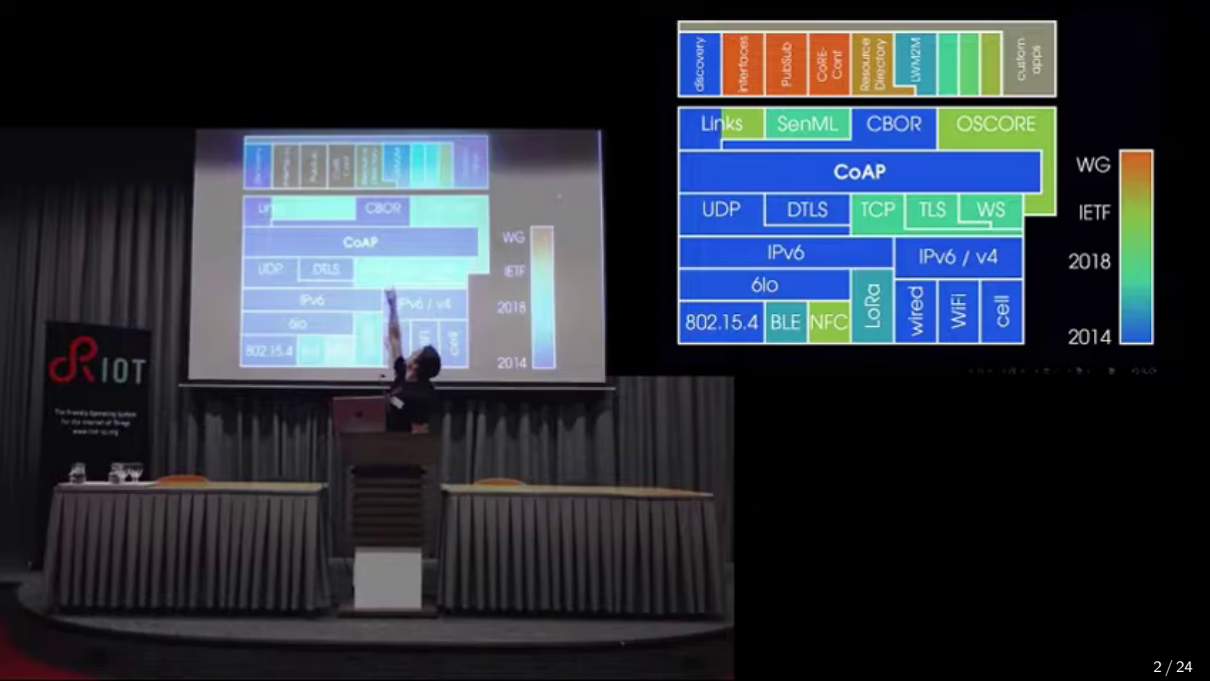
Pieces to Picture: Security components in the CoRE ecosystem

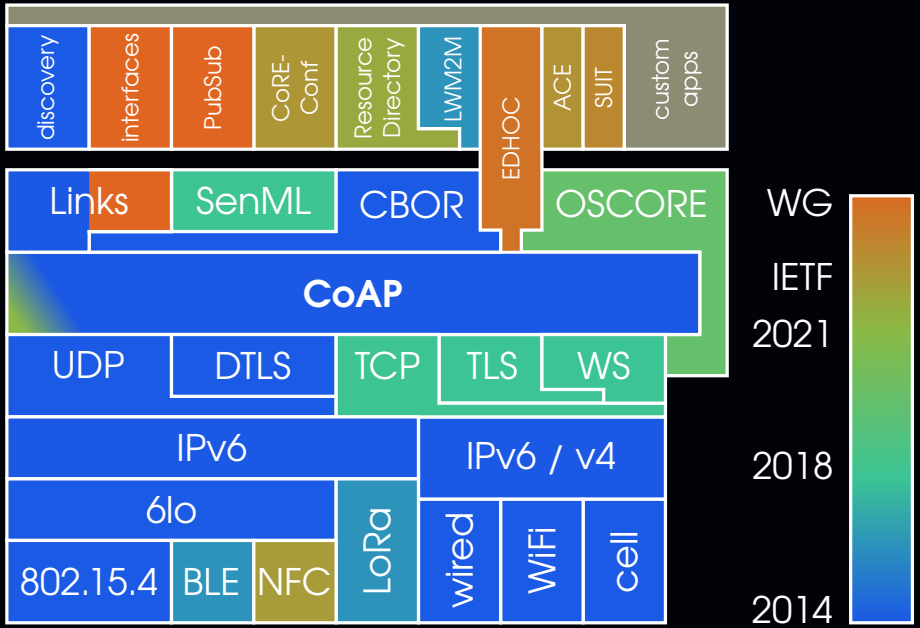
Christian Amsüss <ca@etonomy.org>

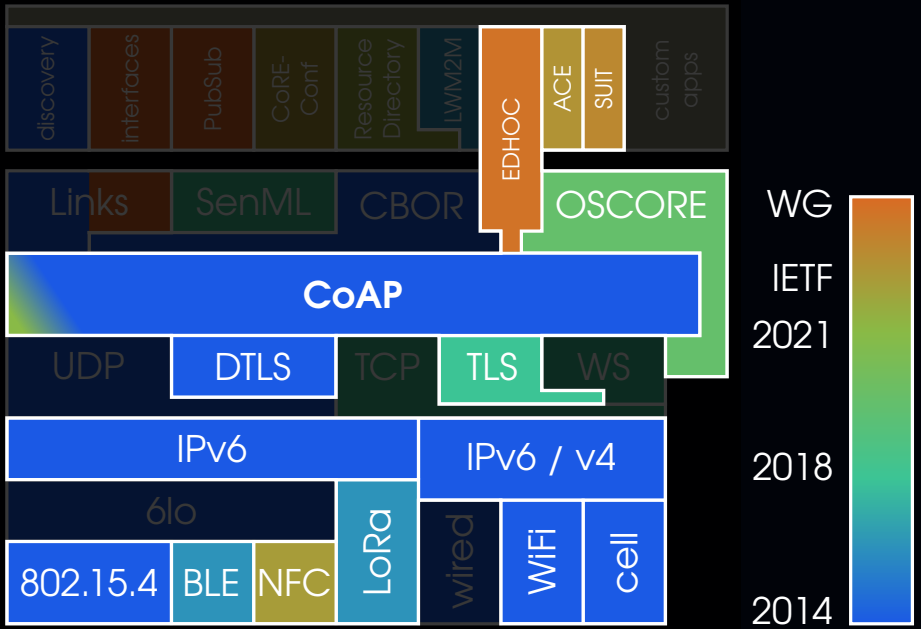
2021-09-09

etonomy

RIOT

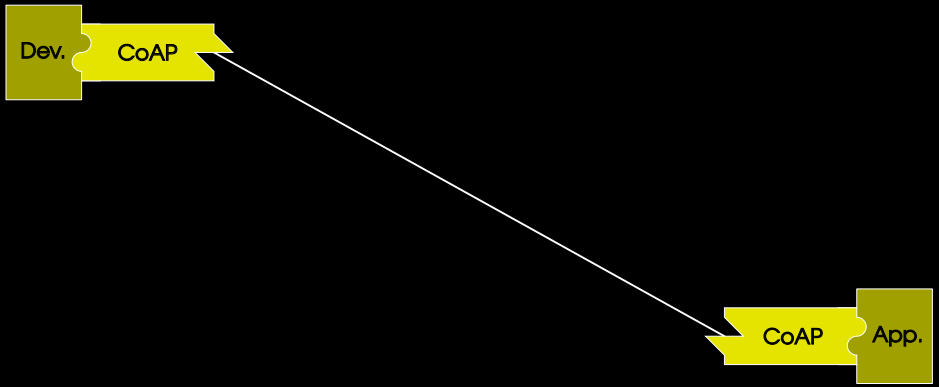

discovery
Interfaces
Pub/Sub
CoRE-Conf
Resource Directory
LWM2M
custom apps
Links
SenML
CBOR
OSCORE
CoAP
UDP
DTLS
TCP
TLS
WS
IPv6
IPv6 / v4
6lo
802.15.4
BLE
NFC
LoRa
wired
WiFi
cell
WG
IETF
2018
2014
RIOT


discovery
interfaces
PubSub
CoRE-Conf
Resource Directory
LWM2M
EDHOC
ACE
SUIT
custom apps
Links
SenML
CBOR
OSCORE
CoAP
UDP
DTLS
TCP
TLS
WS
IPv6
IPv6 / v4
6lo
802.15.4
BLE
NFC
LoRa
wired
WiFi
cell
WG
IETF
2021
2018
2014

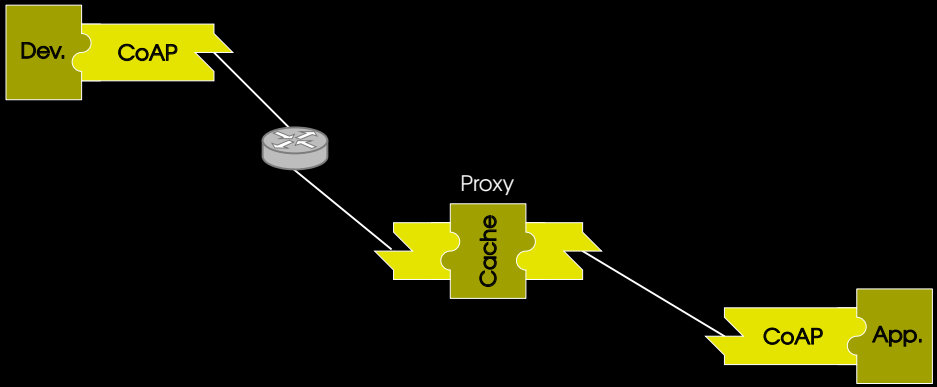

discovery
interfaces
PubSub
CoRE-Conf
Resource Directory
LWM2M
EDHOC
ACE
SUIT
custom apps
Links
SenML
CBOR
OSCORE
CoAP
UDP
DTLS
TCP
TLS
WS
IPv6
IPv6 / v4
6lo
802.15.4
BLE
NFC
LoRa
wired
WiFi
cell
WG
IETF
2021
2018
2014

RFC7252: CoAP

The Little Picture (NoSec mode)

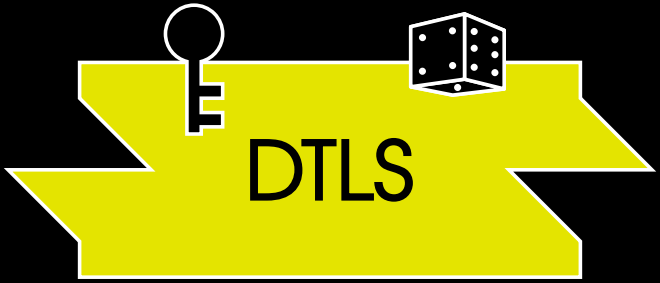


The Little Picture (NoSec with proxy)



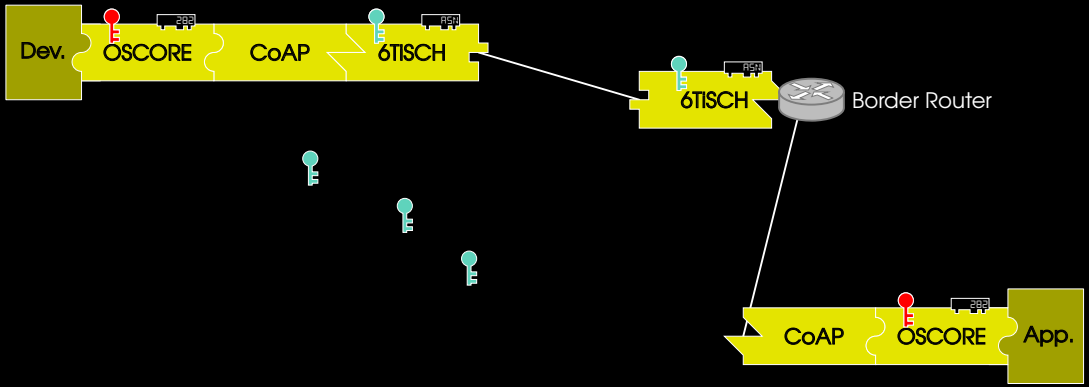
RFC8613: OSCORE

RFC7252: CoAP-over-DTLS PSK

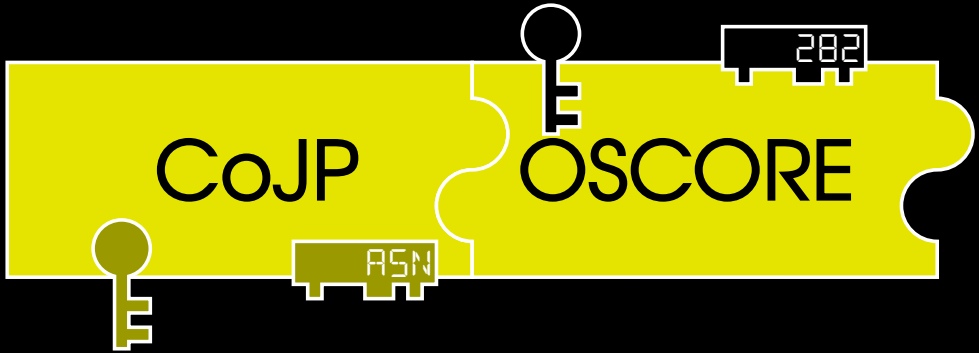


RFC8180: Minimal 6TiSCH, and IEEE 802.15.4

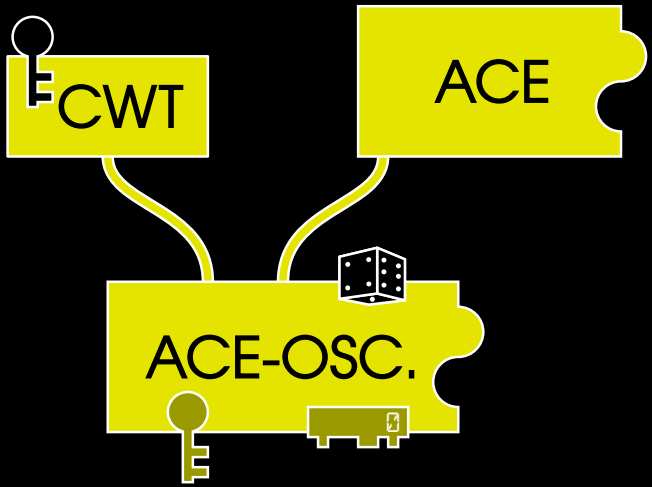
The Big Picture I



RFC9031: Constrained Join Protocol for 6TiSCH



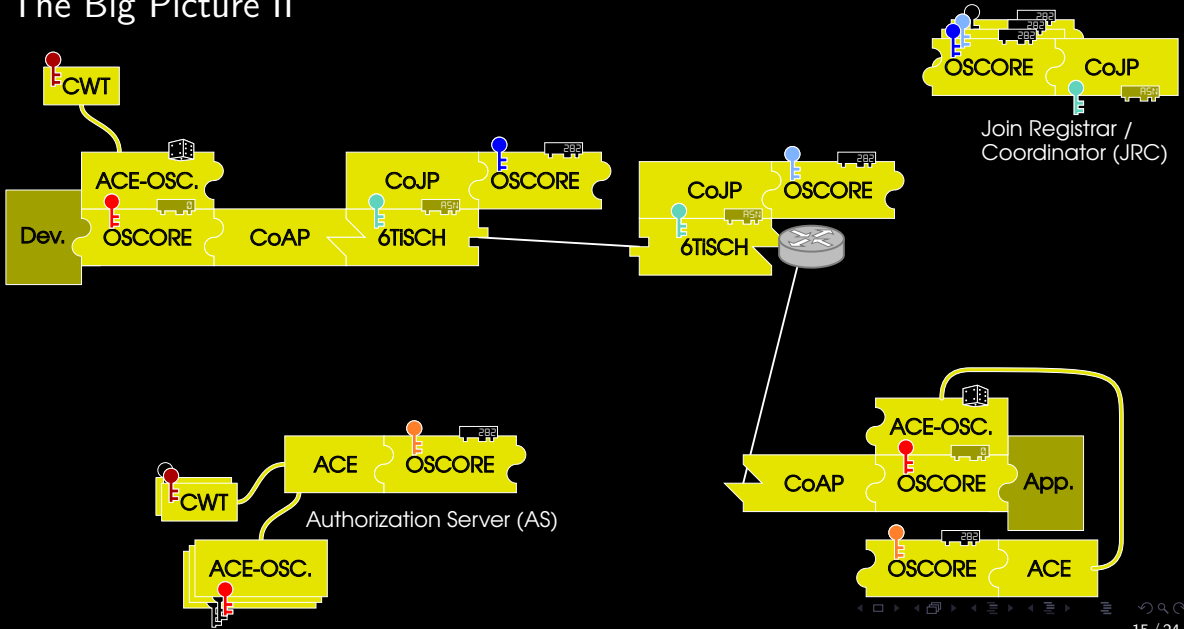
draft-ietf-ace-oscore-profile



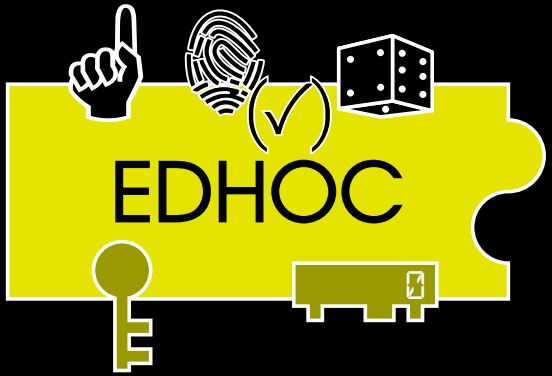
Excursion: COSE

- RFC8152: COSE – CBOR Object Signing and Encryption
- RFC8392: CWT – CBOR Web Token
- RFC9019: SUIT – A Firmware Update Architecture for Internet of Things

The Big Picture II



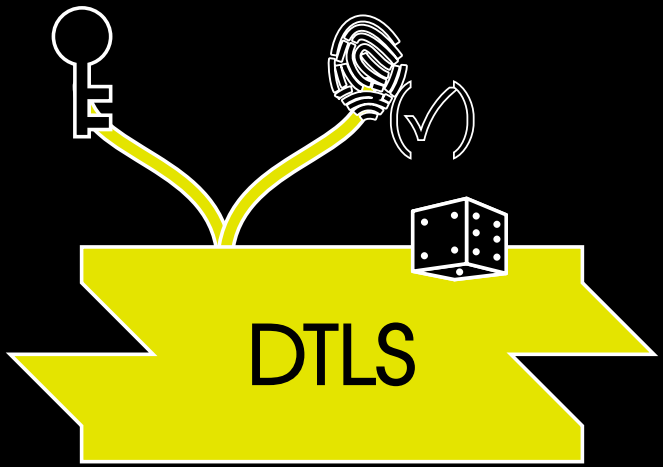
draft-ietf-lake-edhoc



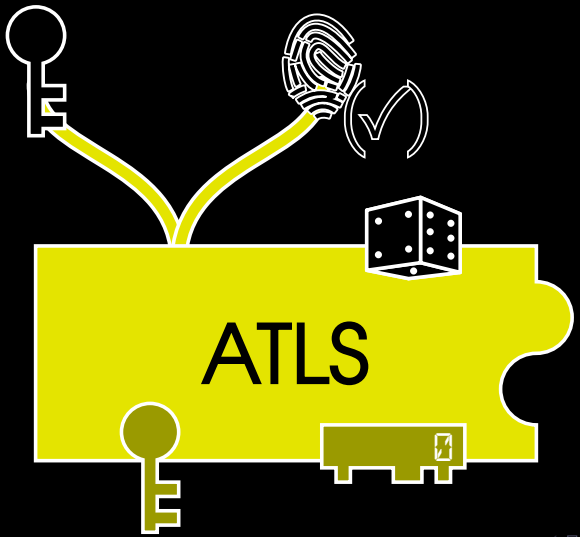
with optimizations for single round trip before OSCORE in draft-ietf-core-oscore-edhoc

draft-ietf-ace-wg-coap-eap

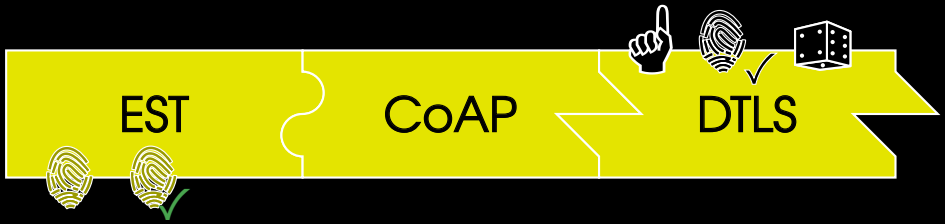
RFC7252: CoAP-over-DTLS (other modes)



draft-friel-tls-atls

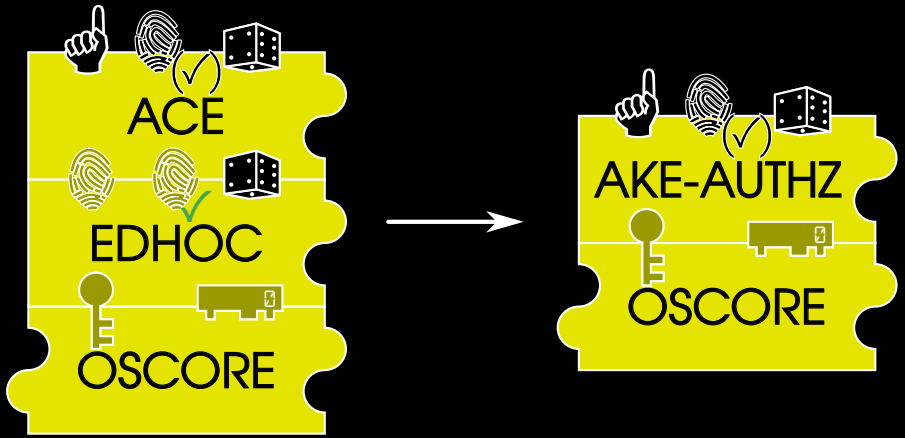


RFC8995: BRSKI



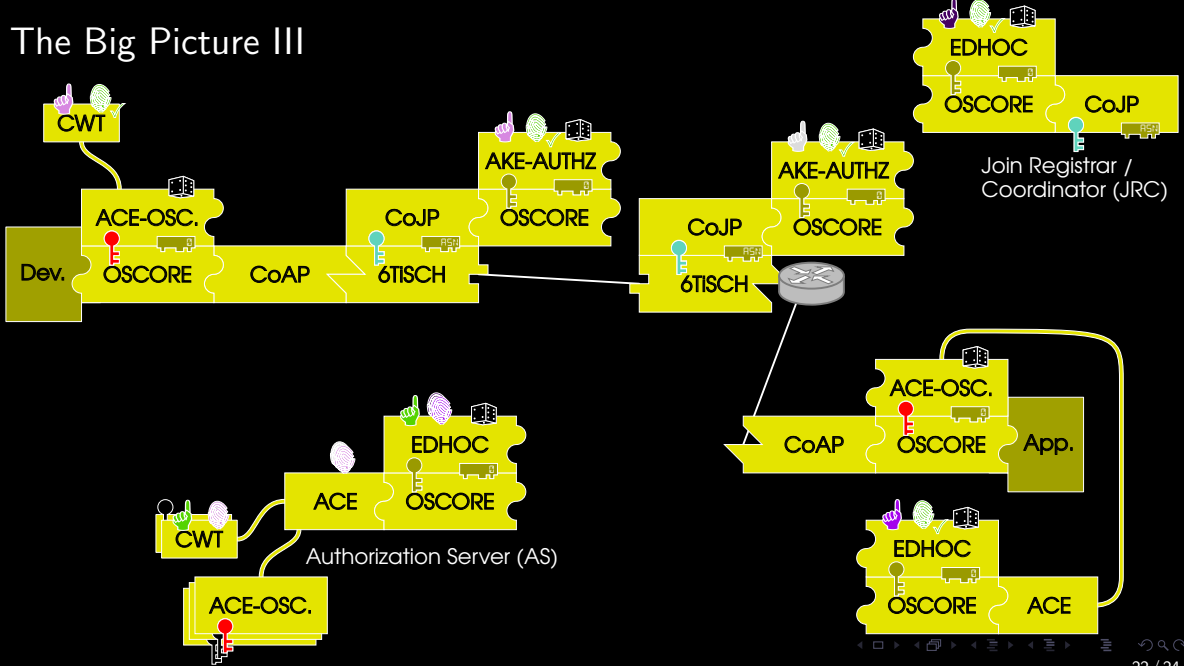
with CoAP mapping from draft-ietf-ace-coap-est

draft-selander-ace-ake-authz

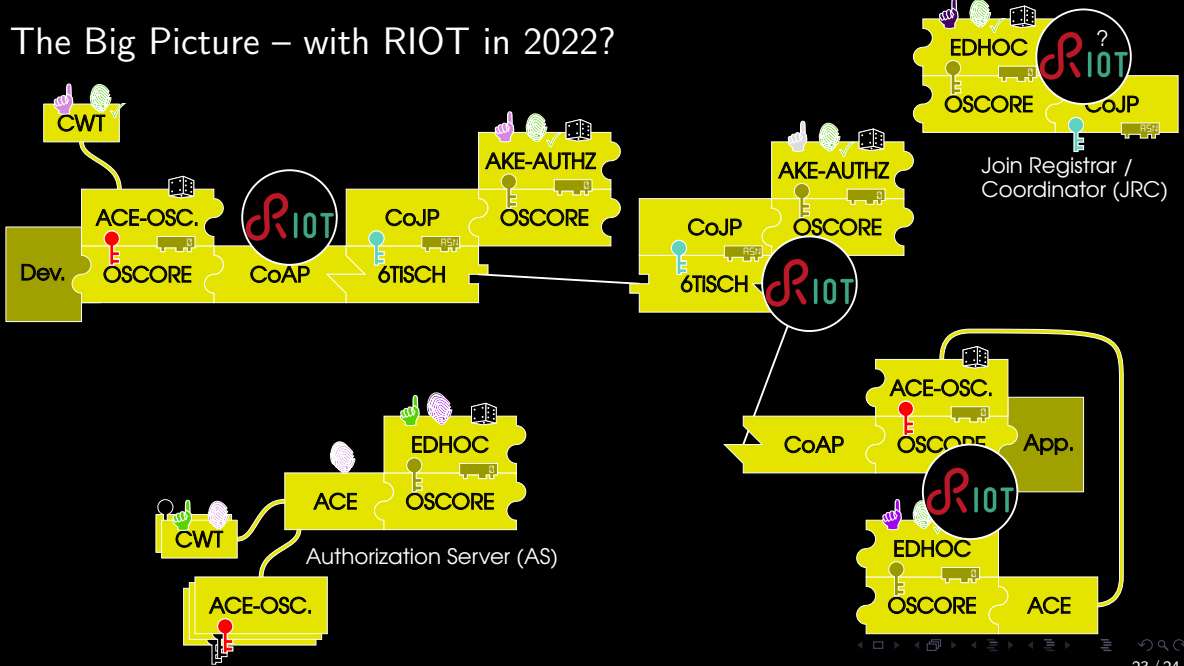


with just two messages before payload is exchanged

The Big Picture III



The Big Picture – with RIOT in 2022?



Thanks for having me here

Slides and more links on
`http://christian.amsuess.com/presentations/2021/summit-core/`

etonomy

RIOT