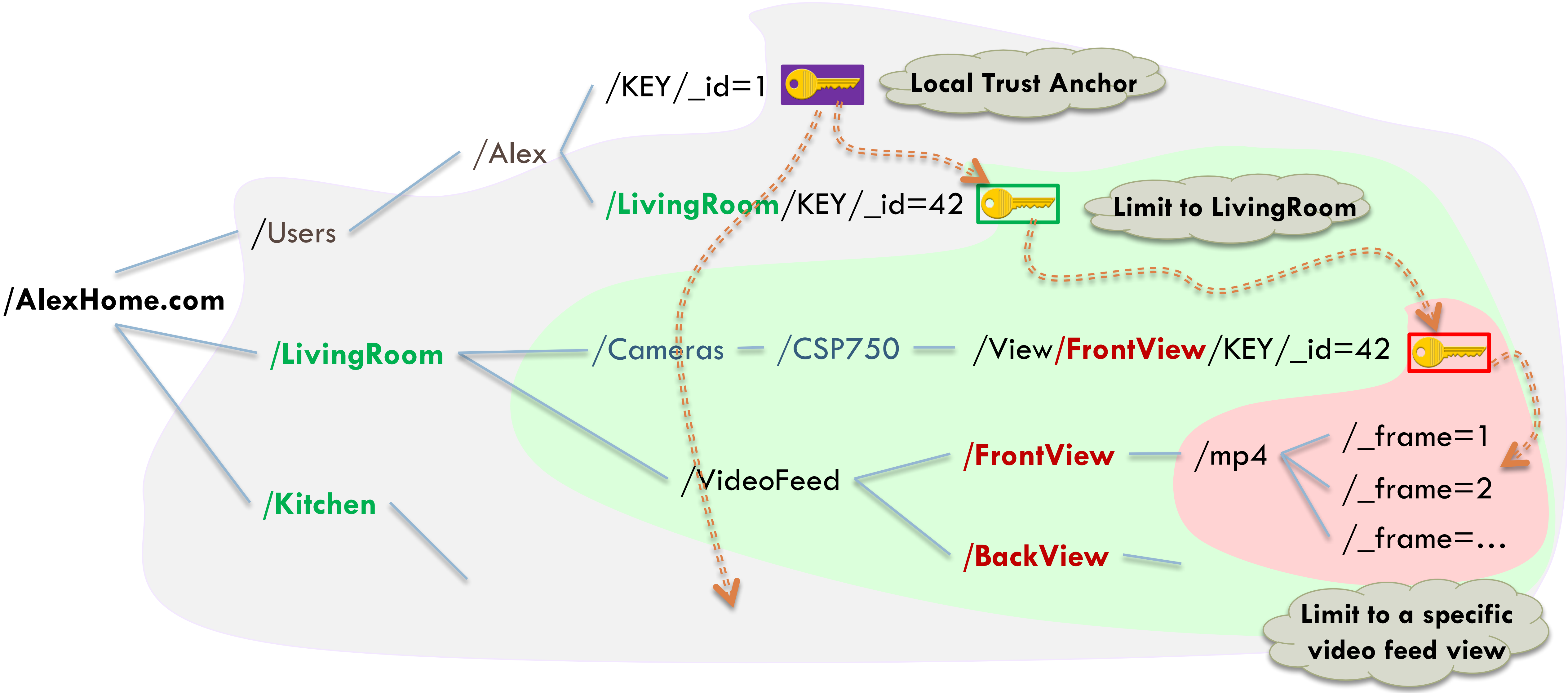
Thermometer

2017-02-28

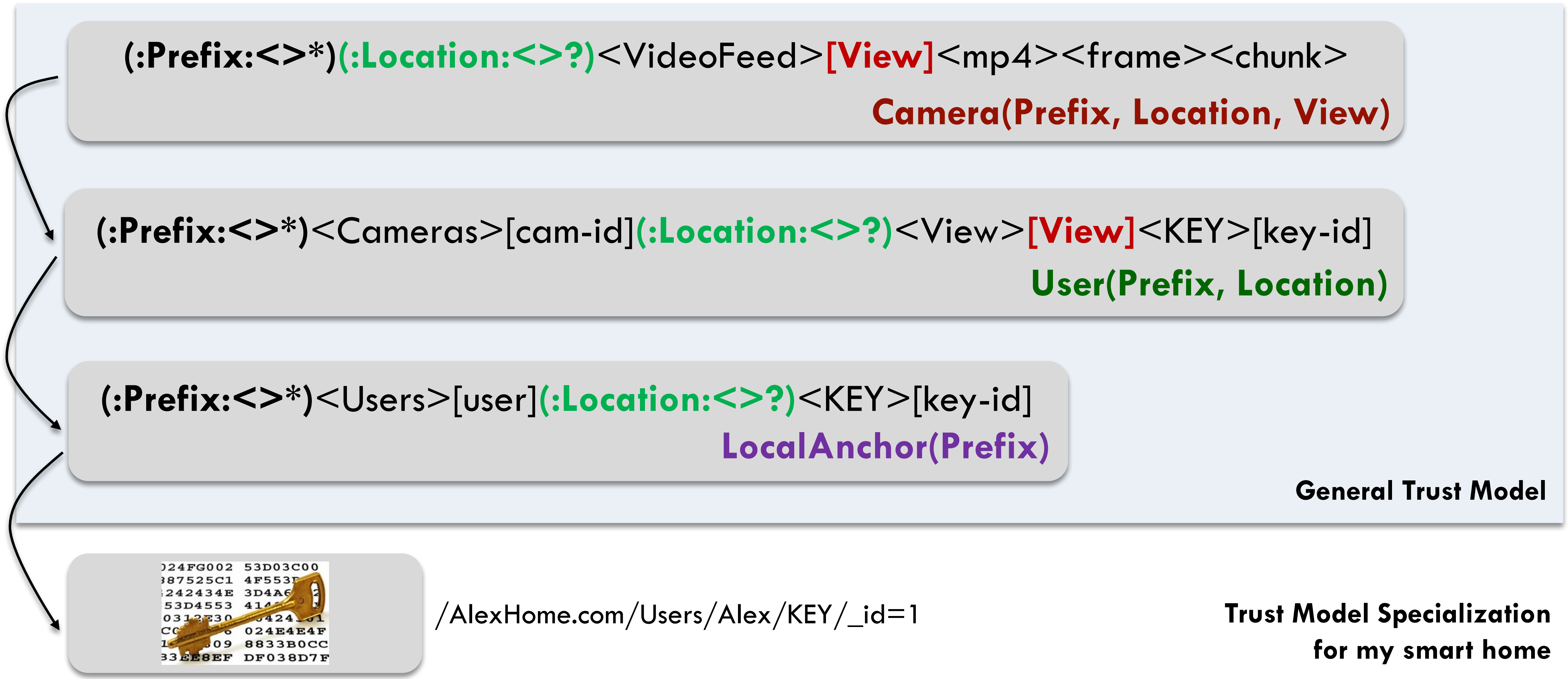
2017-03-01

2017-03-02

Privilege Separation Through Naming



Trust Schema: Name-Based Definition of Trust Model



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

Camera(Prefix, Location, View)

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

User(Prefix, Location)

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

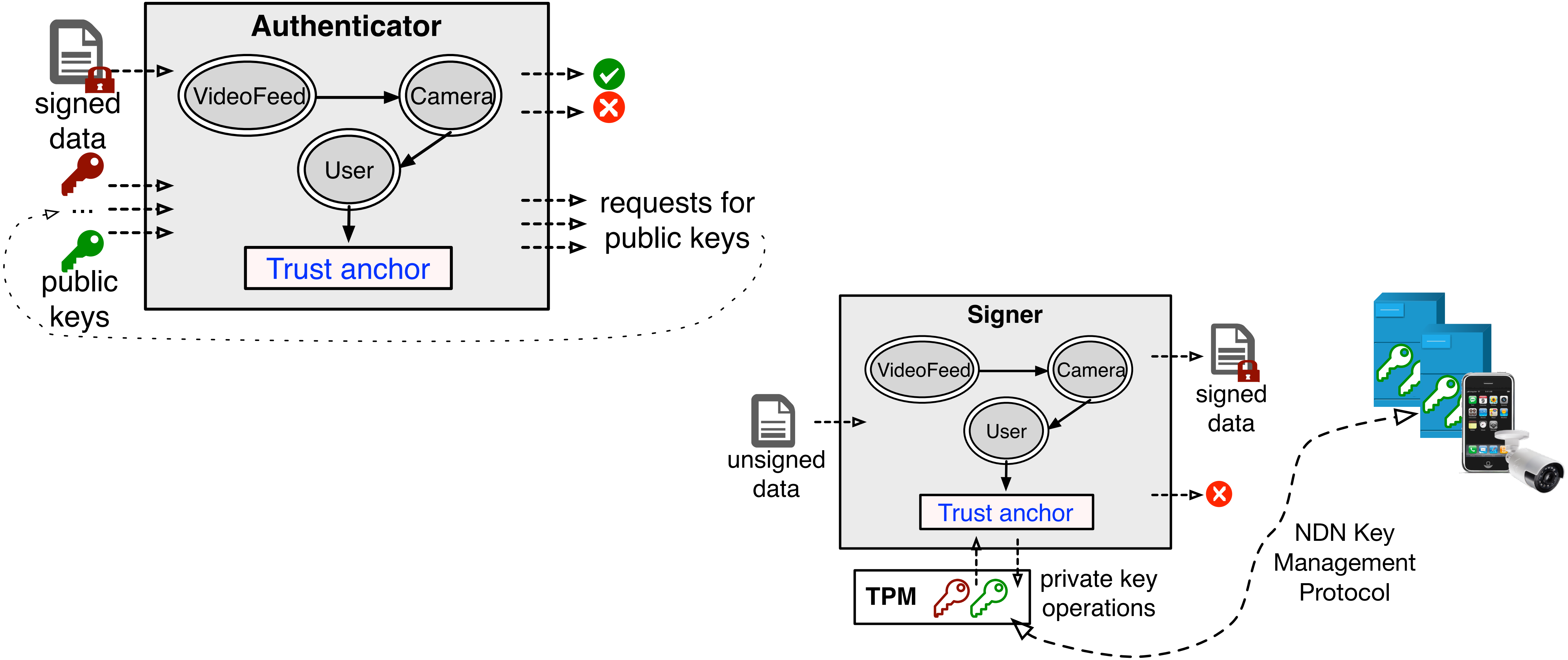
LocalAnchor(Prefix)

General Trust Model

/AlexHome.com/Users/Alex/KEY/_id=1

Trust Model Specialization for my smart home

Trust Schema as an Automation Tool



Automatic Signing With Trust Schema

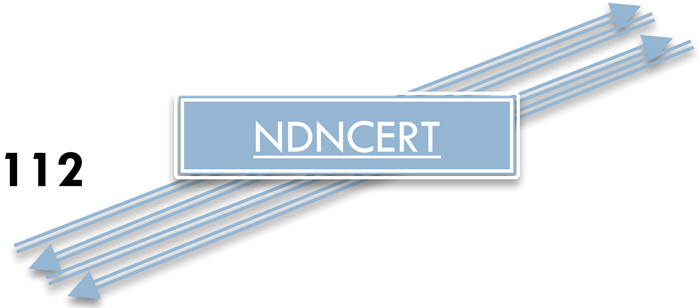
Local CA

/**AlexHome.com**/CA

Create Cert Request For

/**AlexHome.com**/Cameras/**CSP750**

/LivingRoom/View/**FronView**/KEY/**1112**

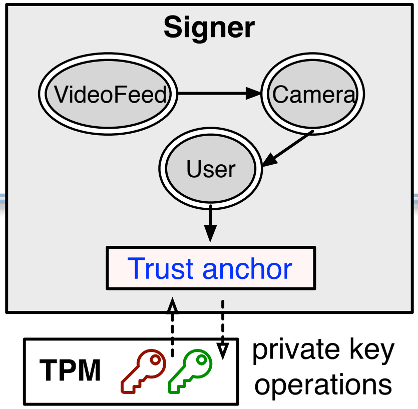


/AlexHome.com

/LivingRoom

/VideoFeed/FrontView

/mp4/_frame=12/_chunk=20

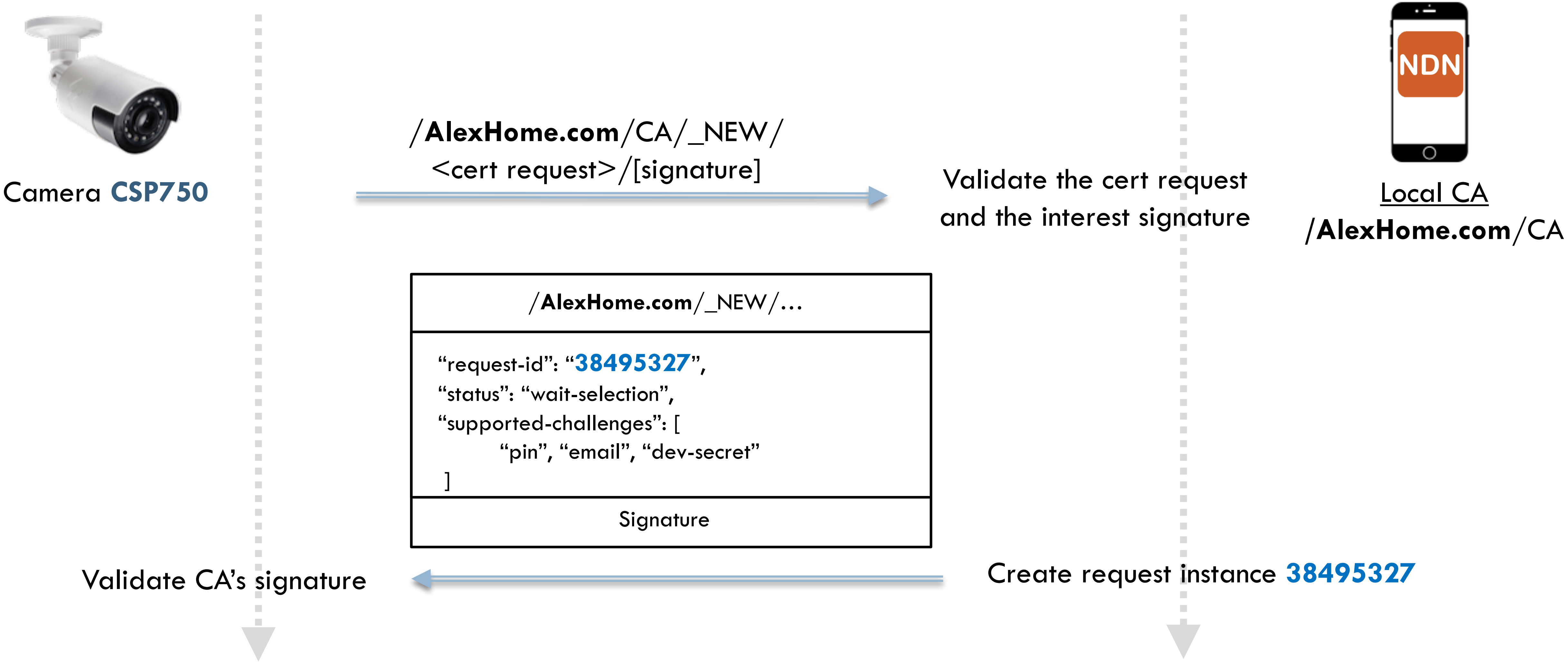


Need Key

/**AlexHome.com**/Cameras/[cam-id]

/LivingRoom/View/**FronView**/KEY/[key-id]

Automatic Request for NDN Certificate



Camera **CSP750**

/**AlexHome.com**/CA/_NEW/
<cert request>/[signature]

Validate the cert request
and the interest signature

<u>Local CA</u>
/**AlexHome.com**/CA

/**AlexHome.com**/_NEW/…

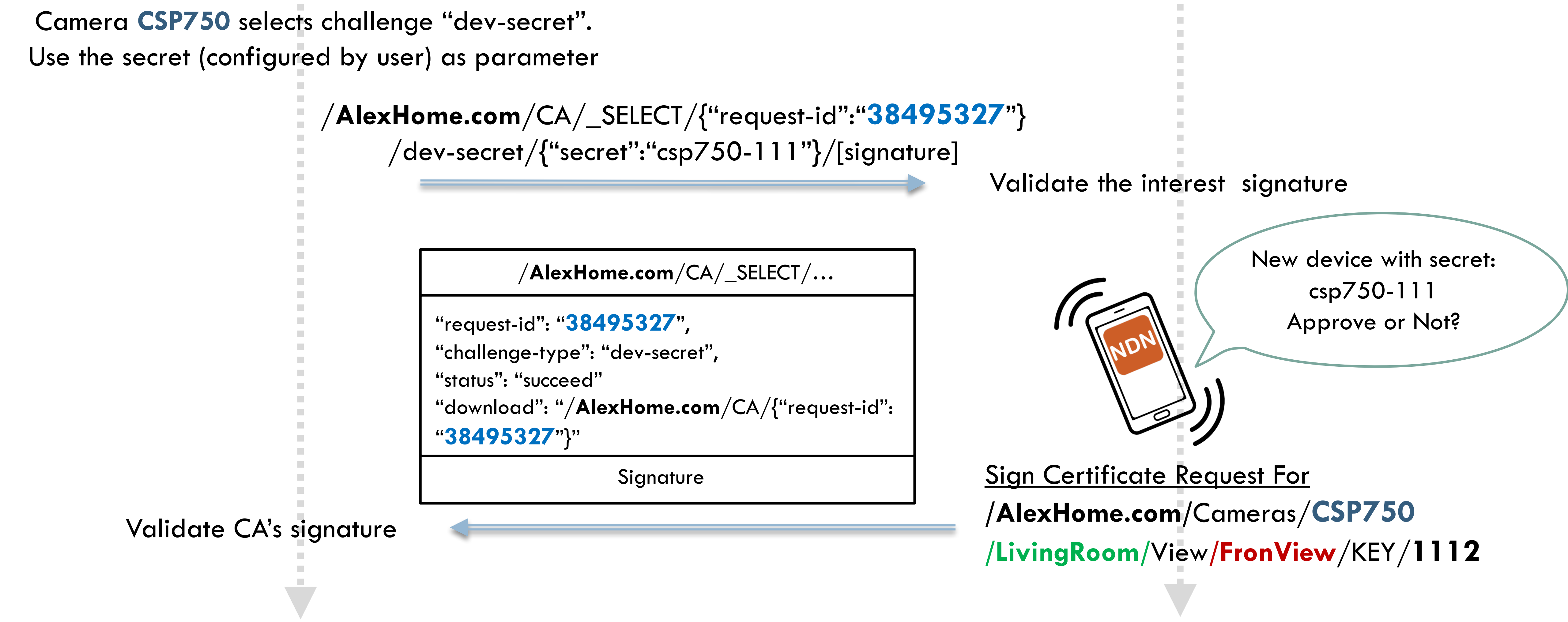
```
“request-id”: “38495327”,
“status”: “wait-selection”,
“supported-challenges”: [
        “pin”, “email”, “dev-secret”
 ]
```

Signature

Validate CA’s signature

Create request instance **38495327**

Certificate Approval



Camera **CSP750** selects challenge “dev-secret”.
Use the secret (configured by user) as parameter

/**AlexHome.com**/CA/_SELECT/{“request-id”:“**38495327**”}
/dev-secret/{“secret”:“csp750-111”}/[signature]

Validate the interest signature

/**AlexHome.com**/CA/_SELECT/…

“request-id”: “**38495327**”,
“challenge-type”: “dev-secret”,
“status”: “succeed”
“download”: “/**AlexHome.com**/CA/{“request-id”: “**38495327**”}”

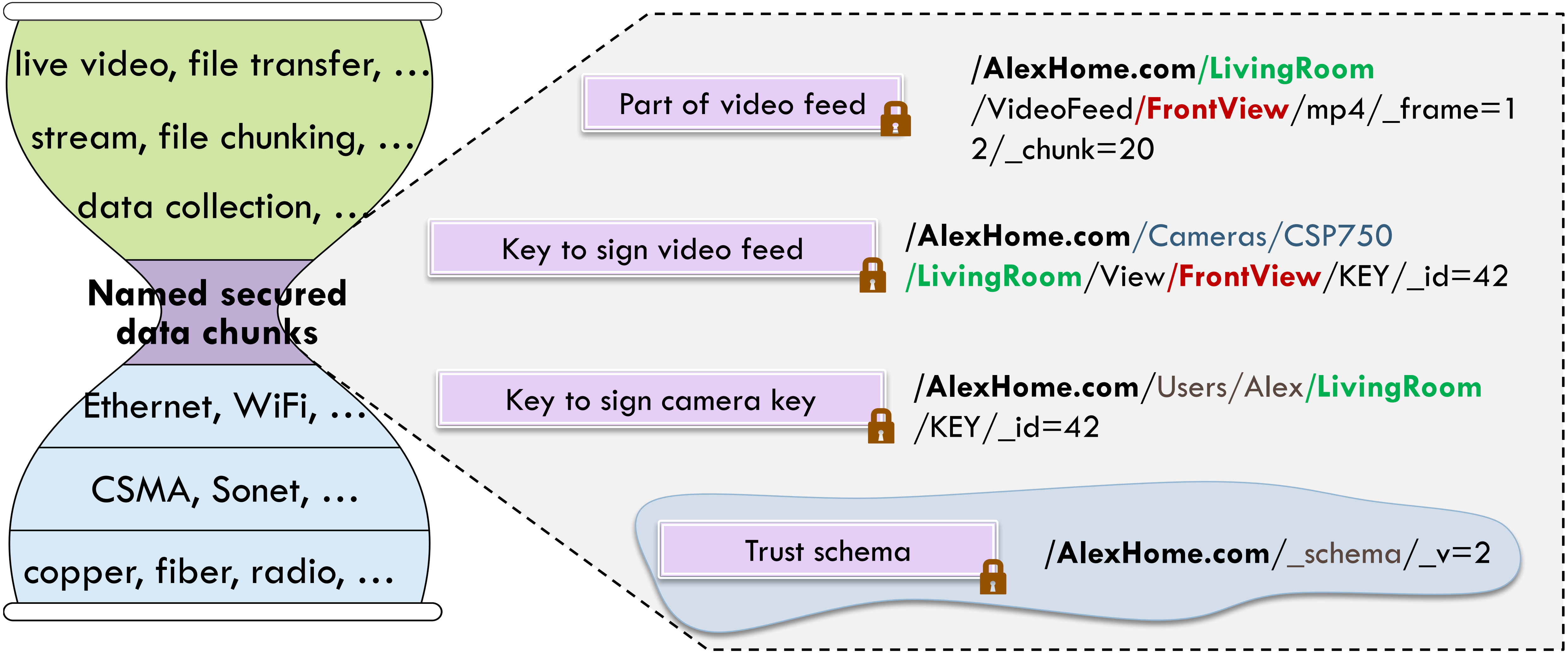
Signature

New device with secret:
csp750-111
Approve or Not?

Sign Certificate Request For
/**AlexHome.com**/Cameras/**CSP750**
/LivingRoom/View**/FronView**/KEY/**1112**

Validate CA’s signature

Every Bag of Bits is a Piece of Named Data



live video, file transfer, …

stream, file chunking, …

data collection, …

Named secured data chunks

Ethernet, WiFi, …

CSMA, Sonet, …

copper, fiber, radio, …

Part of video feed 🔒 — **/AlexHome.com**/LivingRoom/VideoFeed/**FrontView**/mp4/_frame=12/_chunk=20

Key to sign video feed 🔒 — **/AlexHome.com**/Cameras/CSP750/LivingRoom/View/**FrontView**/KEY/_id=42

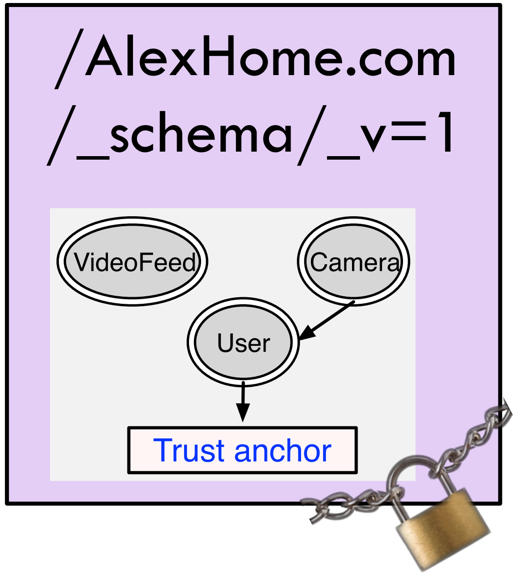
Key to sign camera key 🔒 — **/AlexHome.com**/Users/Alex/LivingRoom/KEY/_id=42

Trust schema 🔒 — **/AlexHome.com**/_schema/_v=2

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



/AlexHome.com/_schema/_v=1

Foundation for the Secure Autonomous Networking

Takeaway Points

- Internet-of-Things is booming, but is seriously impacted by limitations of IP
  - Mismatched application semantics
  - Patched up security
  - Critical dependencies on the cloud
- NDN provides a great solution to boost secure, reliable, yet simple IoT
  - Network and application use the same namespace
  - Security is built-in into every packet
  - Trust schema to “autonomously” manage trust
  - Certificate management to realize usable security