Security of smart grid communication protocols

Erik Poll
Radboud University Nijmegen

C-DAX is funded by the European Union's Seventh Framework Programme (FP7-ICT-2011-8) under grant agreement n° 318708

Overview

- *Before* starting to secure communications...

- End-to-end security
  - limits of secure tunnels using eg. TLS

- Securing Information Centric Networking (ICN) in C-DAX

Before starting to secure communications...

- *Primary* goal of ICT is to provide functionality

- Security is about controlling the risks that this functionality brings.

  This is always a *secondary* concern

  People will typically choose functionality over security...

- So, before starting to securing communications:

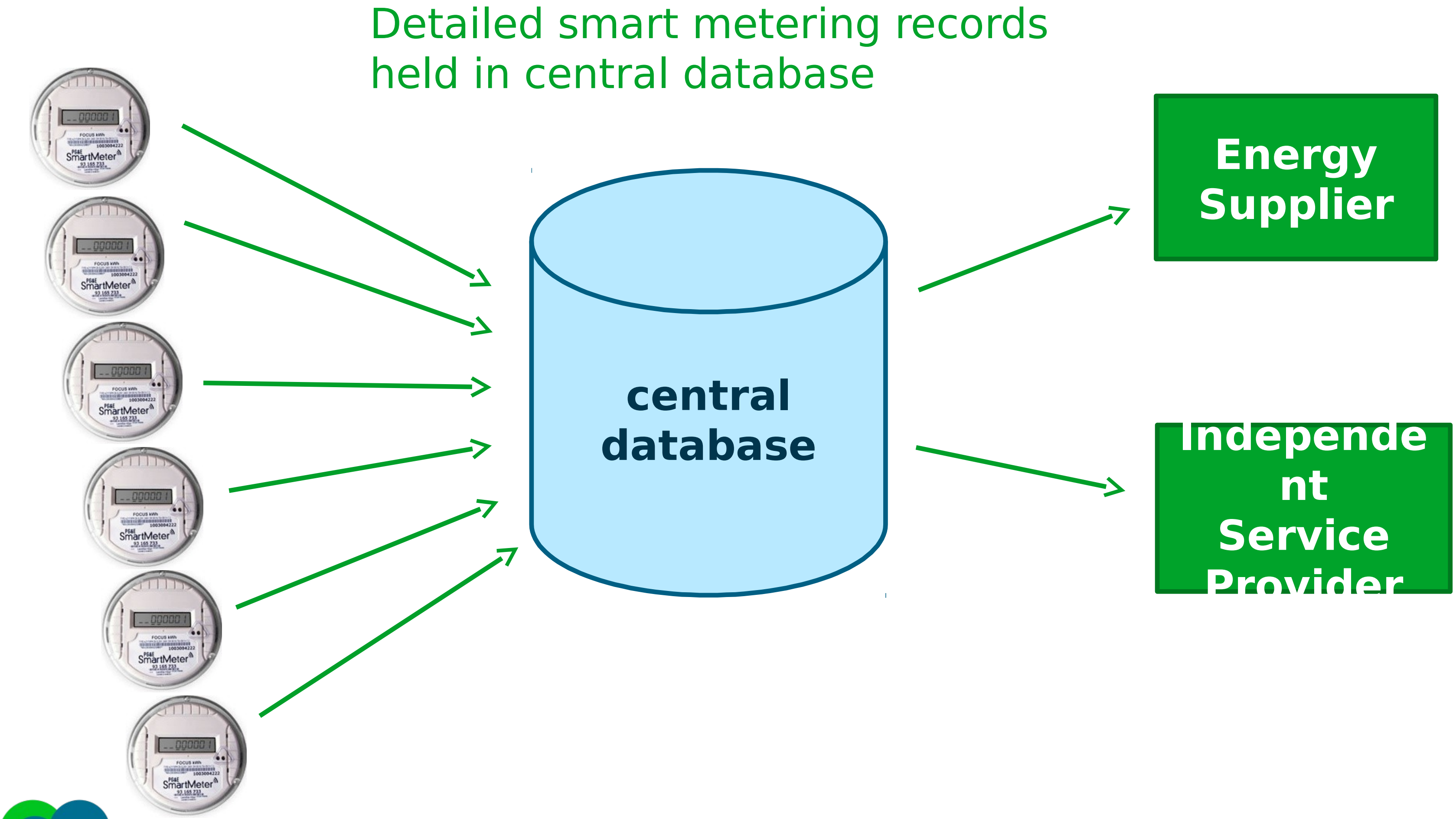
  Which functionality & data do you want to provide?

  When, where and to whom?

  Basis for deciding: a good risk assessment

Example 1: smart metering in the Netherlands

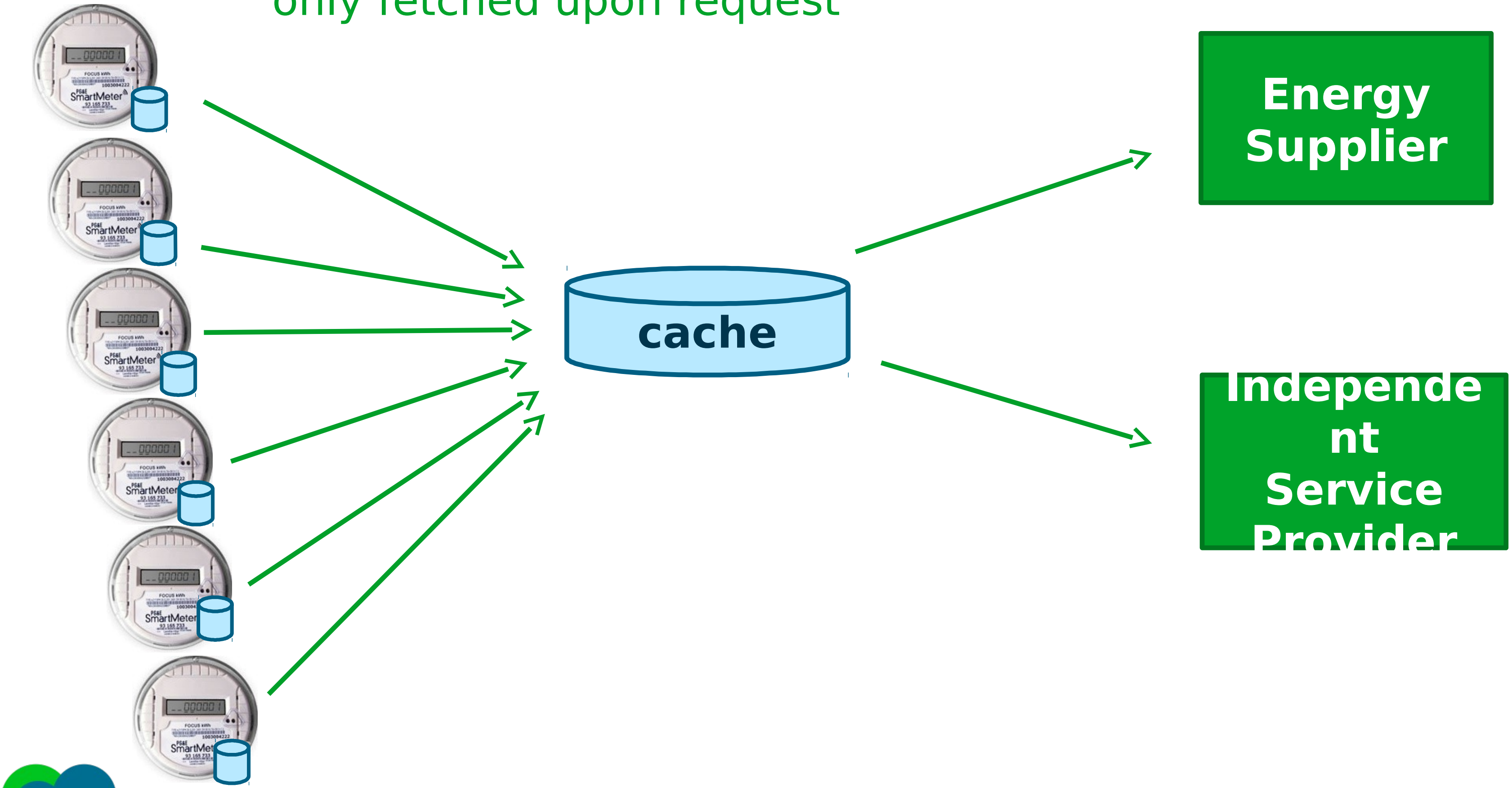
Original planned smart metering information architecture



Example 1: smart metering in the Netherlands

Revised architecture due to privacy concerns

Detailed records kept in the meter itself, only fetched upon request



Example 2: smart metering in the Netherlands

Smart meter can act as remote off switch

- restricting or stopping delivery

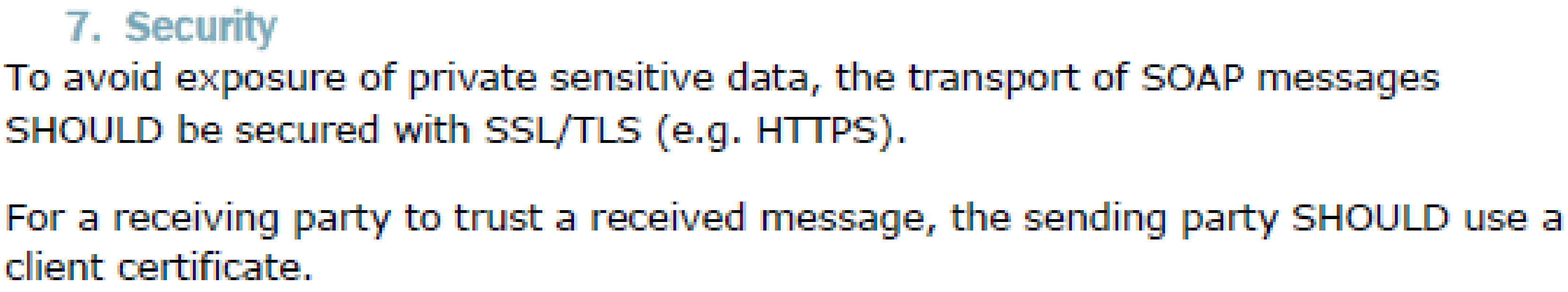
Does this convenient functionality outweigh the security concerns it brings?

After some discussion, smart meters in Netherlands now won’t have this capability.

Rare example of a choice for security over functionality!

Example: Security as after-thought?

- Open Charge Point Protocol (OCPP) by Open Charge Alliance



7. Security

To avoid exposure of private sensitive data, the transport of SOAP messages SHOULD be secured with SSL/TLS (e.g. HTTPS).

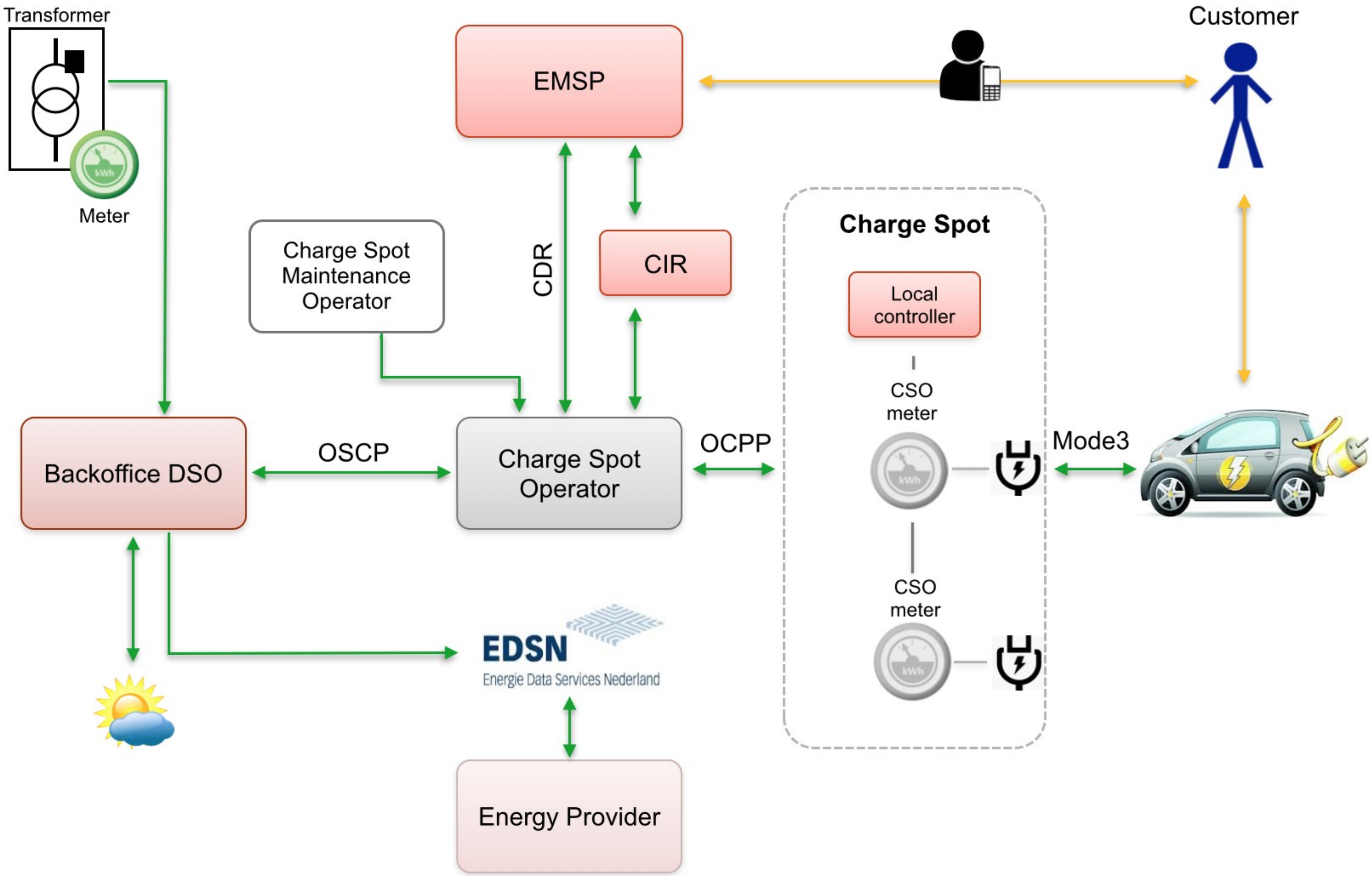
For a receiving party to trust a received message, the sending party SHOULD use a client certificate.

  - NB “SHOULD” not “MUST”
  - This is the *only* mention of security, on the very last (200th!) page

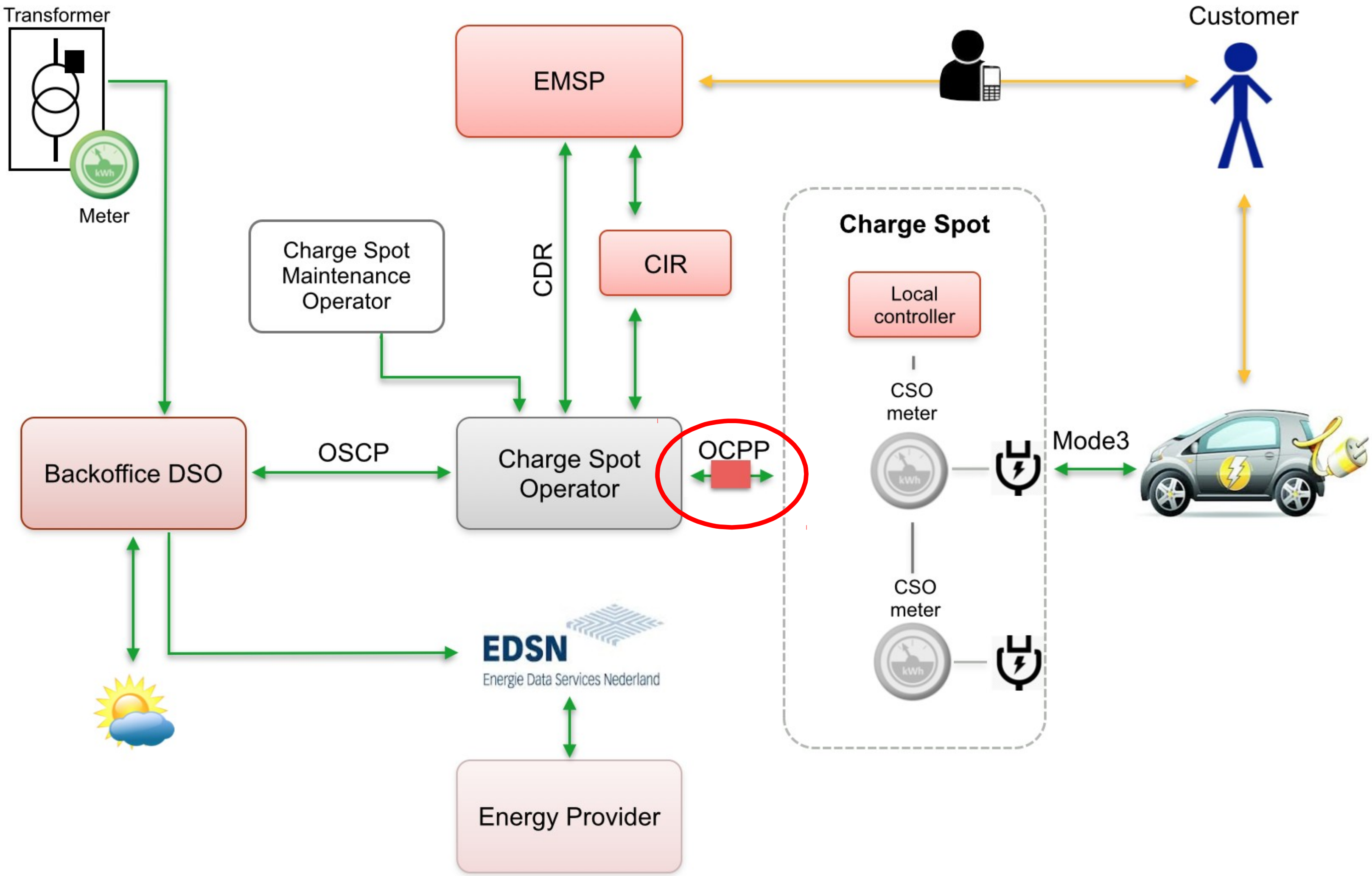
+ using a standard security solution such as TLS is a good idea

– securing this link might not provide end-to-end security we want…

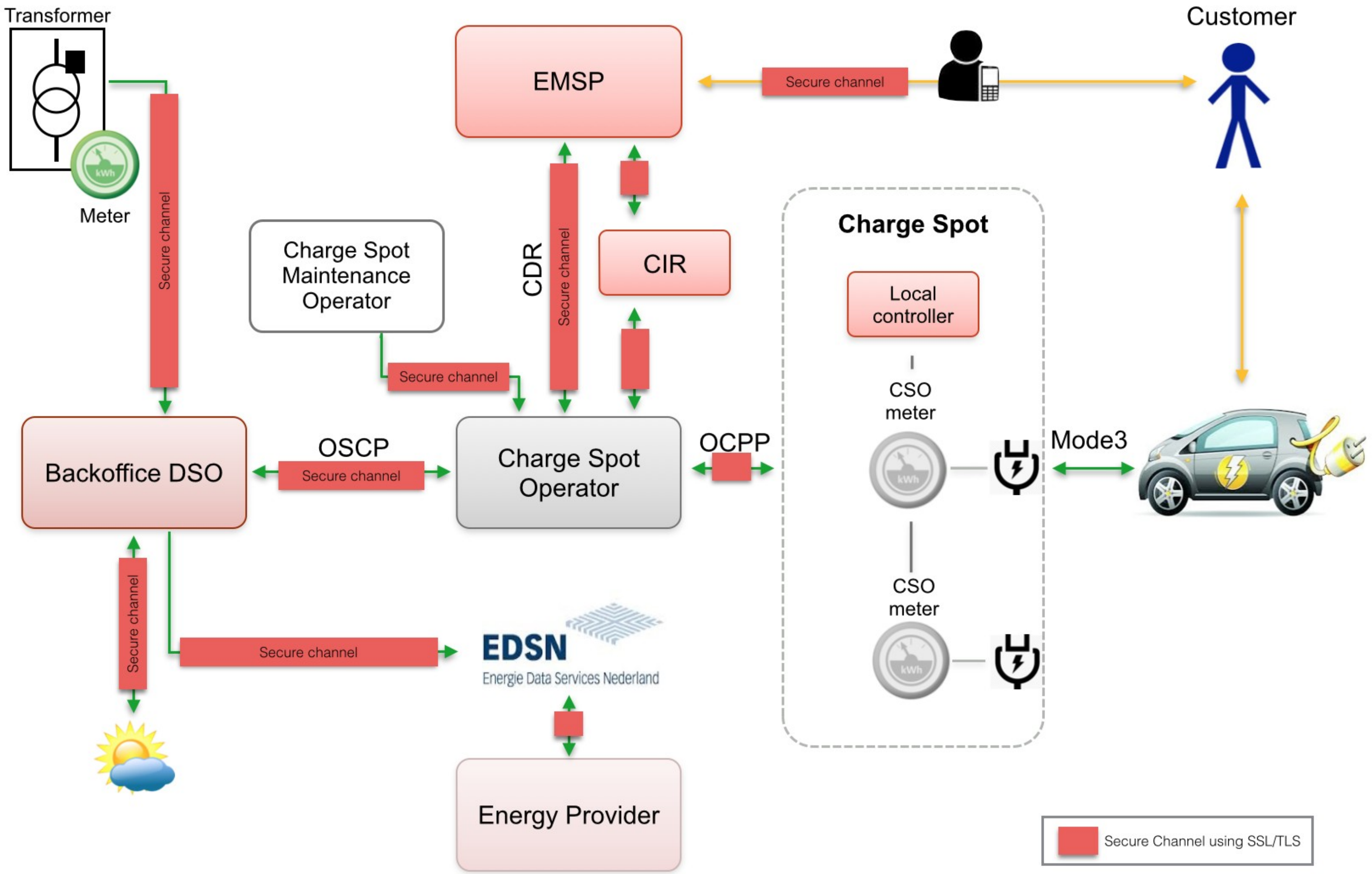
Possible architecture for smart EV charging



Possible architecture for smart EV charging



Possible architecture for smart EV charging



Limits of securing communication links

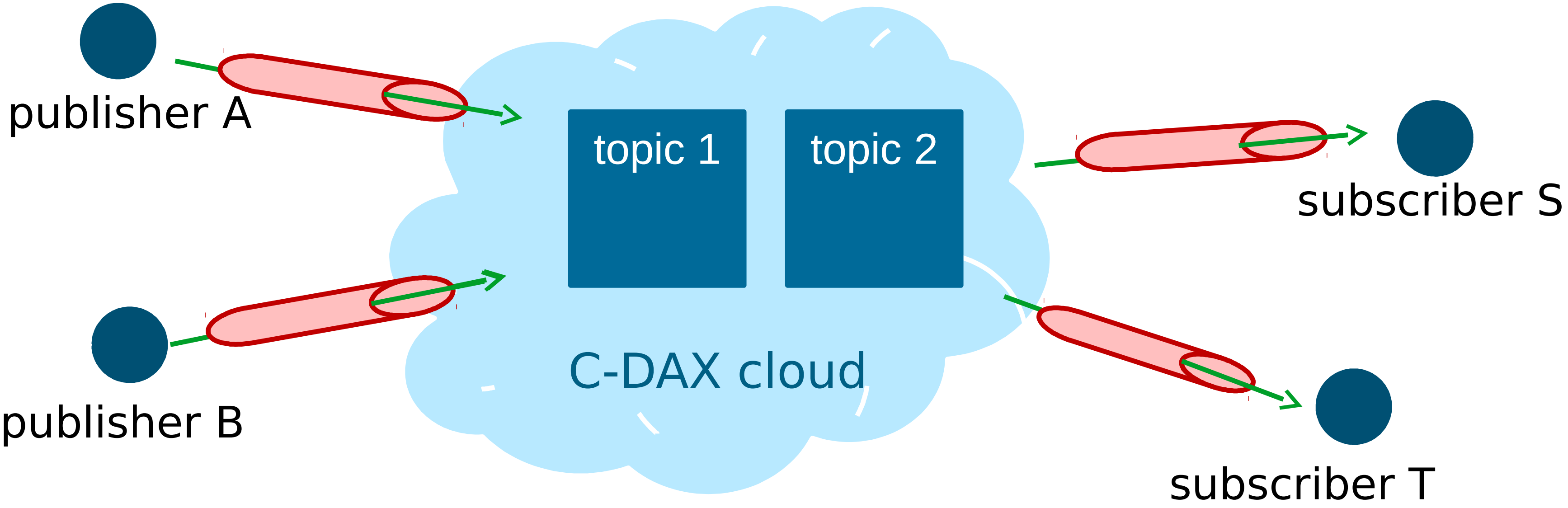
- Securing a communication link using standard solution like TLS is a great idea
  - + we don’t have to trust the underlying infrastructure
    - except for availability
  - + security is ‘automatically’ enforced
  - – once data leaves the pipe, the security of the data is gone
  - – it provides end-to-end security for one link between two parties

- link-by-link security will not provide end-to-end security over multiple links
  - we have to trust all intermediate parties

Securing Information Centric Networking (ICN)

One security benefit:
clients need not know each other's IP address

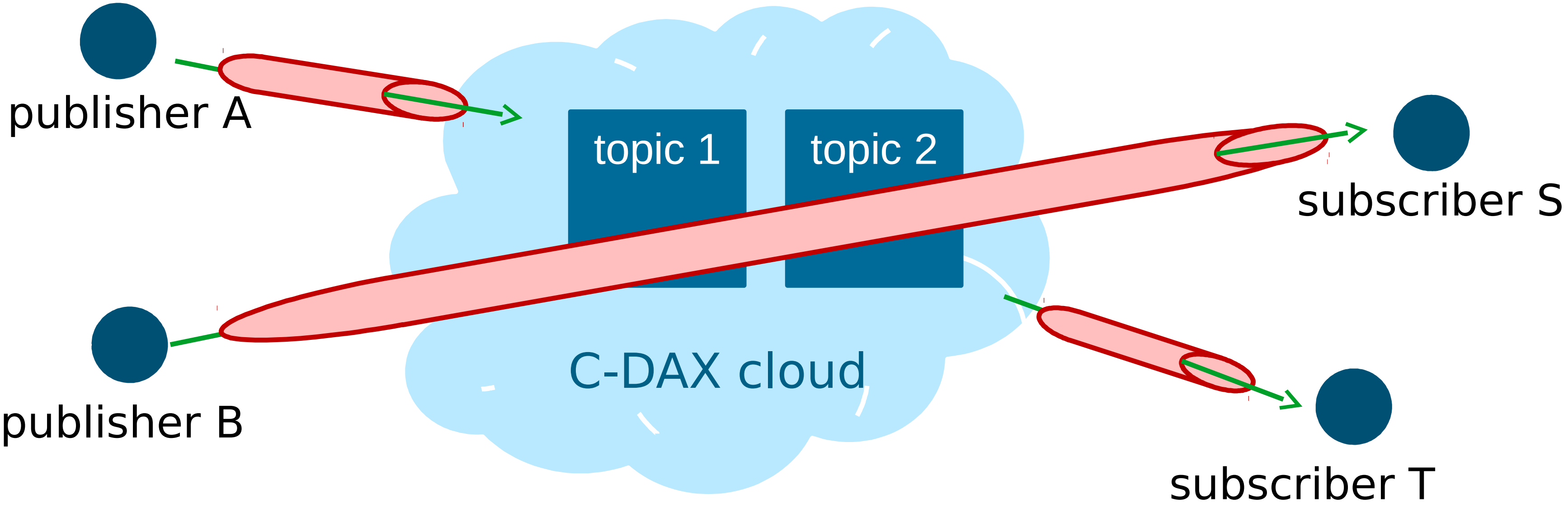
Secure TLS tunnels won't provide end-to-end security
between publishers and subscribers



Securing Information Centric Networking (ICN)

One security benefit:
clients need not know each other's IP address

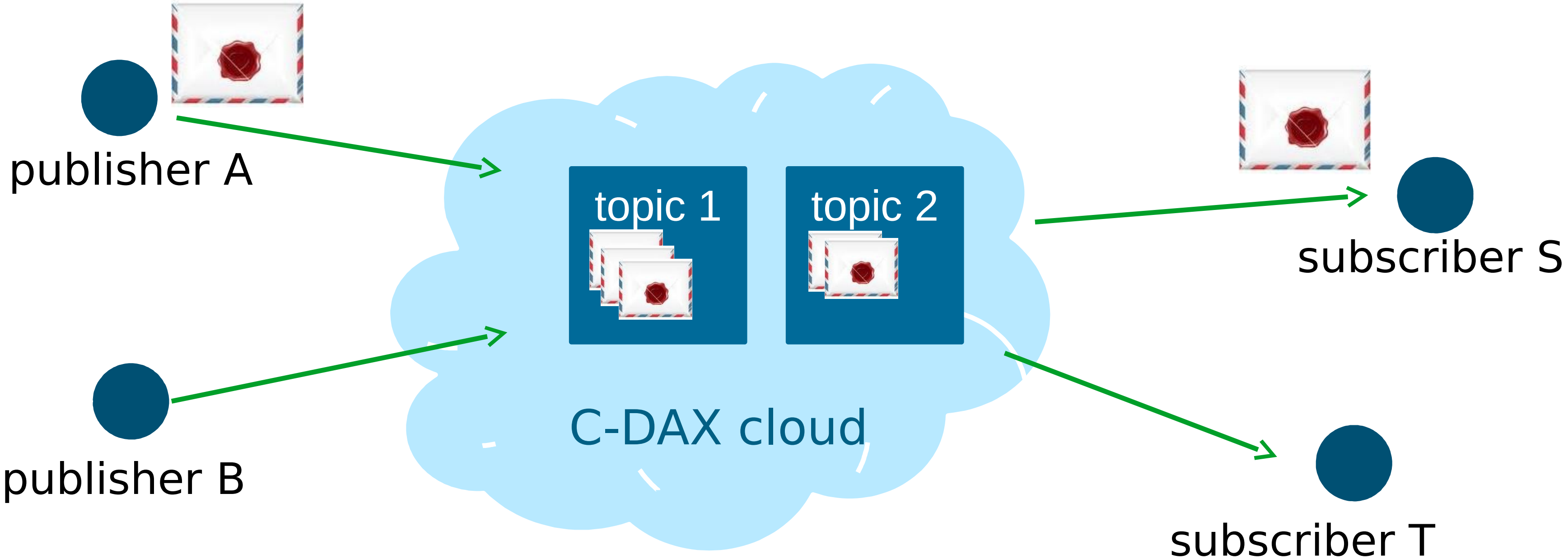
Secure TLS tunnels won't provide end-to-end security
between publishers and subscribers



Securing Information Centric Networking (ICN)

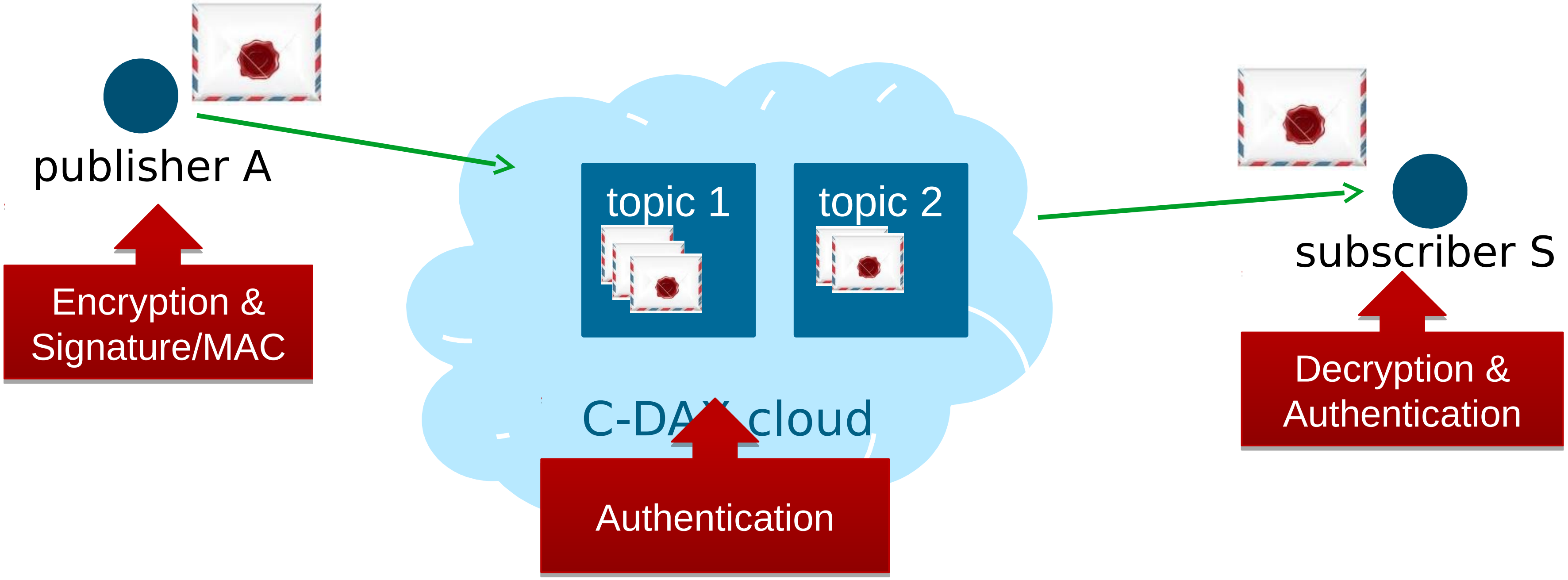
We have to secure the data itself

- Conceptually: data in sealed closed envelope
  - seal gives authenticity/integrity – using digital signature or MAC
  - closed evelope gives confidentiality – using encryption



Securing Information Centric Networking (ICN)

NB no need to trust the C-DAX cloud at all

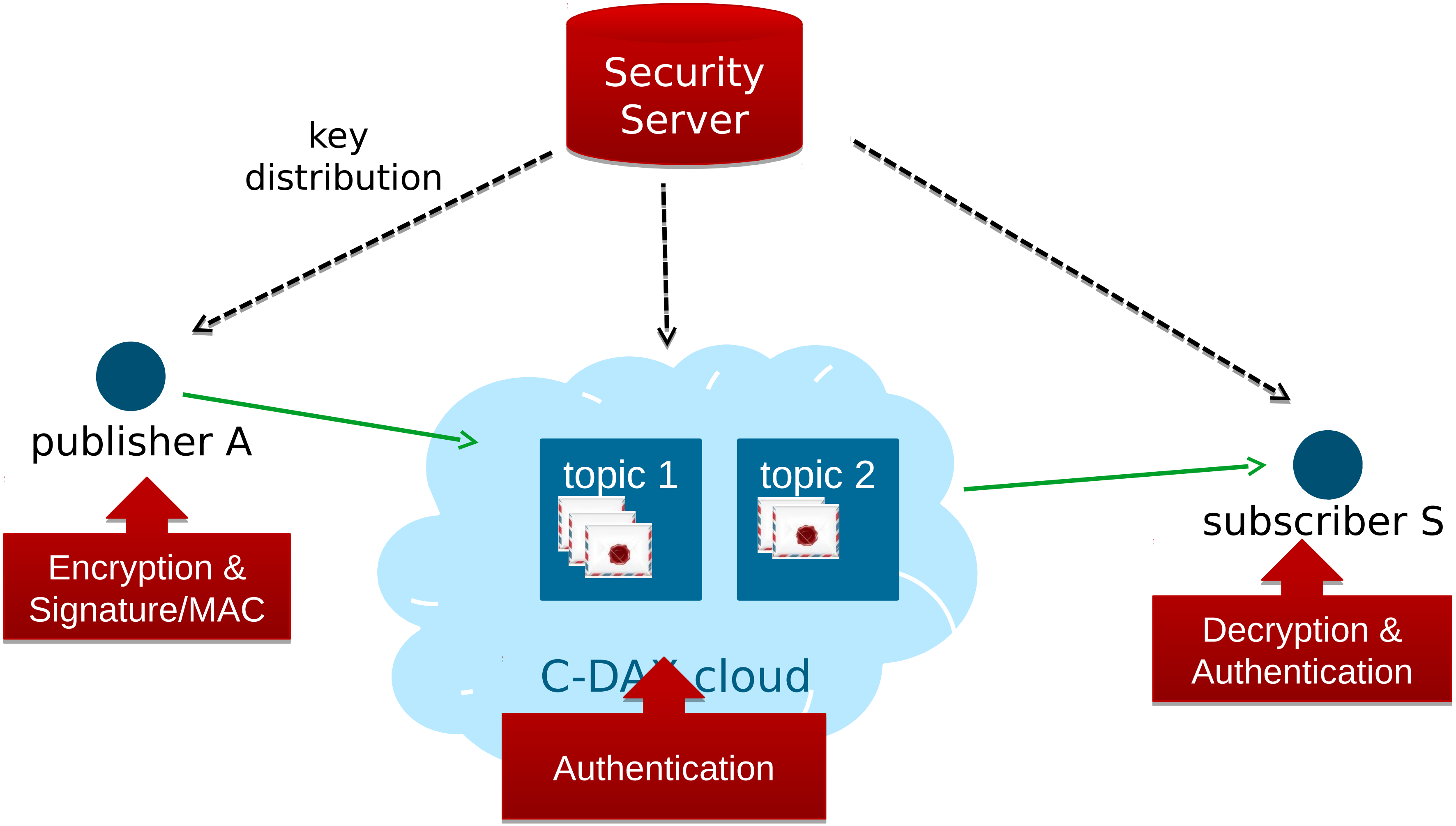


Crypto scheme & key distribution

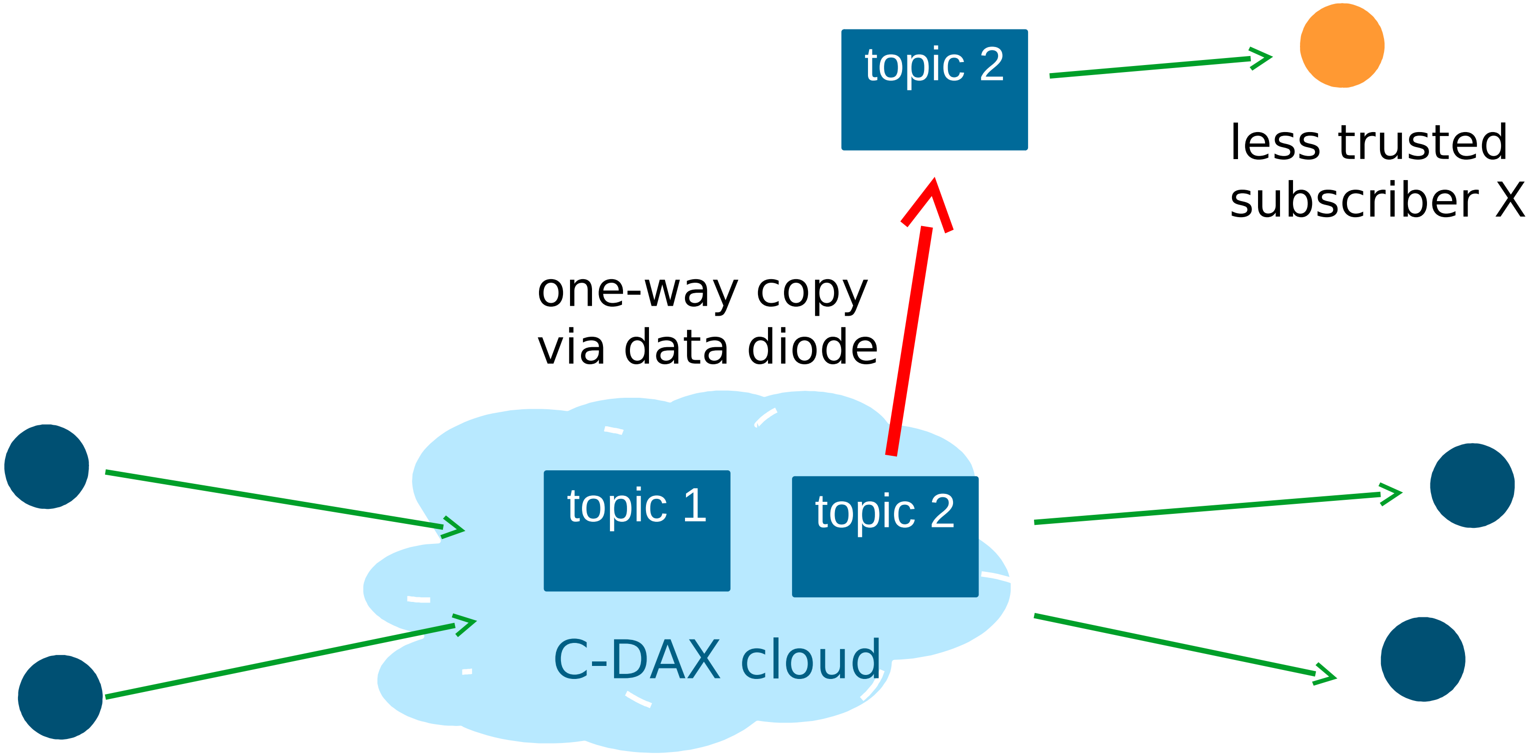
- Choice in cryptographic scheme & key distribution.

  Eg.
  - Long lived public/private keypair per client for authentication (like normal PKI)
  - Symmetric keys per topic
    - different keys for authentication and encryption, so that cloud can authenticate but not eavesdrop
- Choice in which information to reveal on outside of envelope
  - eg to allow filtering, though limited forms of filtering of encrypted data are possible
- We do need to include time stamps or sequence numbers to guarantee order & freshness
  - which we get for free with TLS

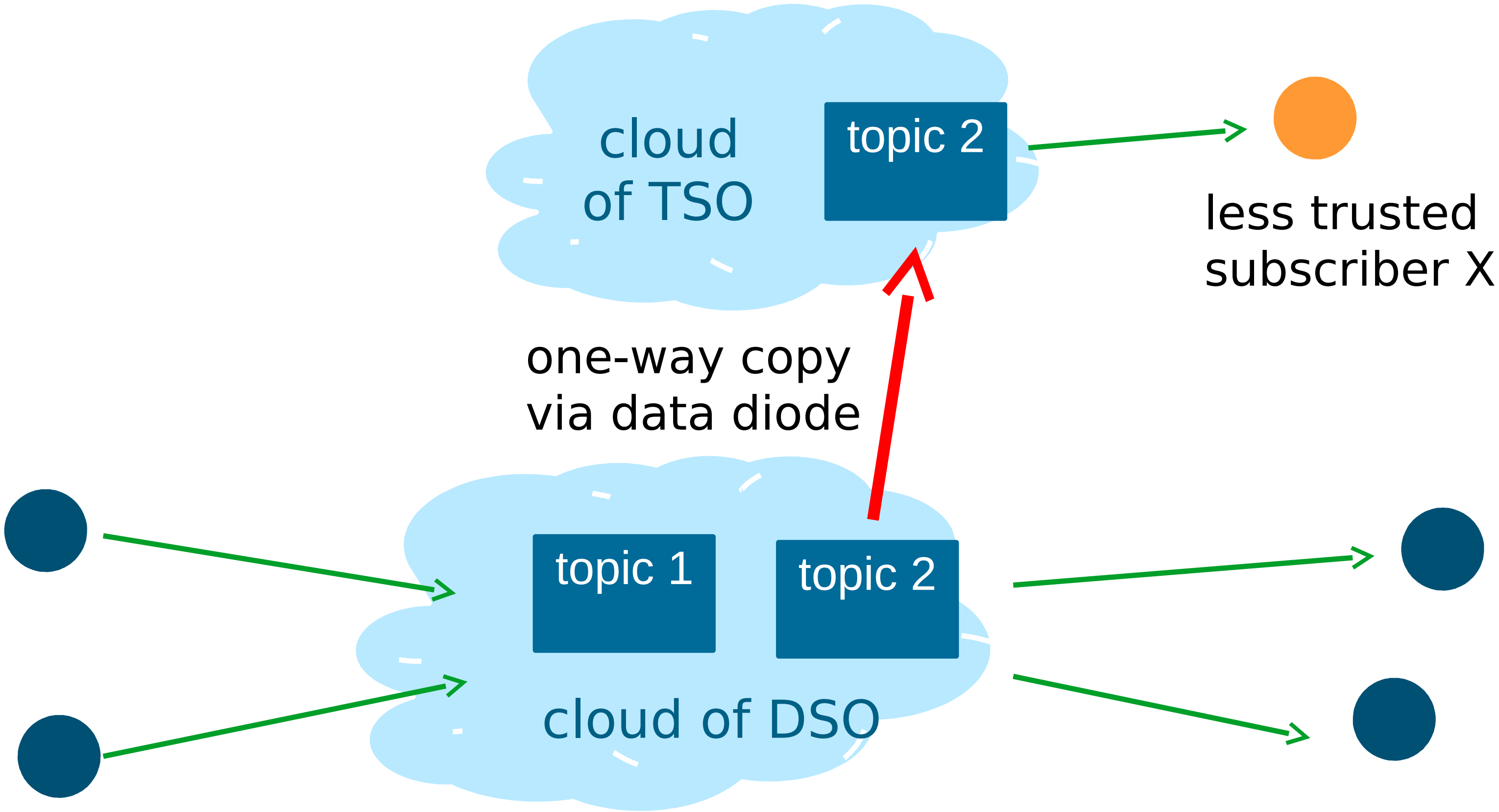
Securing Information Centric Networking (ICN)



Securing Inter Domain Communications



Securing Inter Domain Communications



Conclusions

- *Before* you start securing communications,
  think about the data & functionality you want to expose

- Standard solutions like TLS are for securing connections
  - but securing individual links might not provide the end-to-end security you want…
- Information-centric networking naturally provides end-to-end security

  C-DAX network overlay can provide end-to-end security independent of underlying communication networks

- *After* you secure communications, you still want to secure the end points…