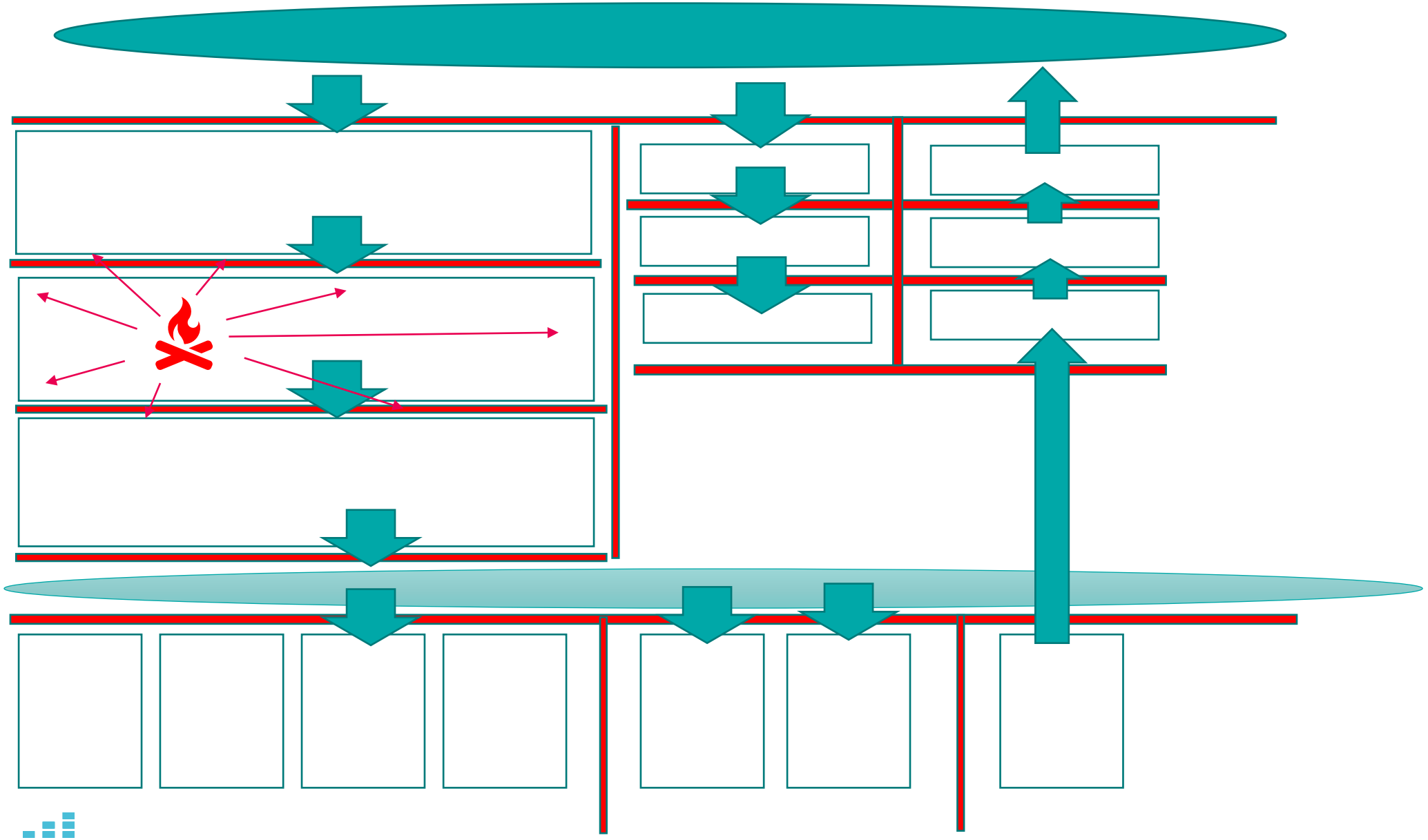
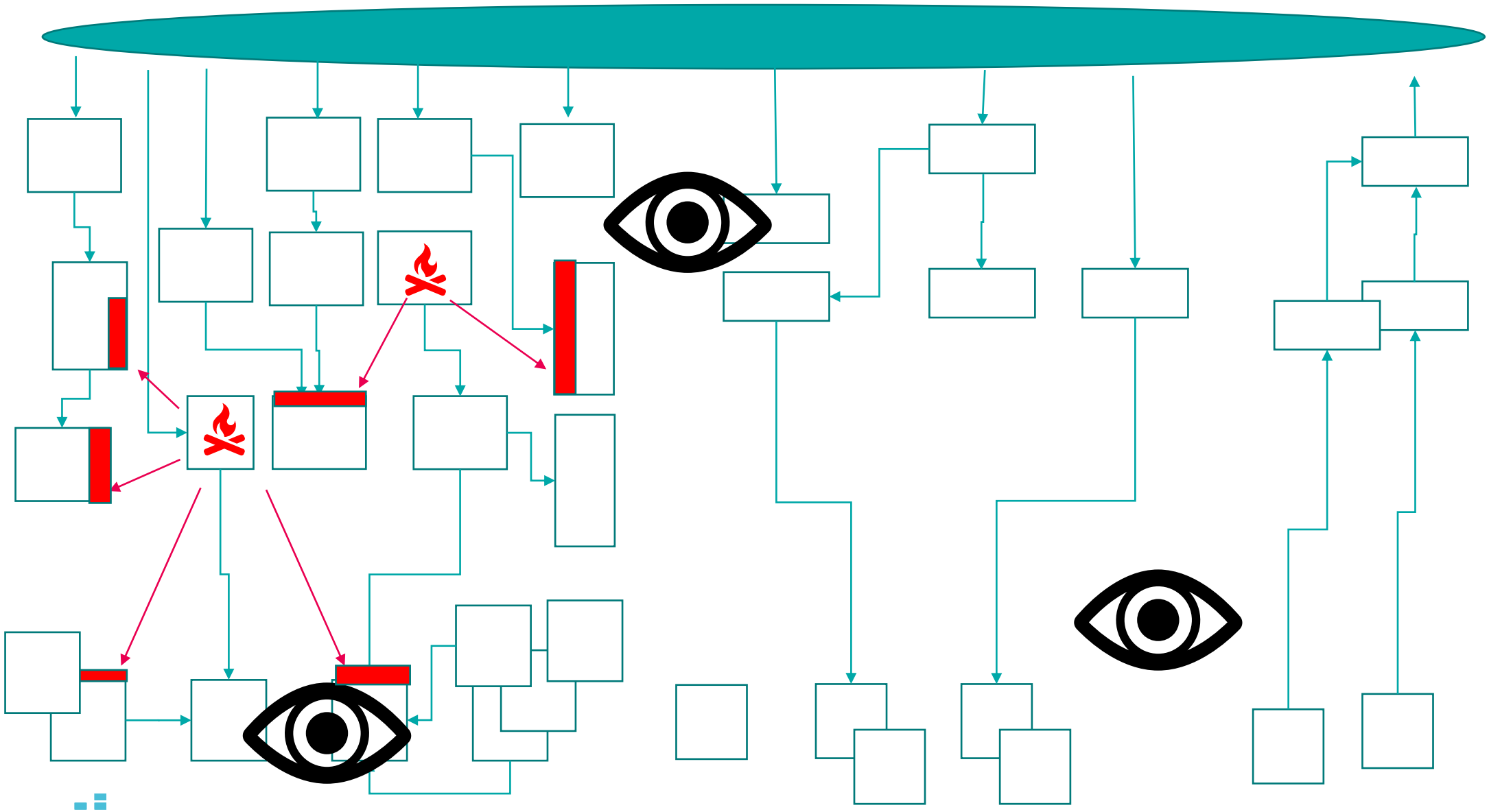
Herbsttagung 2020
Fazit

Paul Schöbi
Zürich, 9. September 2020

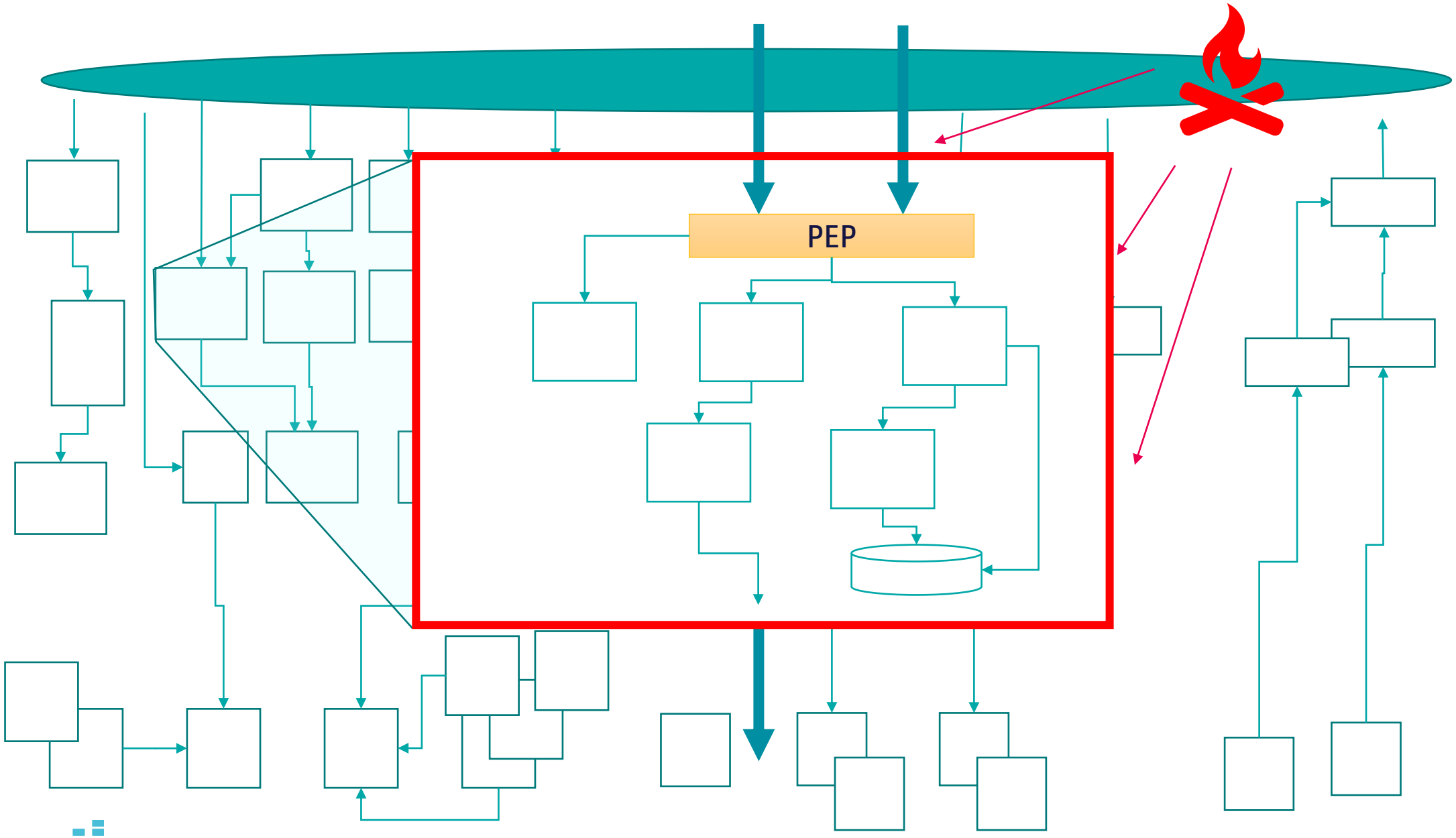
cnlab

Zero Trust bekämpft moderne Angriffe (ATP)





Die Bedeutung der Segmentierung

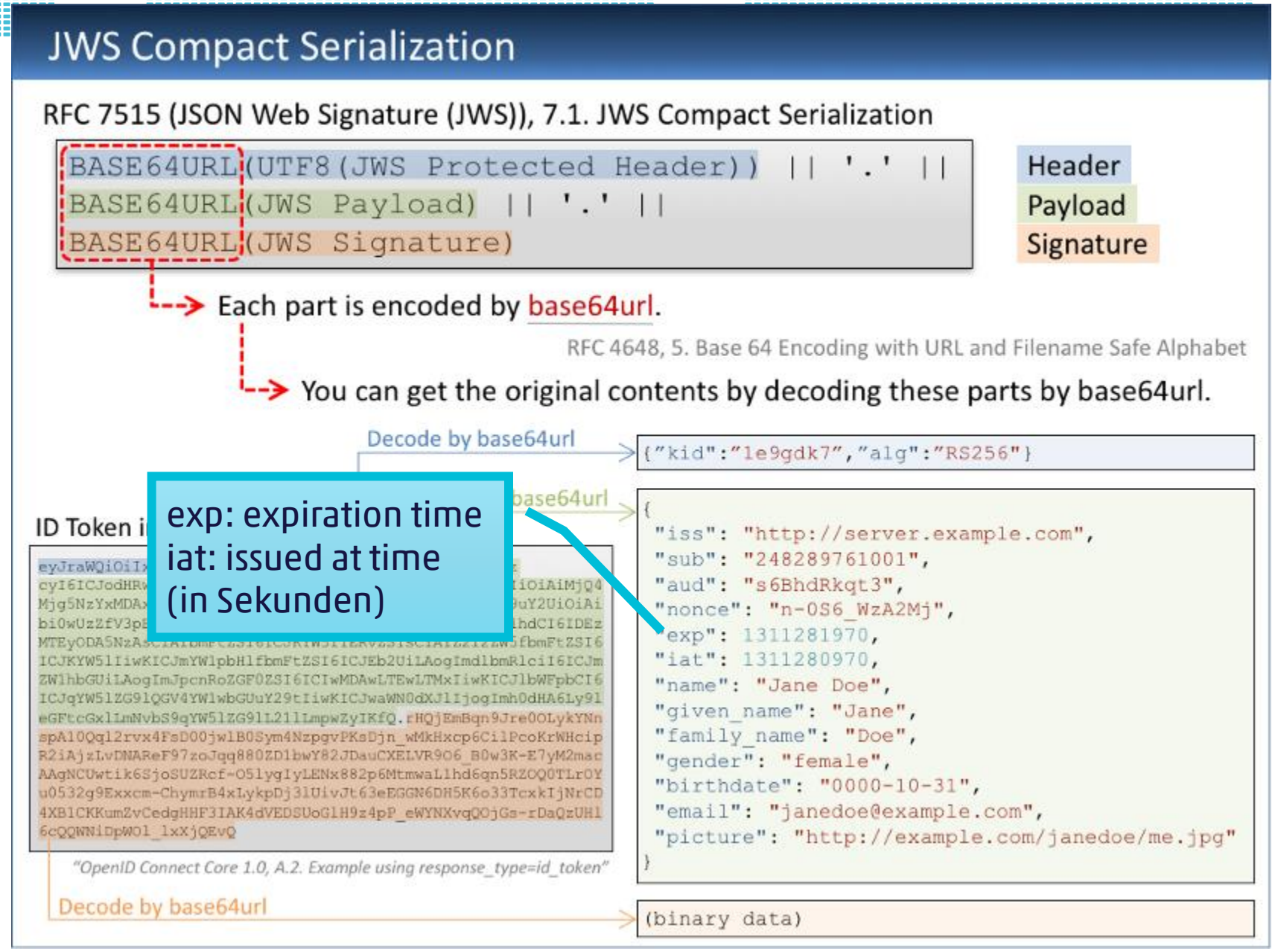

PEP

Beim Token liegt der Teufel im Detail

Token

ID-Token identifiziert Partner (Name, Authentisierungsart, .., Gültigkeit)

Access-Token definiert Zugangs-Rechte (Dienst, Rolle, .., Gültigkeit)



Quelle: https://medium.com/@darutk/understanding-id-token-5f83f50fa02e

Die alten ISO-Layer

Zero-Trust und Layer-Modelle

layer	ISO OSI	TCP/IP	Netzwerk-Protokolle	Traditionelle Security	Zero-Trust
7	Application	Application	HTTP, FTP, HTTPS SMTP, DNS, DHCP	https, DNS-Sec	Fein-granulare Zugangskontrolle
6	Presentation				
5	Session				
4	Transport	Transport	TCP, UDP, ..	Firewalls	?
3	Network	Network	IP, IPSec	ACLs, VPNs	?
2	Data Link	Physical	Ethernet, WLAN	ACLs	?
1	Physical		1000BASE-T	Pysischer Schutz	?

Und nun die Thesen:

PEPs schützen (kleine) Zonen.
- Zonen haben bedeutet Segmentierung.
- Die Segmentierung muss «dicht» sein.

Tokens müssen richtig eingesetzt werden.
- Die Standards definieren nur Teilbereiche.
- Sichere Sessionen mit Token sind nicht einfach.

Zero Trust wird eingesetzt:
- Beim Neuaufbau bleiben die Netze flexibel.
- Es funktioniert mit traditionellen Systemen zusammen.

Das alte ISO-OSI-Layer-Modell kann man immer noch brauchen.

Vielen Dank für Ihre Aufmerksamkeit_

info@cnlab-security.ch
+41 55 214 33 40

cnlab security AG
Obere Bahnhofstrasse 32b
CH-8640 Rapperswil-Jona
Switzerland

cnlab