

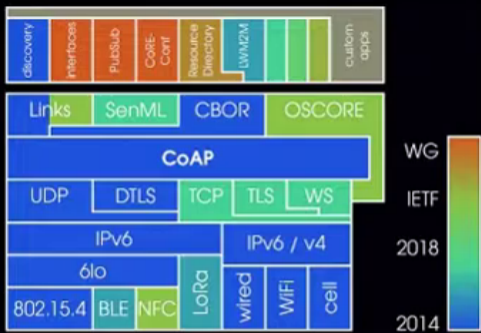
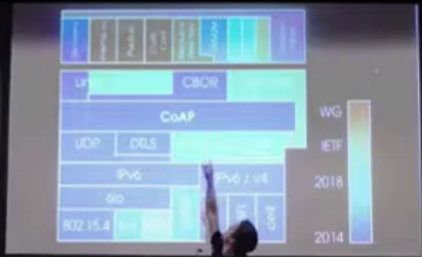
# Pieces to Picture: Security components in the CoRE ecosystem

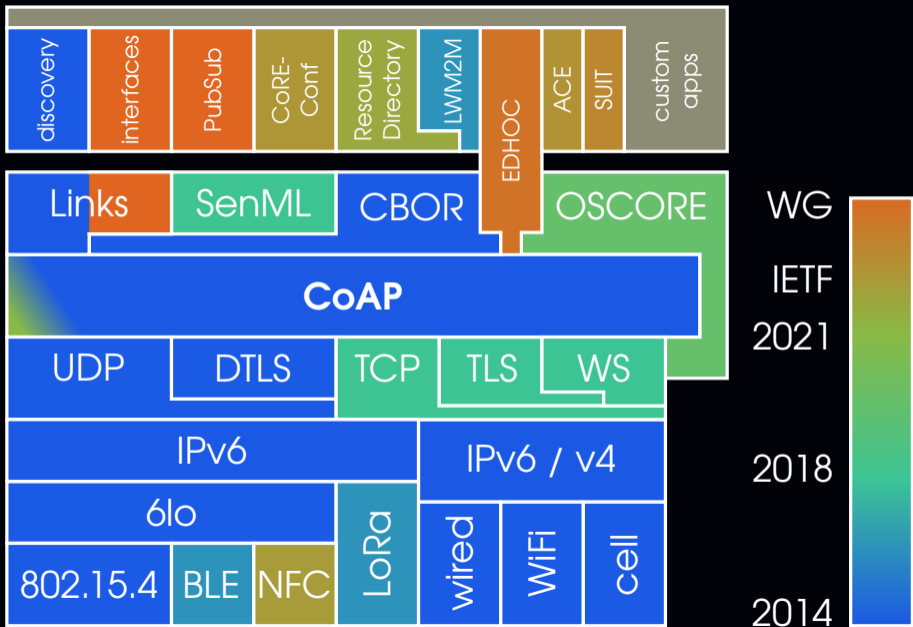
Christian Amsüss <ca@etonomy.org>

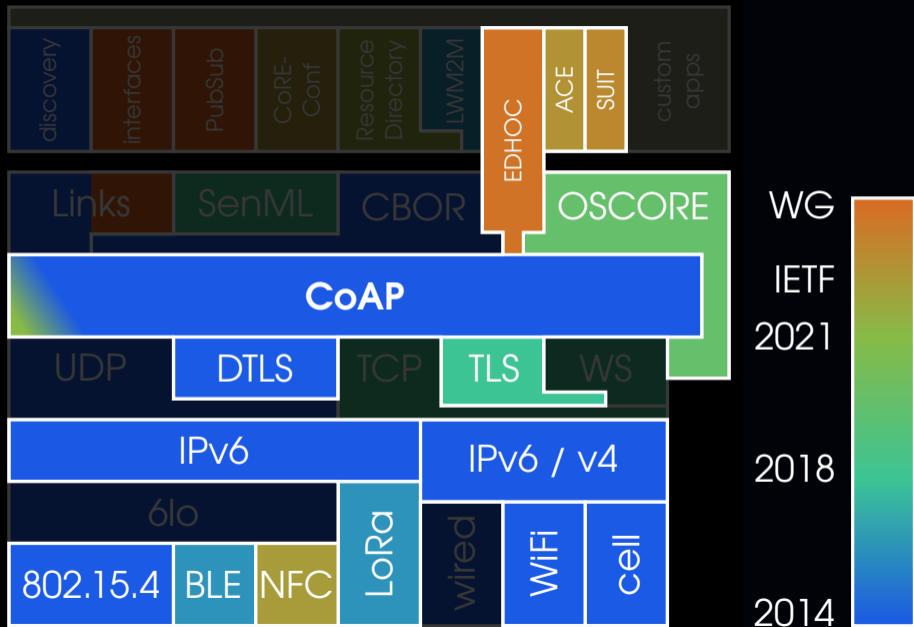
2021-09-09

etonomy



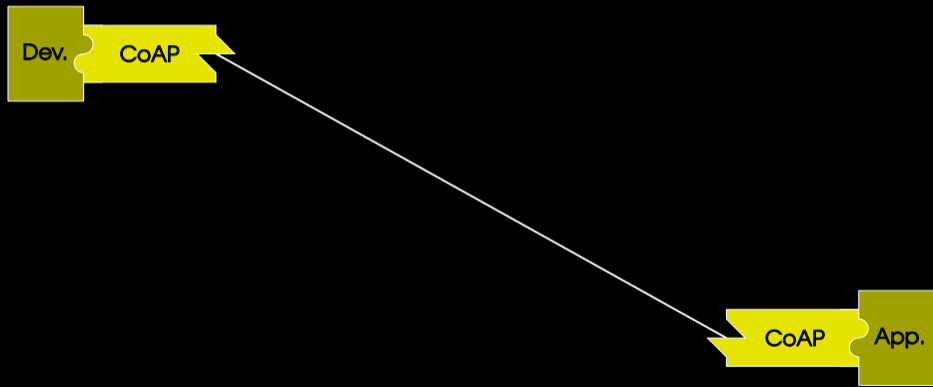




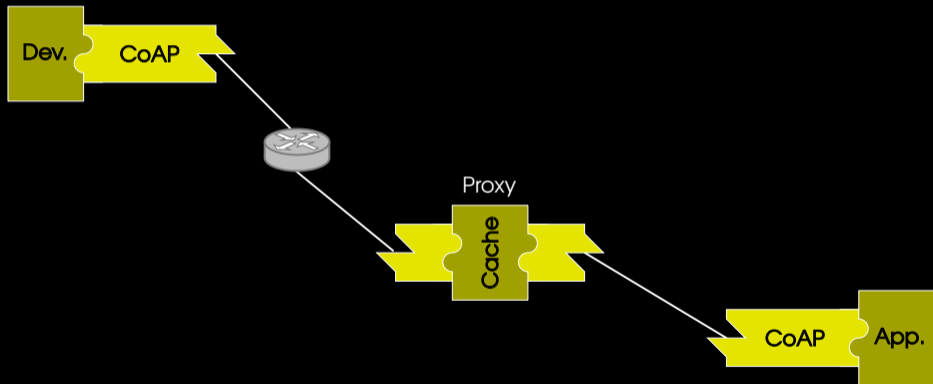


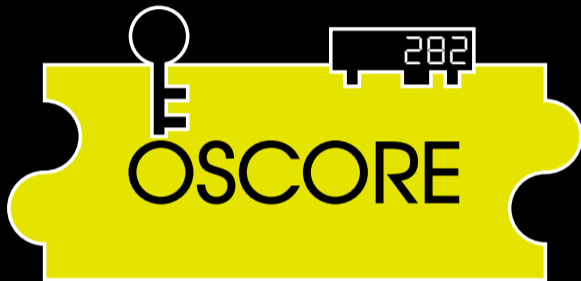


# The Little Picture (NoSec mode)



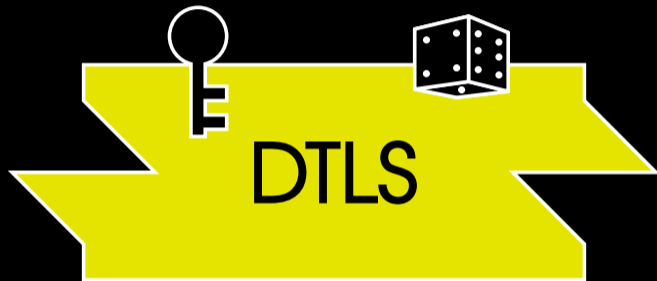
# The Little Picture (NoSec with proxy)



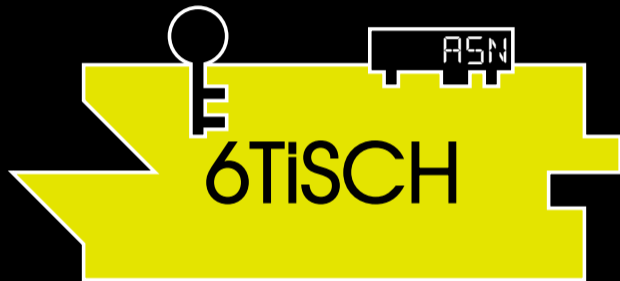




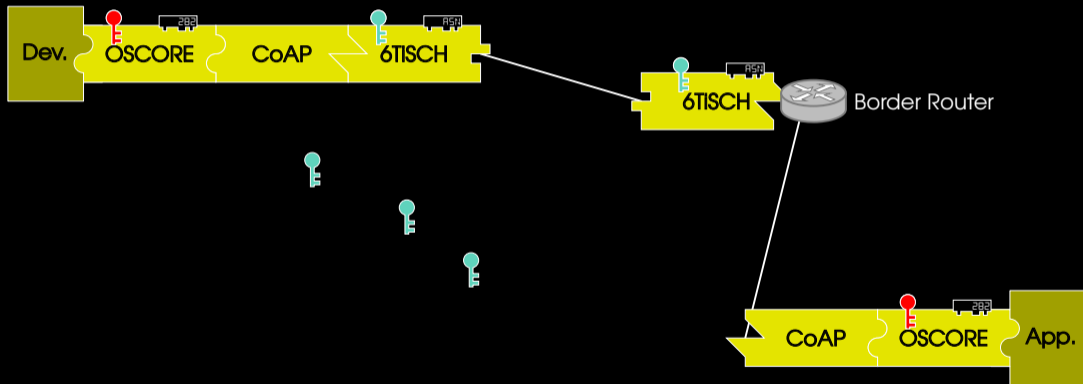
# RFC7252: CoAP-over-DTLS PSK



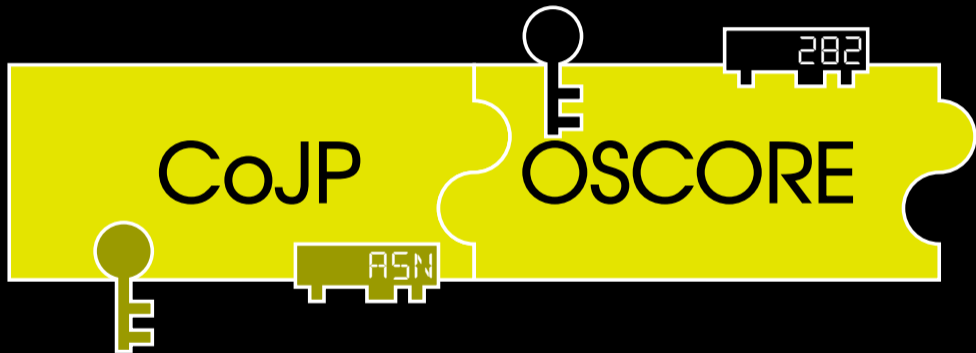
# RFC8180: Minimal 6TiSCH, and IEEE 802.15.4

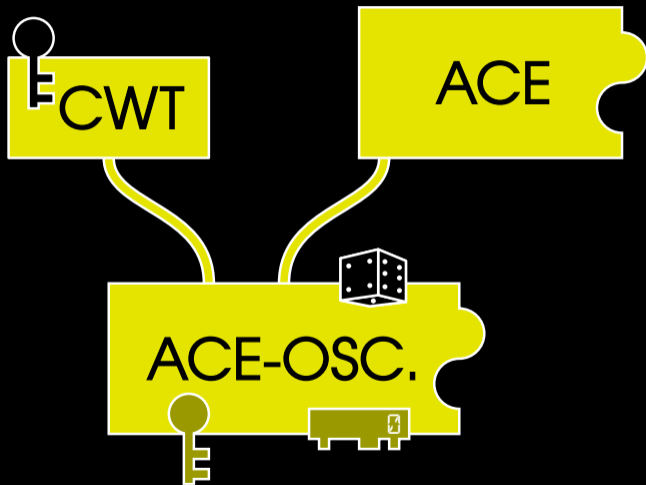


# The Big Picture I



# RFC9031: Constrained Join Protocol for 6TiSCH

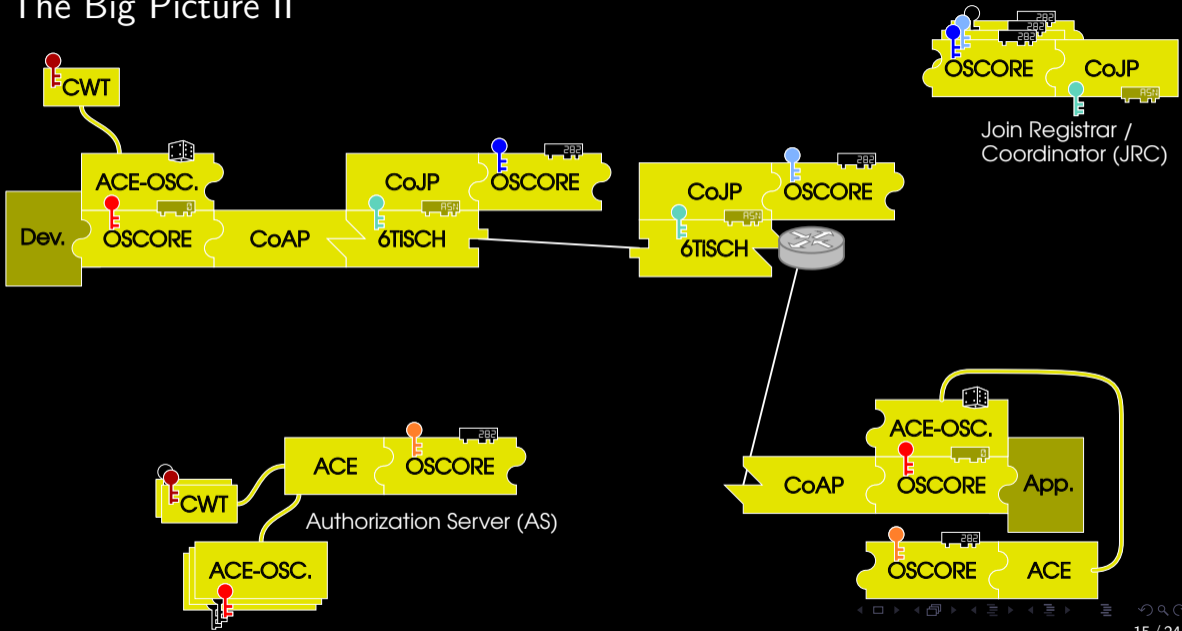


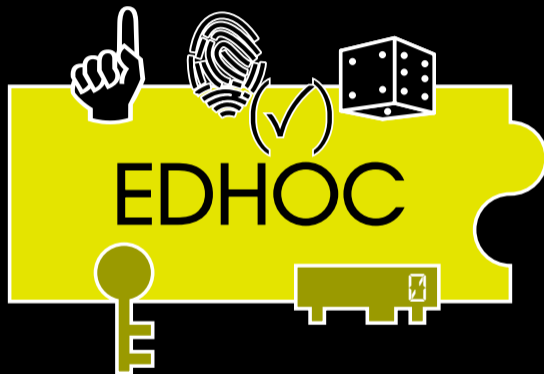


## Excursion: COSE

- ▶ 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



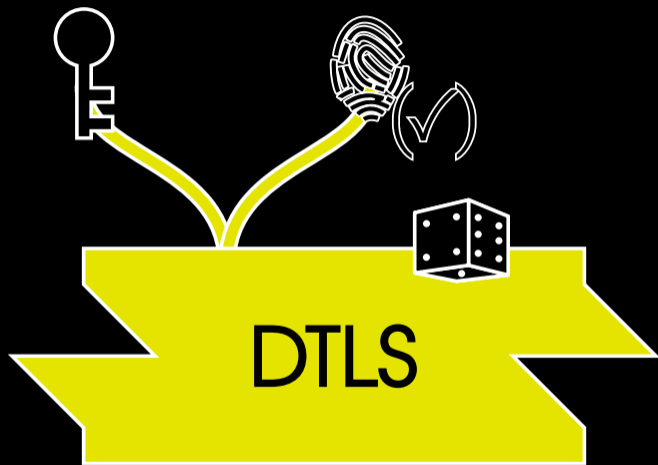


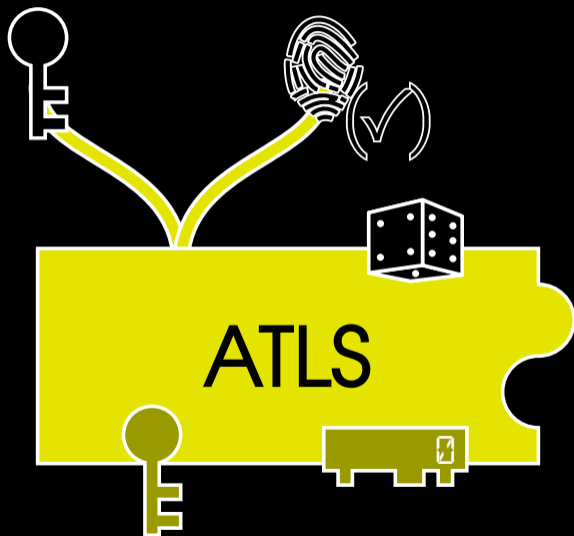
with optimizations for single round trip before OSCORE in draft-ietf-core-oscore-edhoc





# RFC7252: CoAP-over-DTLS (other modes)



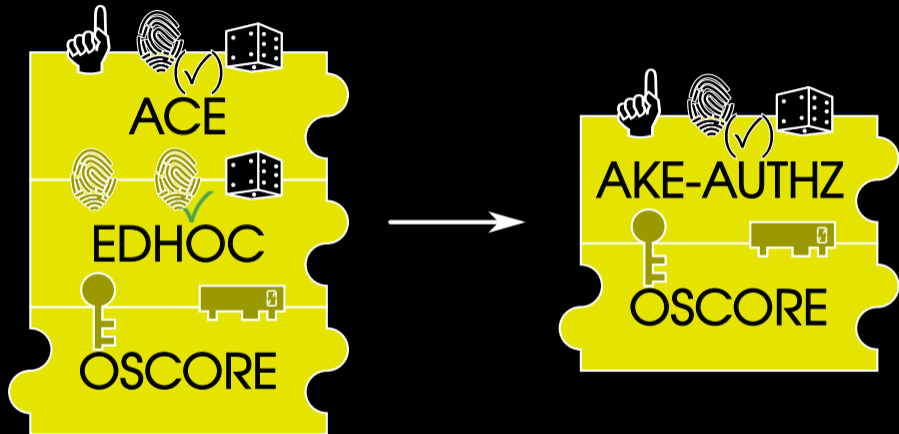


# RFC8995: BRSKI



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

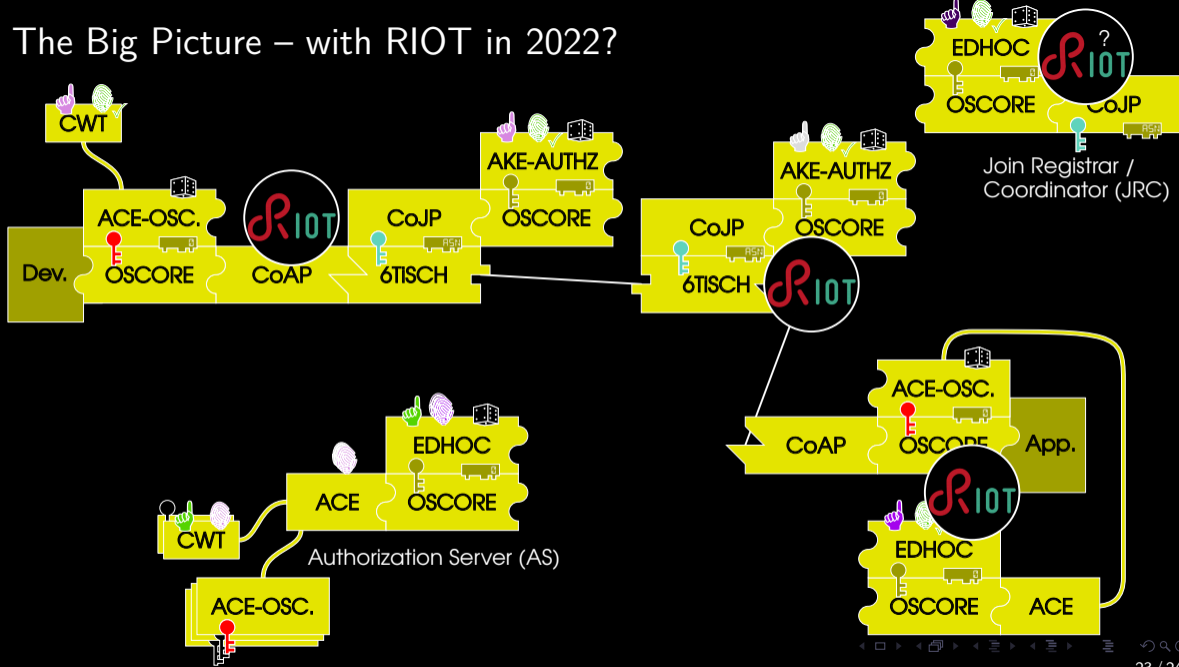
# draft-selander-ace-ake-authz



with just two messages before payload is exchanged



# The Big Picture – with RIOT in 2022?



Thanks for having me here

Slides and more links on

<http://christian.amsuess.com/presentations/2021/summit-core/>



etonomy

R10T