



Herbsttagung 2020

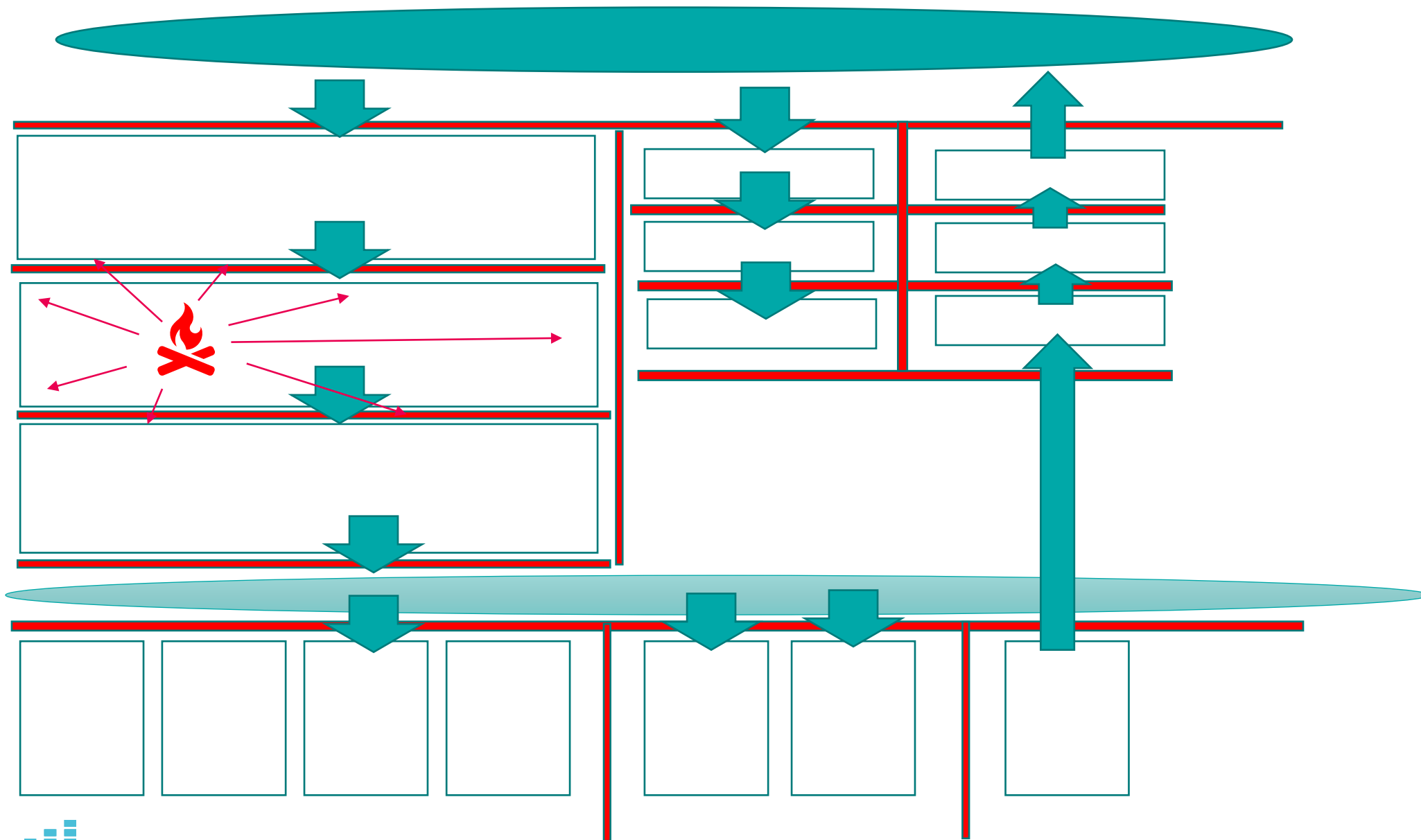
Fazit

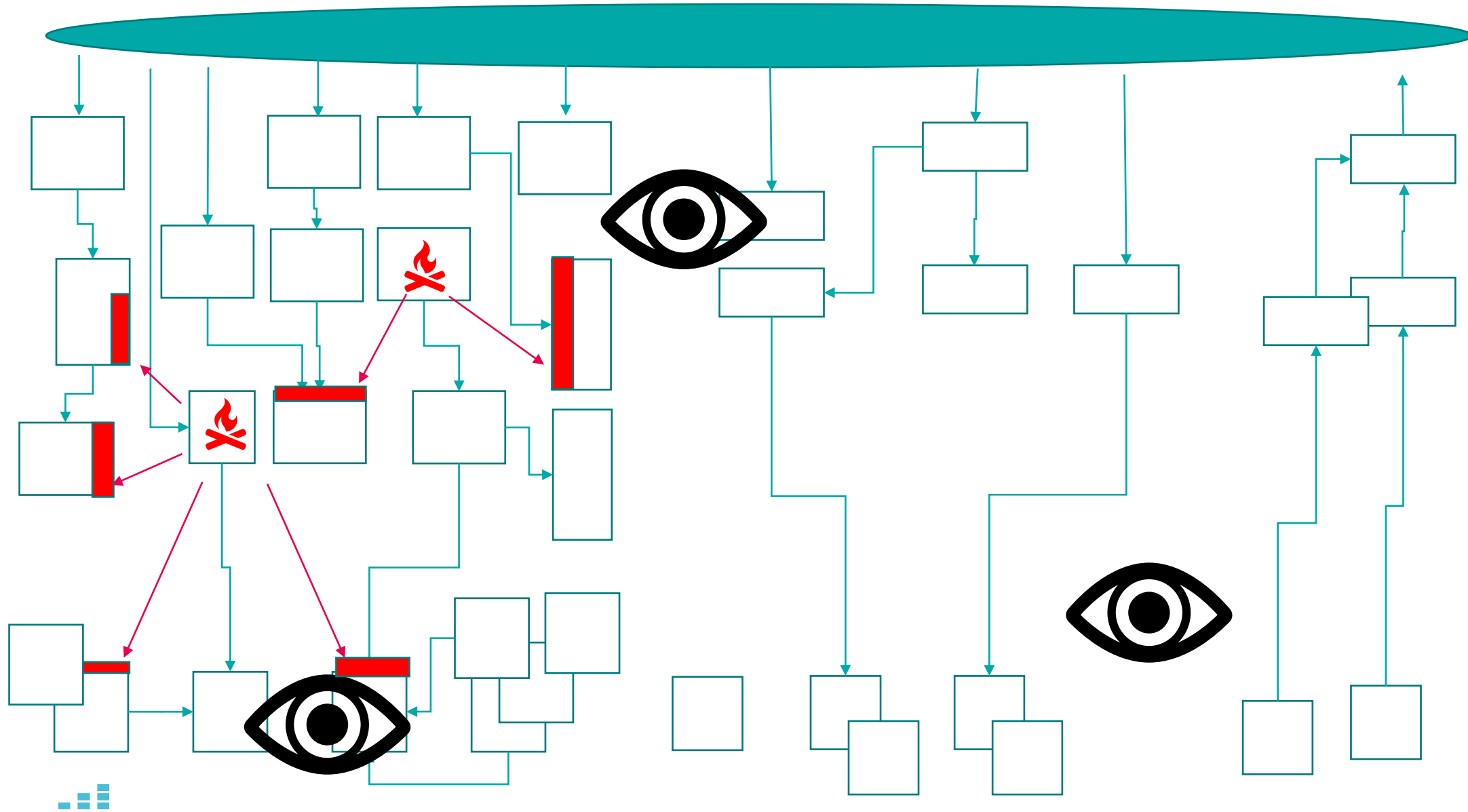
Paul Schöbi
Zürich, 9. September 2020



Zero Trust bekämpft moderne Angriffe (ATP)



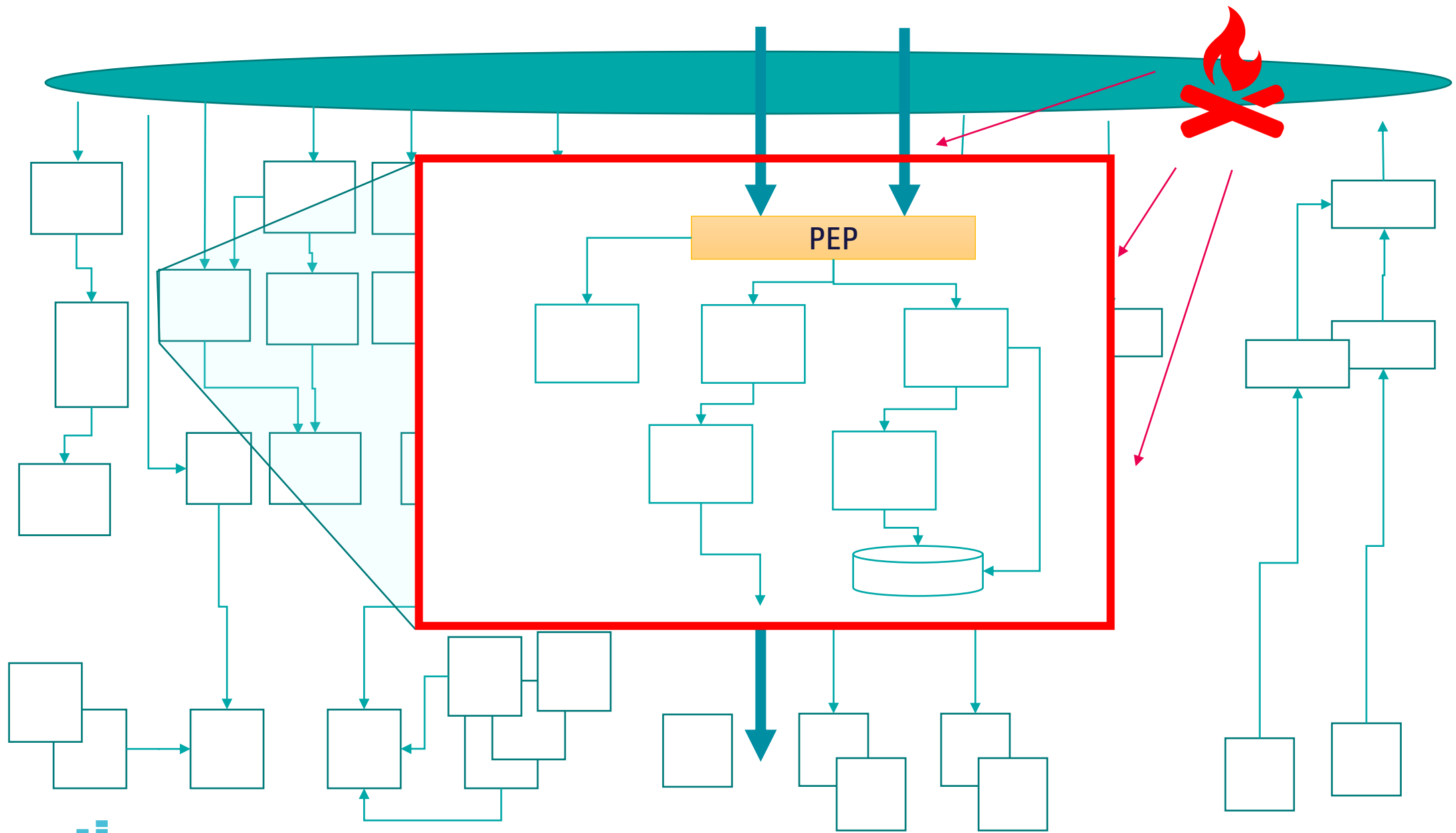






Die Bedeutung der Segmentierung







Beim Token liegt der Teufel im Detail



Token

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

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

JWS Compact Serialization

RFC 7515 (JSON Web Signature (JWS)), 7.1. JWS Compact Serialization

```
BASE64URL(UTF8(JWS Protected Header)) || '.' ||  
BASE64URL(JWS Payload) || '.' ||  
BASE64URL(JWS Signature)
```

Header
Payload
Signature

Each part is encoded by base64url.
You can get the original contents by decoding these parts by base64url.

RFC 4648, 5. Base 64 Encoding with URL and Filename Safe Alphabet



exp: expiration time
iat: issued at time
(in Sekunden)

"OpenID Connect Core 1.0, A.2. Example using response_type=id_token"





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	https, DNS-Sec	Fein-granulare Zugangskontrolle
6	Presentation		SMTP, DNS, DHCP		
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