ERICSSON

Employing Attribute-Based Encryption in Systems with Resource Constrained Devices in an Information-Centric Networking Context

Global IoT Summit (GIoTS)
Geneva, June 6-9, 2017

Börje Ohlman
Ericsson Research

Joakim Borgh (SAAB), Edith Ngai (Uppsala University), Adeel Mohammad Malik (Ericsson Research)

SEVENTH FRAMEWORK PROGRAMME

ICN2020

ICN2020 Consortium

Georg-August-Universität Göttingen
(UGO, Germany)
EU Coordinator

NEC Europe Ltd.
(NEE, UK)

Universita' degli Studi di Roma
Tor Vergata
(URO, Italy)

Cisco Systems France Sarl
(CIS, France)

University College London
(UCL, UK)

Ericsson AB
(ERI, Sweden)

KDDI R&D Laboratories, Inc.
(KDD, Saitama)
Japanese Coordinator

Kozo Keikaku Engineering Inc.
(KKE, Japan)

Osaka City University
(OCU, Japan)

Osaka University
(UOS, Osaka)

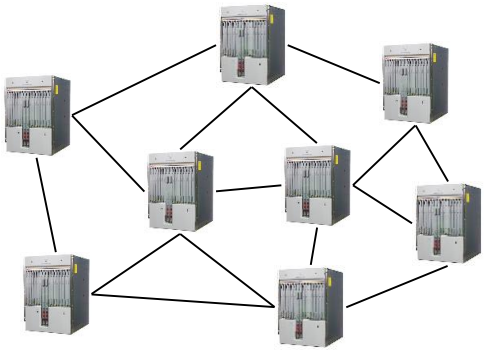
Institut de Recherche Technologique
SystemX
(SYX, France)

Outline

- ICN overview
- ABE overview
- Scenario & Testbed
- Results & Conclusions

Evolution of networking

Today's Internet
Focuses on
Conversations between Hosts
Host-centric abstraction
Who to communicate with



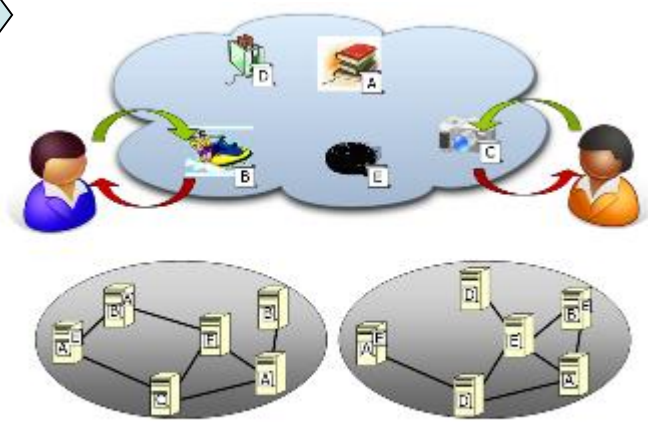
Evolution

Web

CDN

P2P

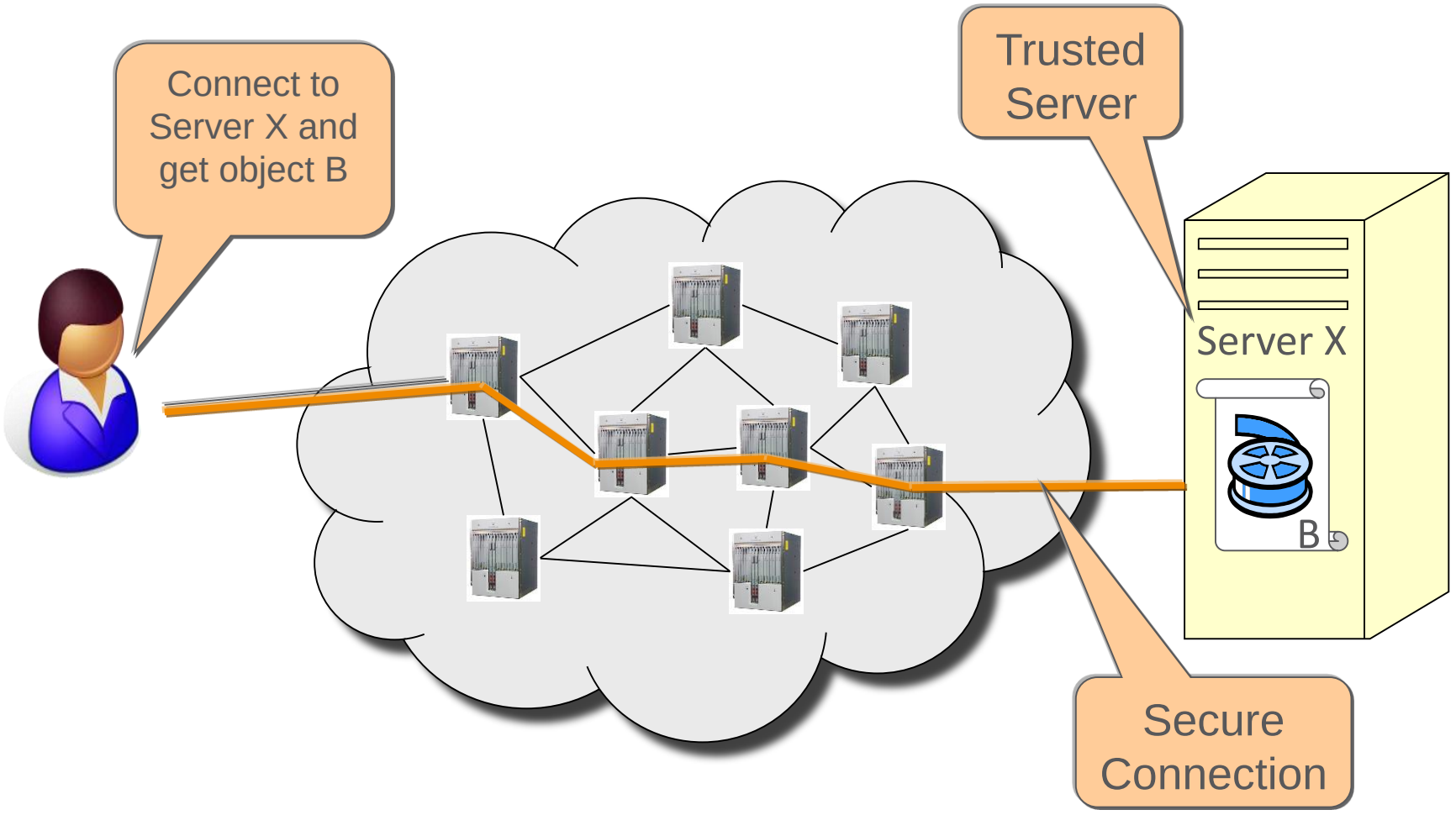
Information-centric network (ICN)
Focuses on
Dissemination of Information objects
Information-centric abstraction



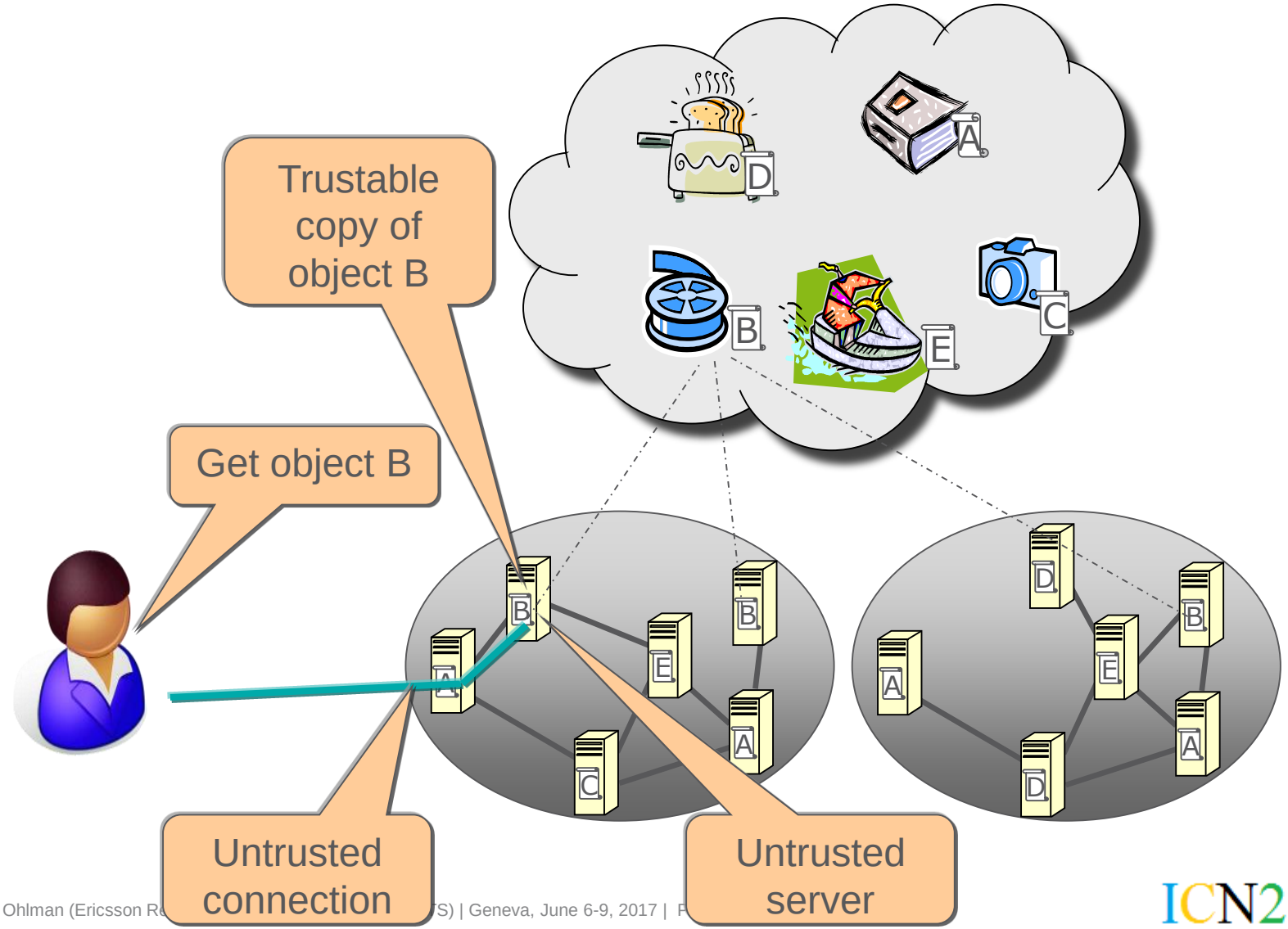
Major ICN approaches

- Content Centric Networking (CCN) / Named Data Networking (NDN)
- Network of Information (NetInf)
- Publish/Subscribe Networking (PSIRP / PURSUIT)

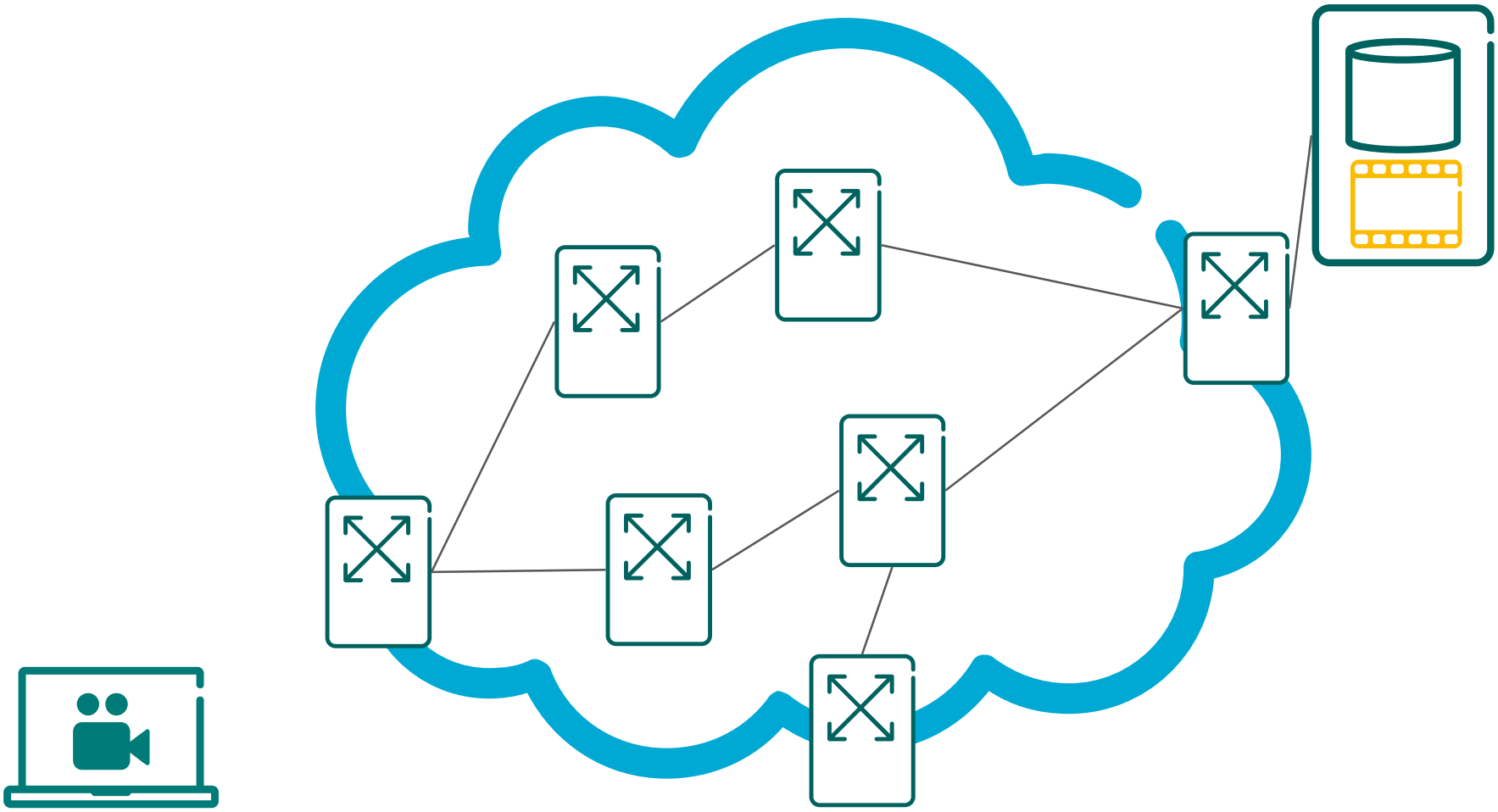
Security model in traditional node-centric networking



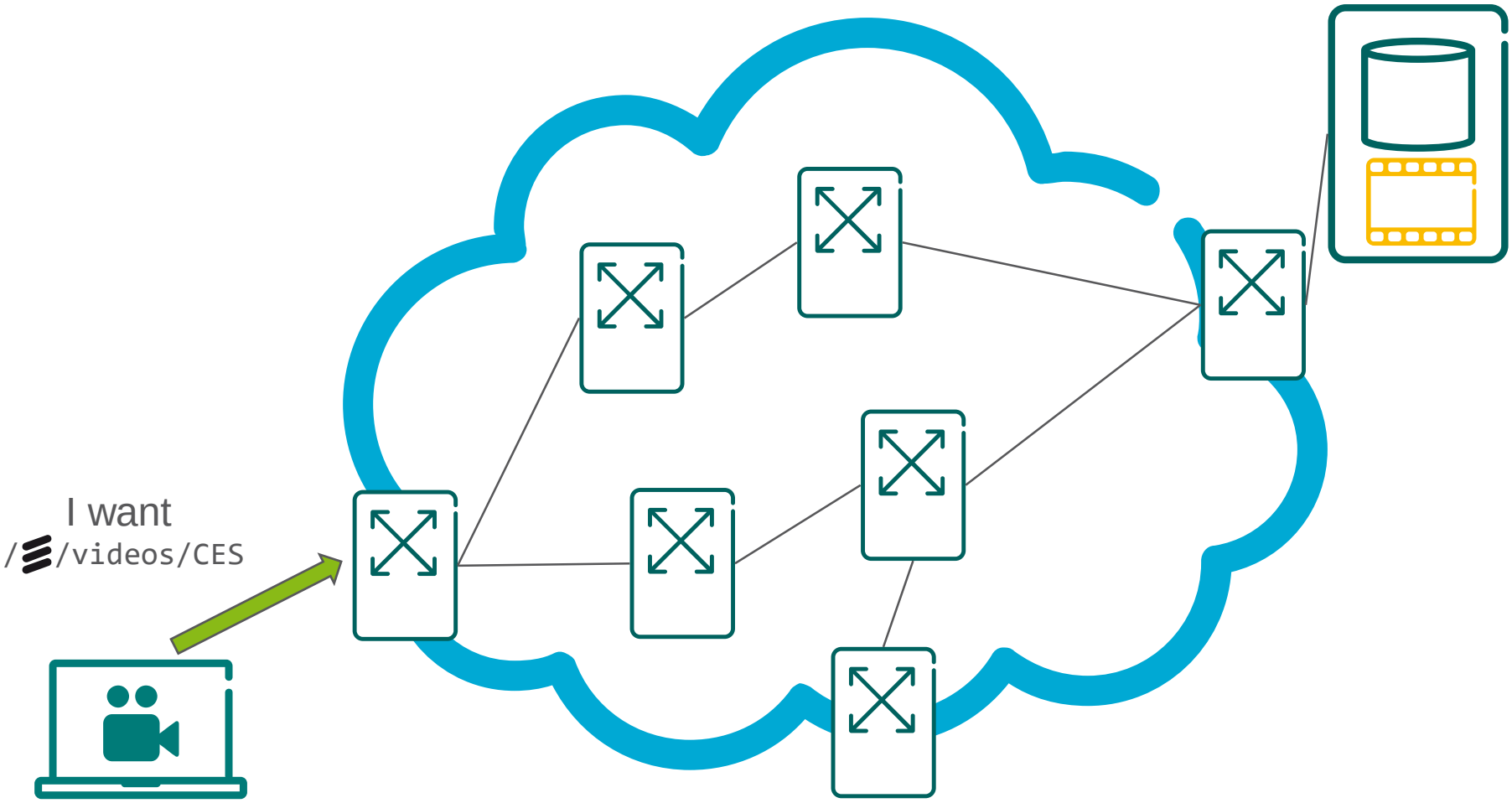
Security model in Information-centric Networking (ICN)



Content Centric Networking (CCN)

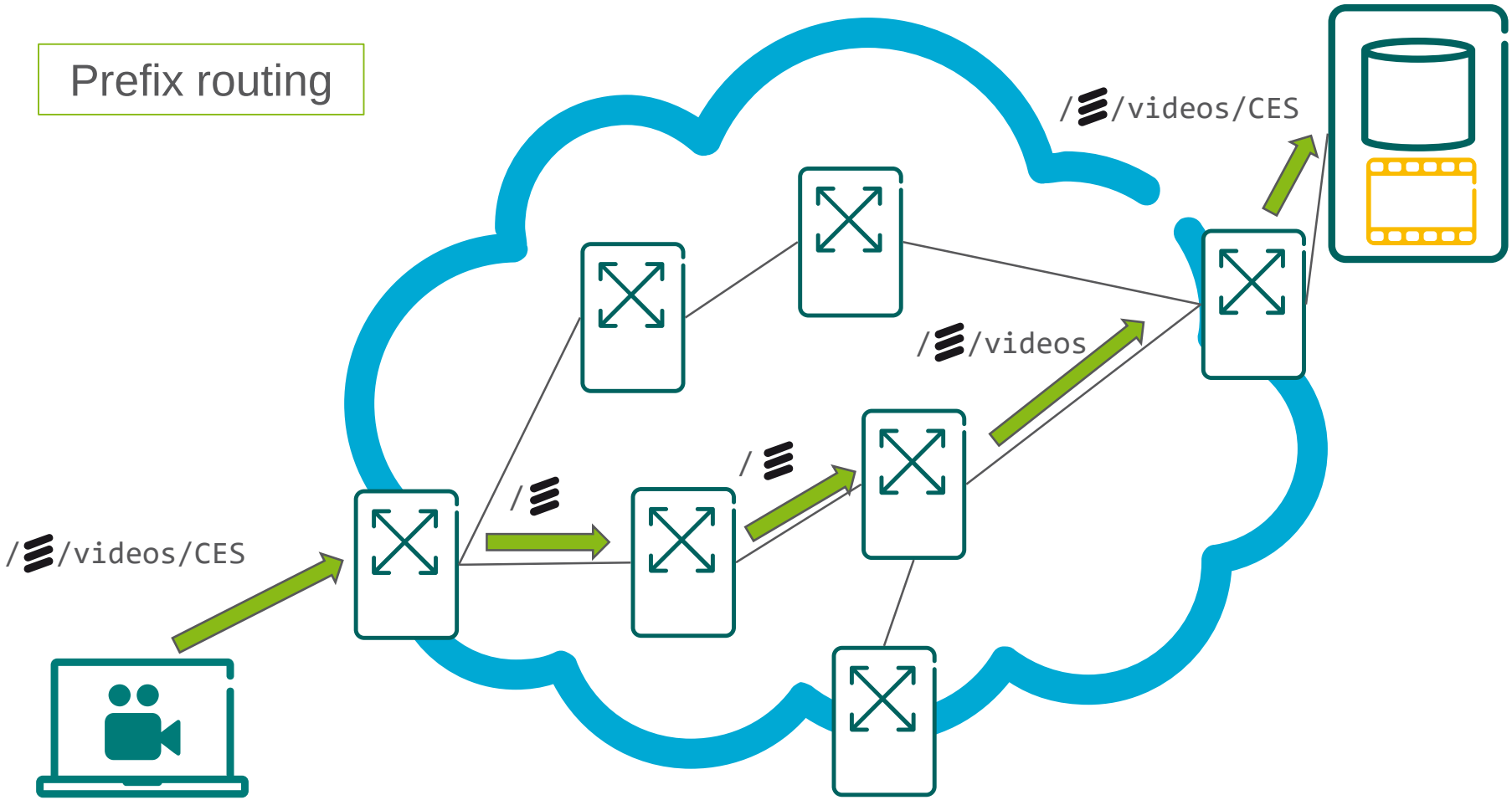


CCN



CCN

Prefix routing

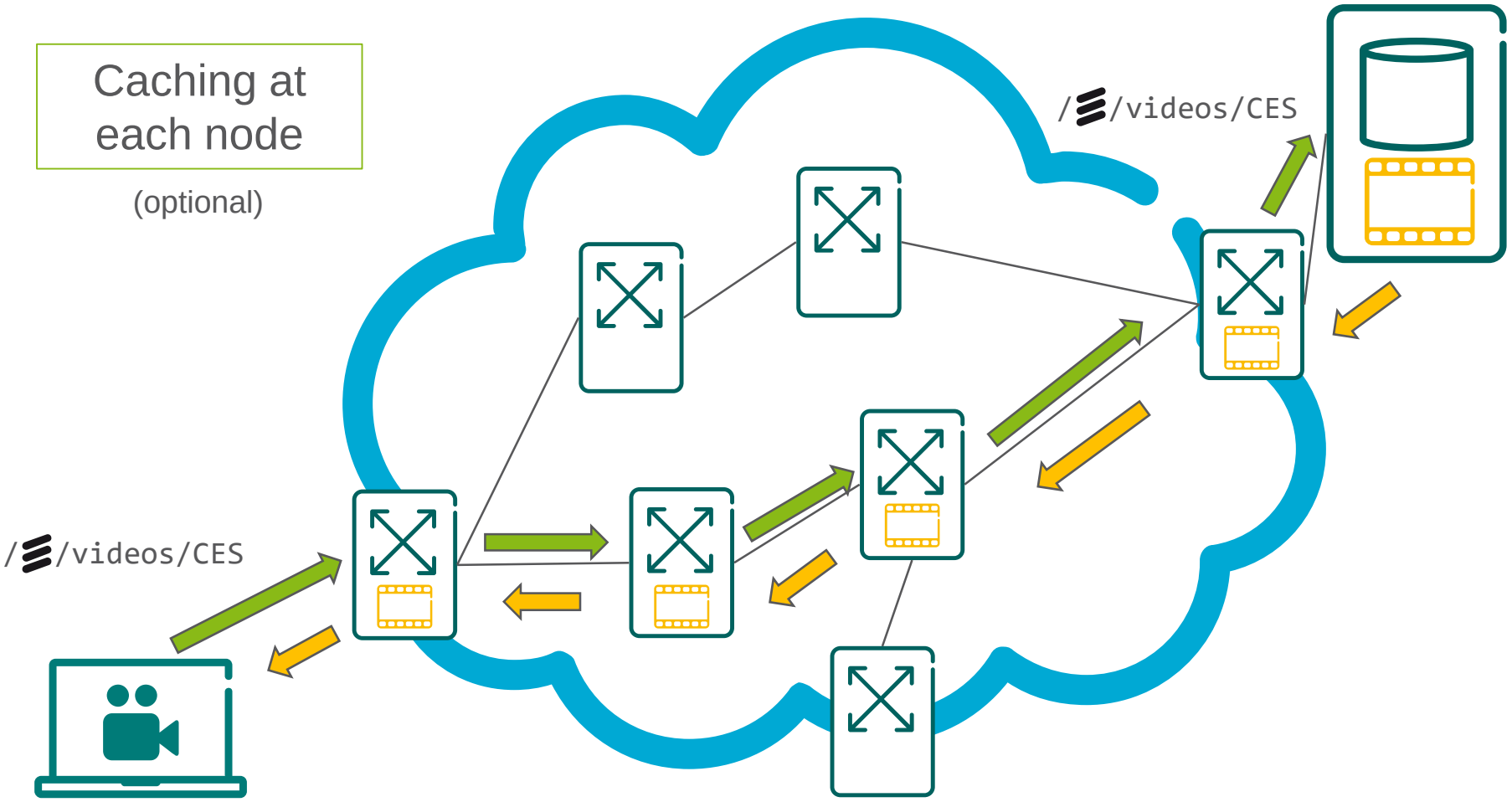


ICN2020

CCN

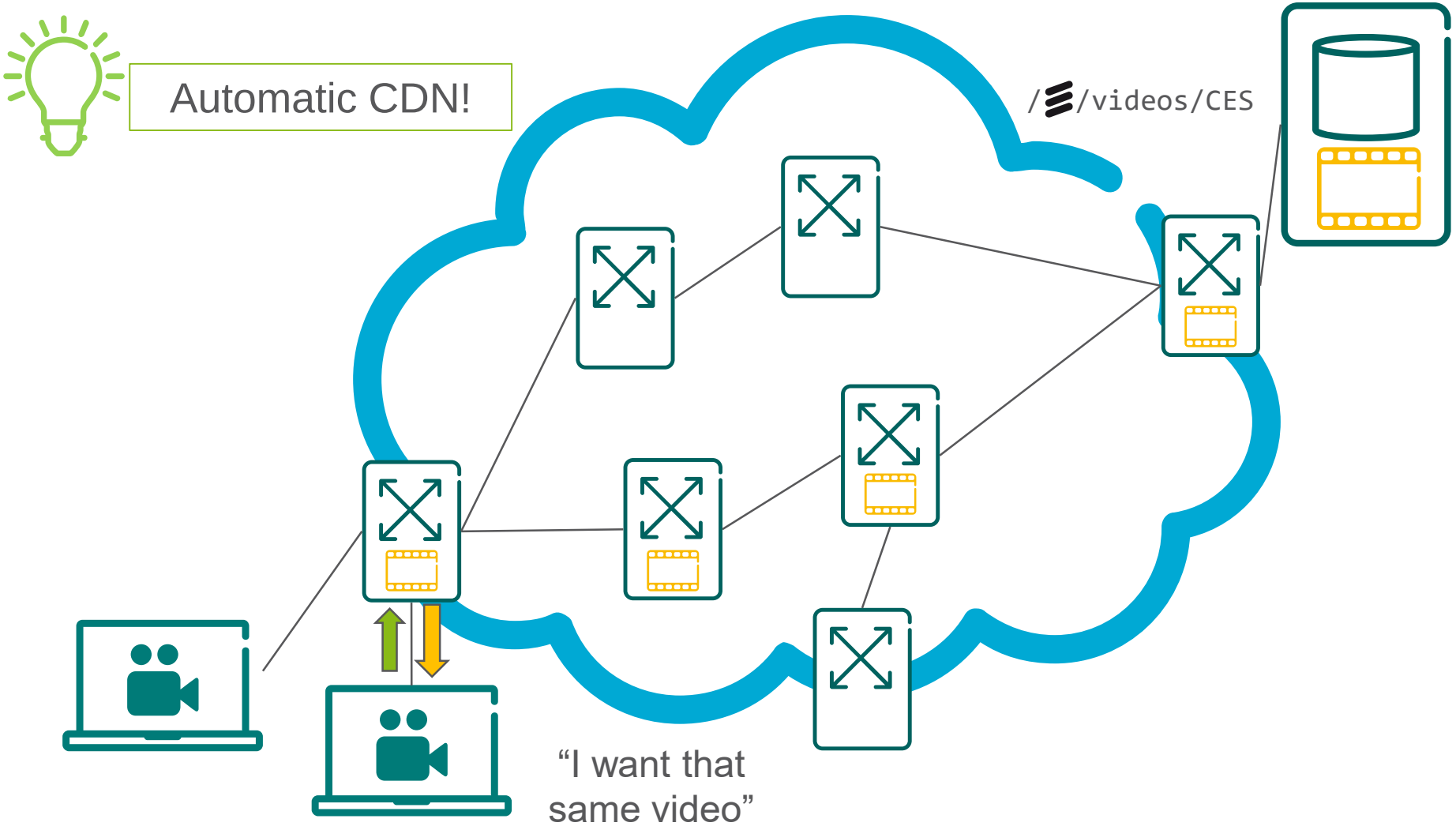
Caching at each node

(optional)



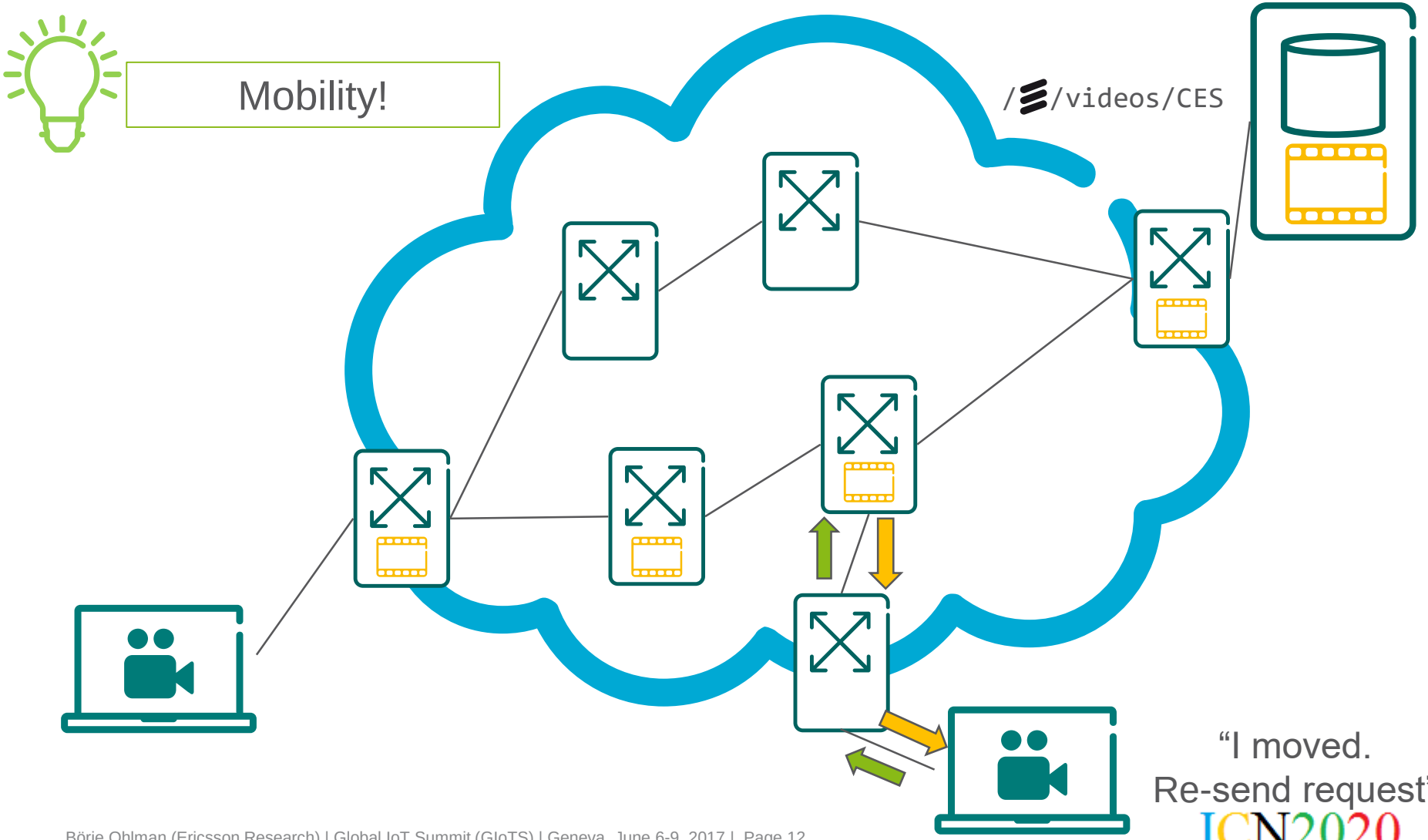
ICN2020

CCN

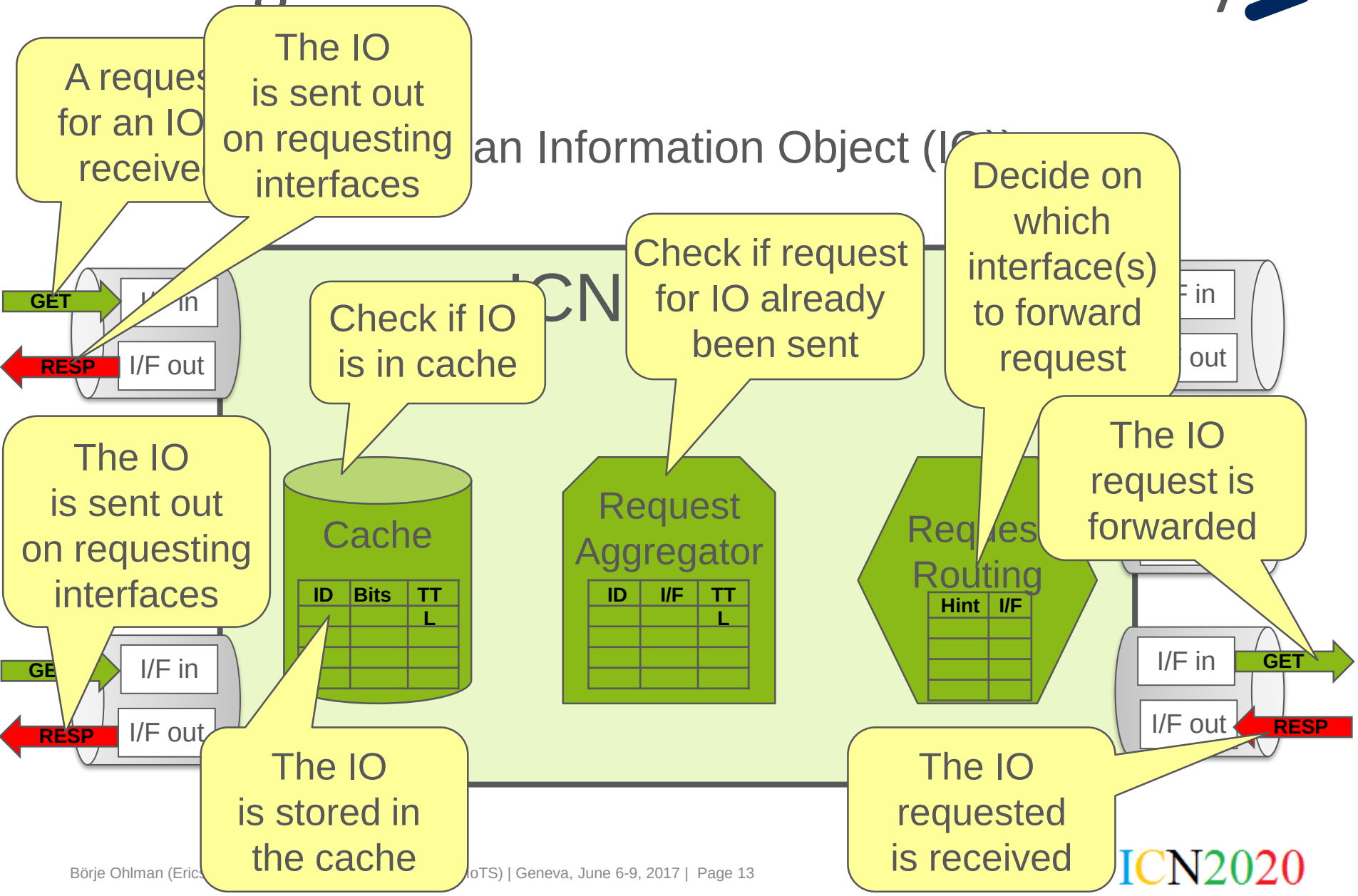


ICN2020

CCN

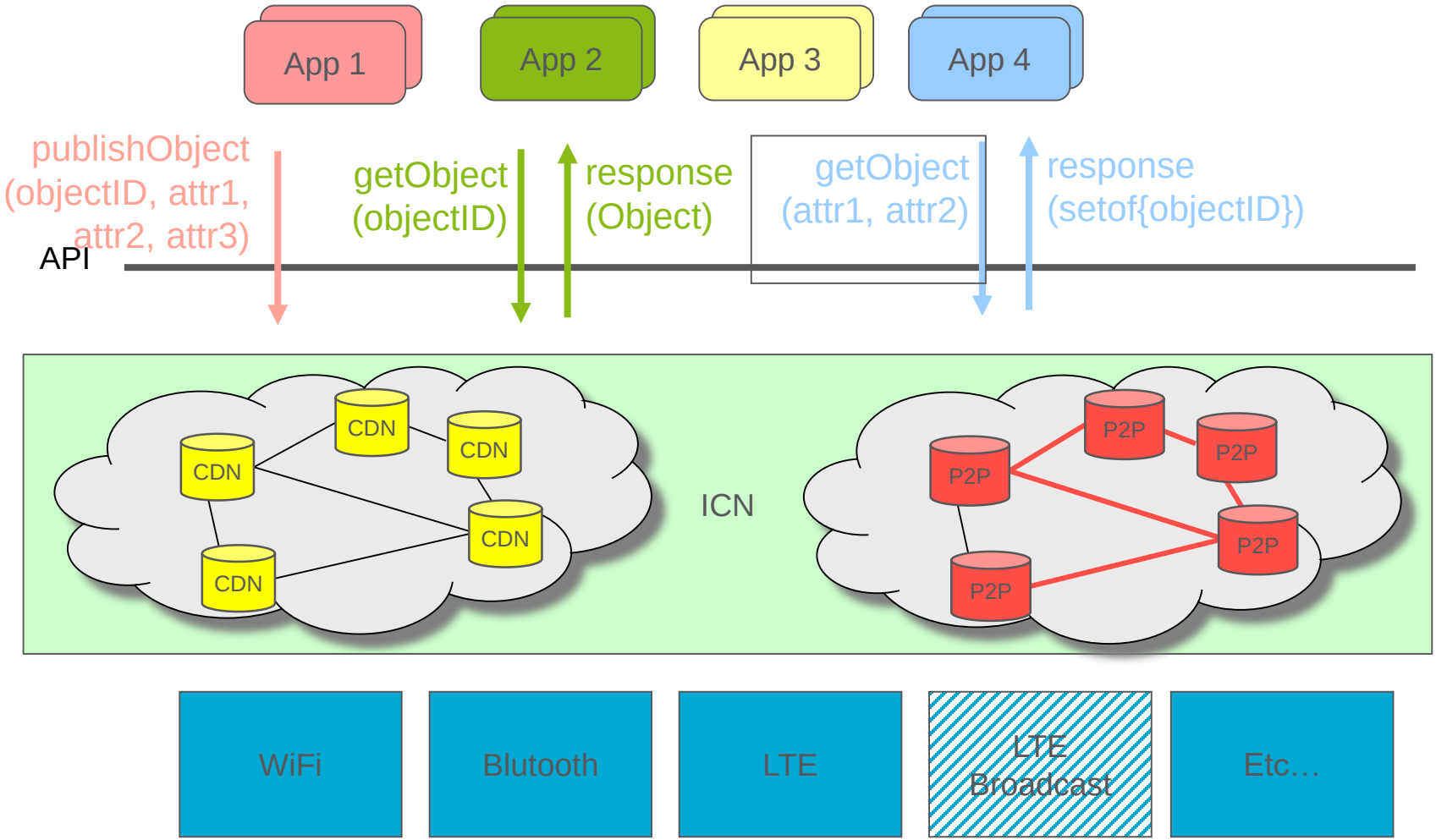


Basic generic ICN Router functionality



ICN2020

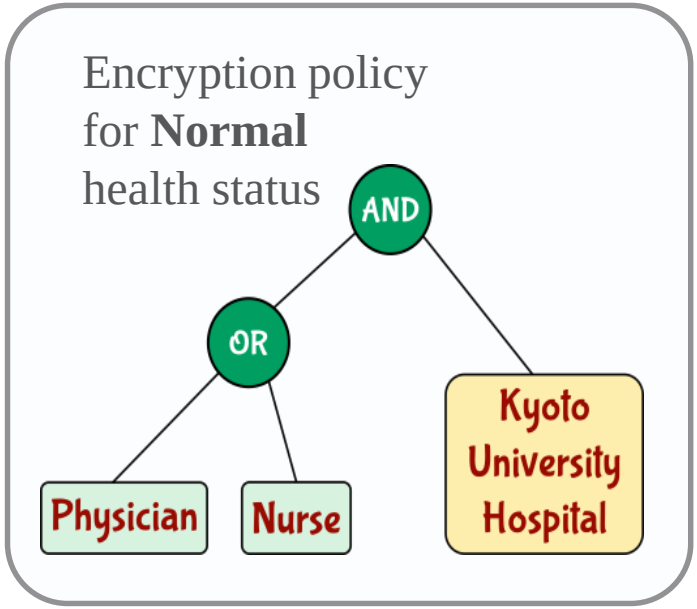
Providing cdn & p2p as an application independent Service for Secured Objects

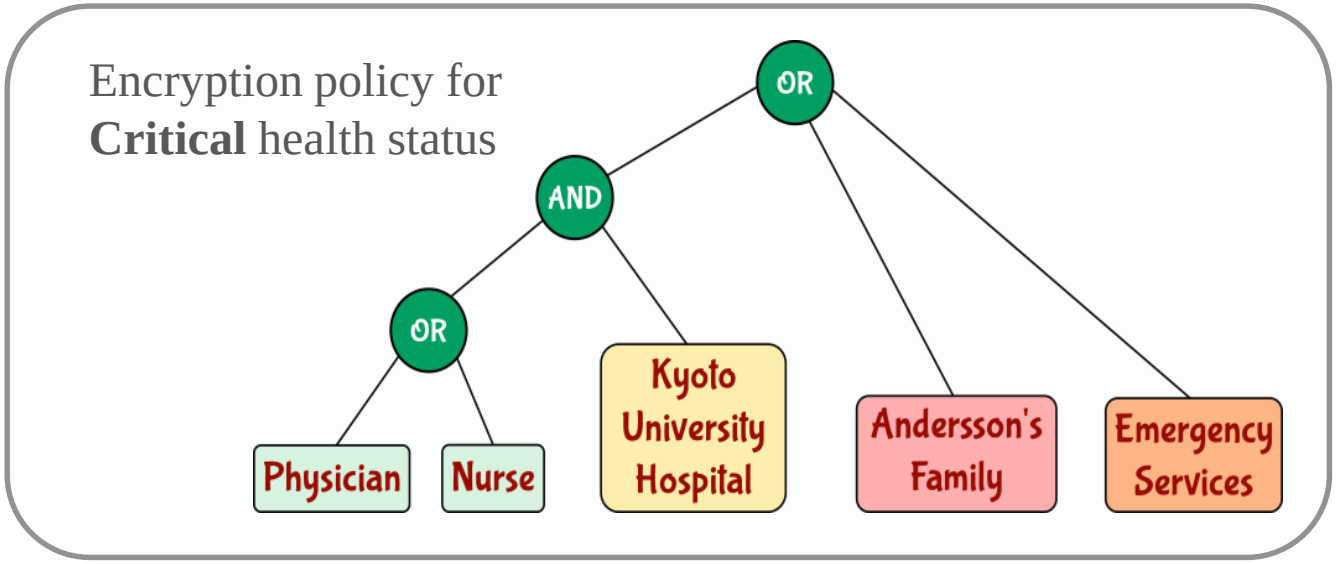


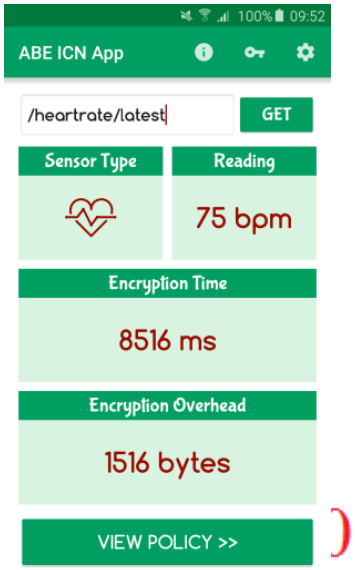
ICN2020

ICN & ABE Scenario

- A person has a personal sensor device that monitors body temperature and heart rate
- Data is privacy protected under ABE encryption policies
- Different encryption policies are used depending on the health status







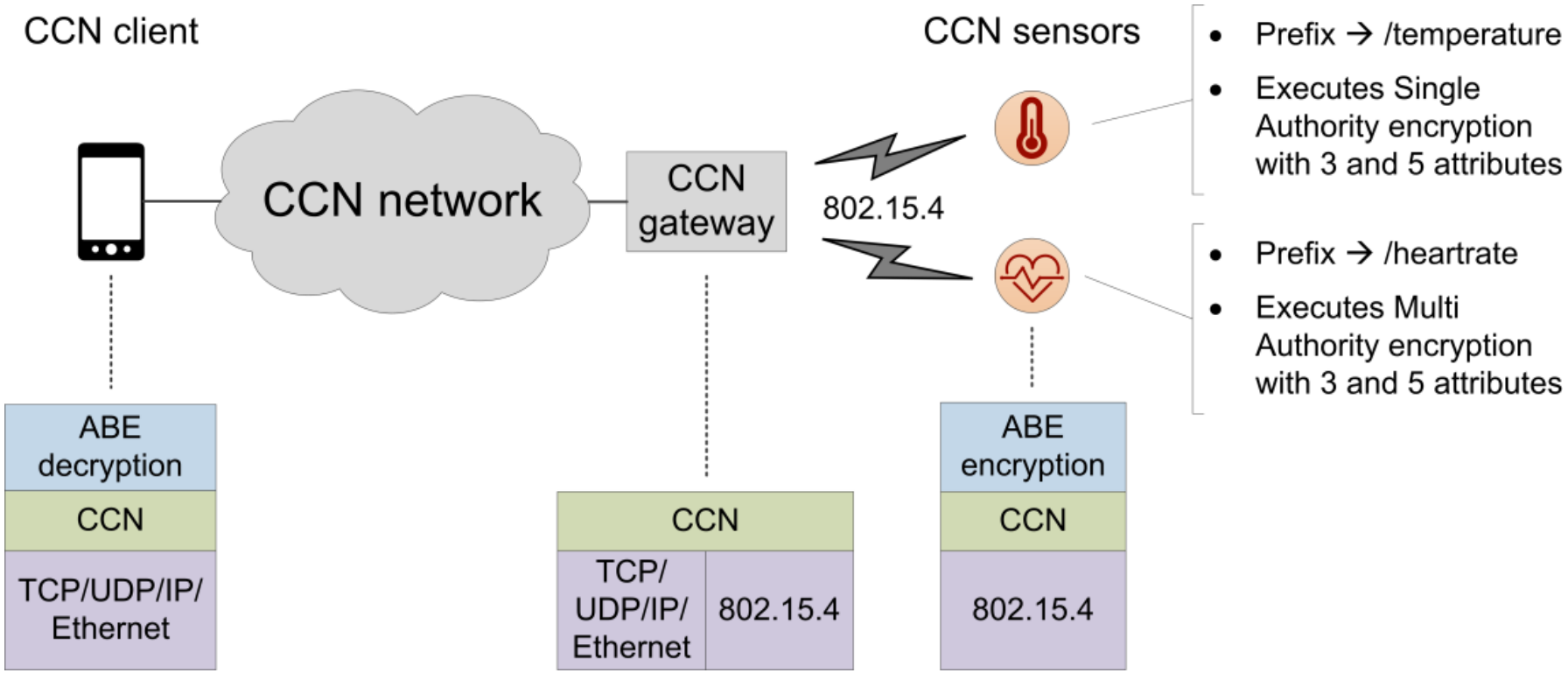
ABE & ICN

- ABE provides object security
- ABE is inline with ICN as both focus on information objects
- ABE allows for complex access policies for objects while maintaining one encrypted version of the object

Attribute-Based Encryption (ABE)

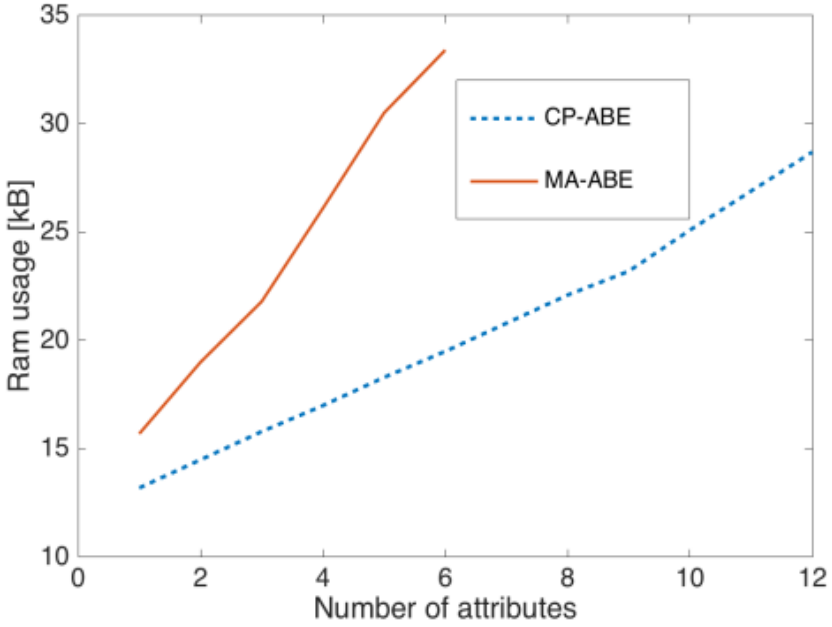
- Pros:
  - Object security that secures the object at the source, no need to trust gateways in the network
  - Successful decryption can be achieved with multiple different keys
  - Does not require online communication with the key management server
  - Can provide good privacy by use of decentralized attribute authorities
- Cons:
  - Computationally heavy
  - No easy solution to revoking attributes/keys

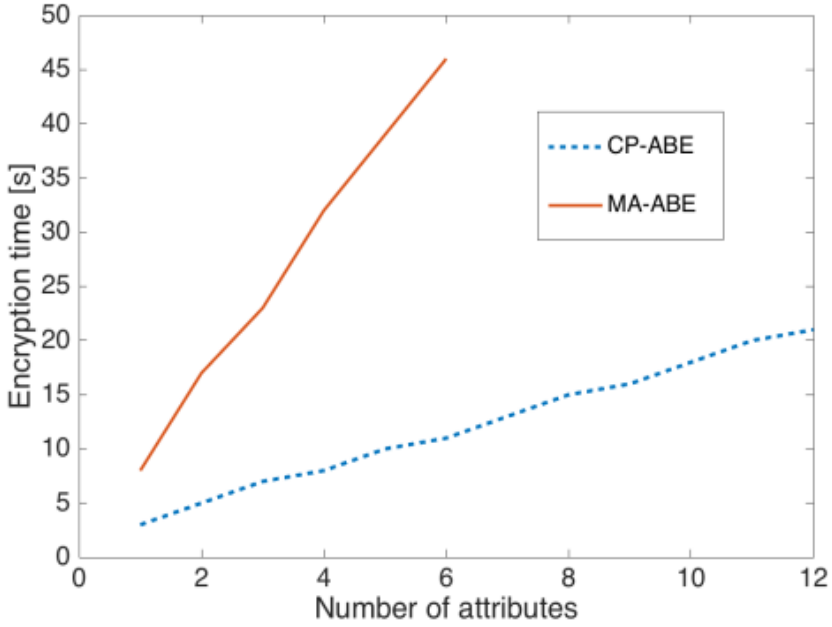
Testbed



- CCN relay implemented in CCN-lite on top of RIOT OS
- Android ICN ABE app developed
- Sensor hardware platform used STM32F4DISCOVERY
  - ARM Cortex-M4 32-bitcore, 1 MB Flash memory and 192 kB RAM

results & Conclusions





- Performing ABE on sensors is feasible
- RAM is the bottle-neck, not processing power

ERICSSON

SEVENTH FRAMEWORK PROGRAMME

ICN2020