

WIRESHARK EDUCATION DAY – Olten CH 2026

MACsec

Überblick über MACsec und Analyse mit Wireshark

Benjamin Pfister

The Wireshark logo, featuring a stylized white shark fin icon above the word "WIRESHARK" in a bold, white, sans-serif font.

WIRESHARK

Sponsored by:  

Über mich



■ Benjamin Pfister

■ Leiter Netze & Telekommunikation

■ IT-Consultant / Trainer

■ Freier Autor

■ Vater von BabyShark





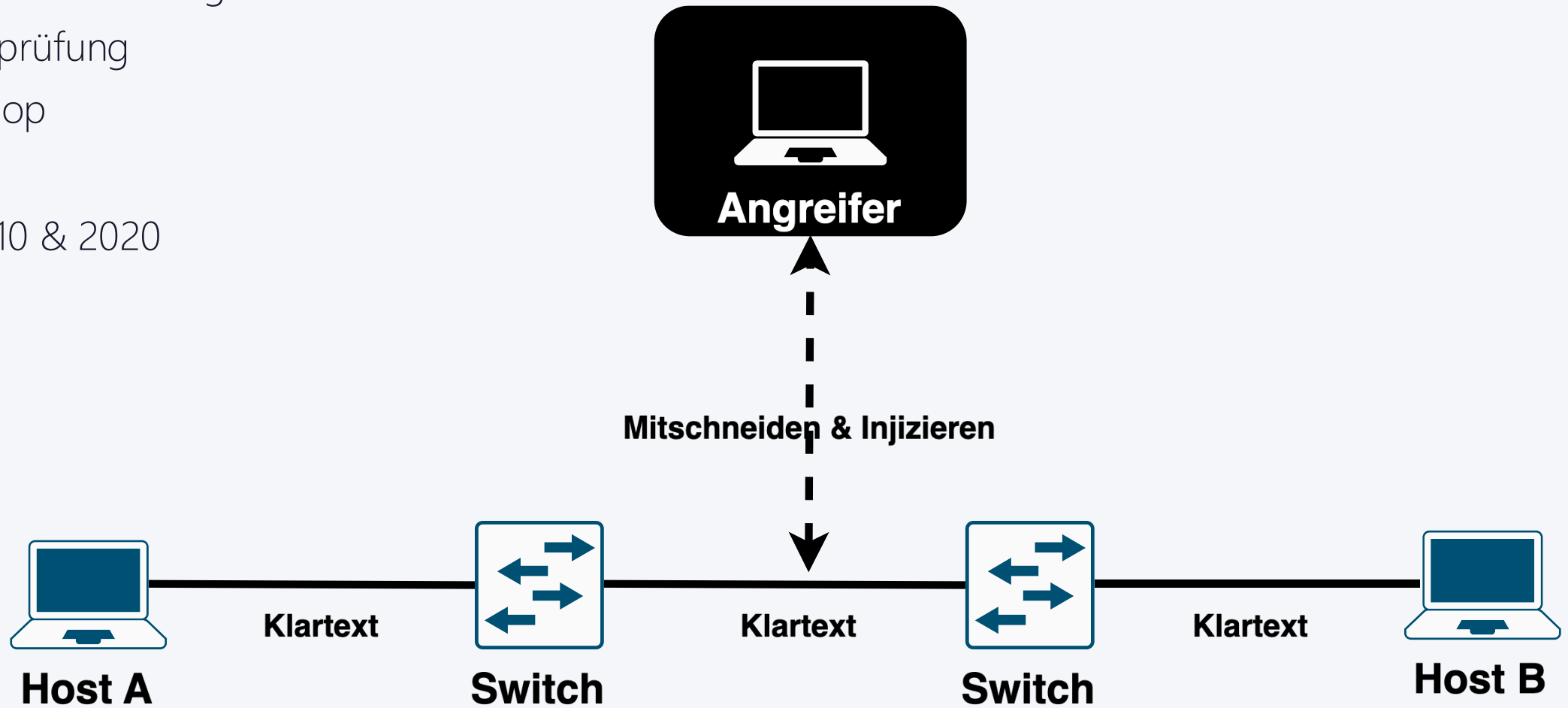
- Was ist MACsec?
- Anwendungsszenarien
- Frame-Aufbau
- Schlüsselverteilung & Analyse

Was ist MACsec?

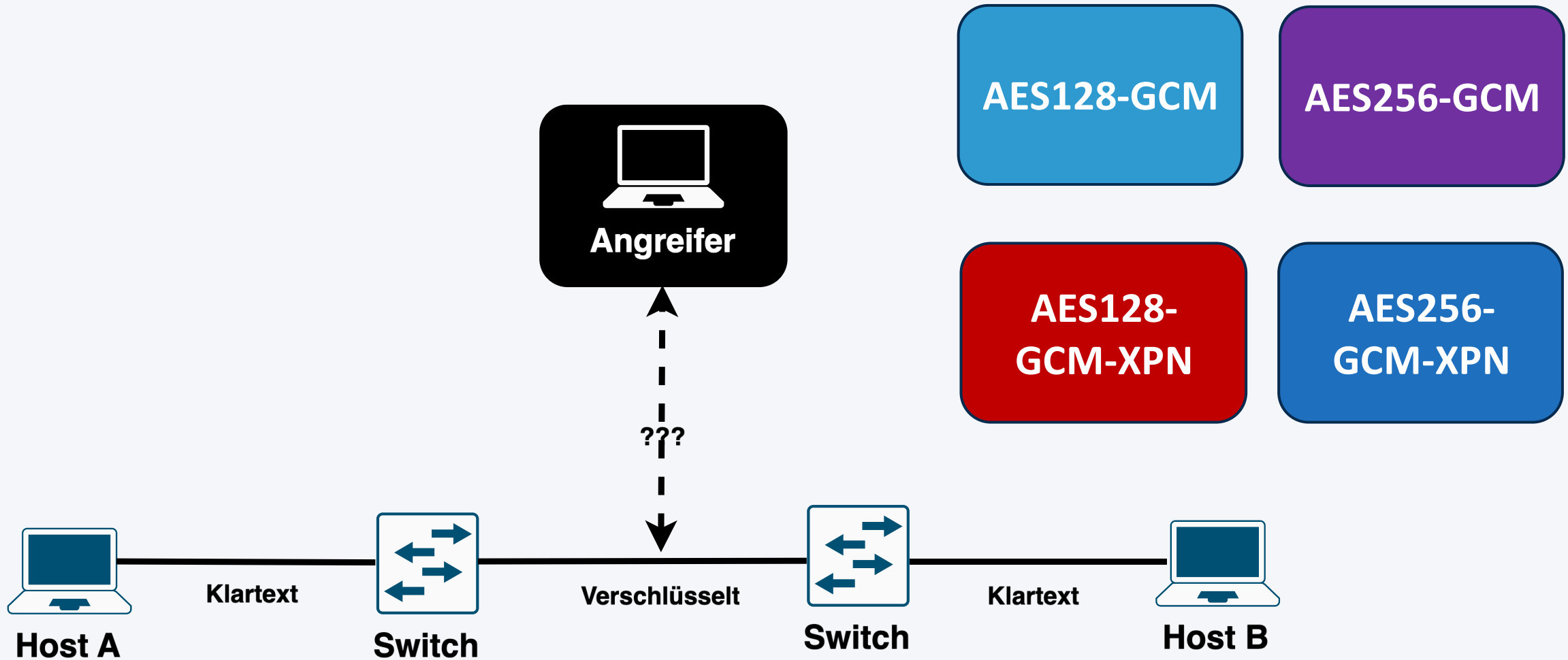
Was ist MACsec?



- Layer 2 Verschlüsselung
- Integritätsprüfung
- Hop-by-Hop
- 802.1AE
- 802.1X-2010 & 2020



Was ist MACsec?



Was ist MACsec?



No.	Time	Delta	Source	Destination	Protocol	Packet number	Length	Info
138	109.2456884...	0.144809668	aa:c1:ab:6e:91:a9	Nearest-non-TPMR-B...	EAPOL...		182	Live Peer List, MACsec SAK Use, XPN, ICV Indicator
139	109.7206302...	0.474941772	aa:c1:ab:31:74:d4	aa:c1:ab:92:ca:4b	MACSEC	29	134	MACsec frame [UNVERIFIED]
140	110.7223165...	1.001686353	aa:c1:ab:31:74:d4	aa:c1:ab:92:ca:4b	MACSEC	30	134	MACsec frame [UNVERIFIED]
141	111.1236656...	0.401349104	aa:c1:ab:1d:d3:cc	Nearest-non-TPMR-B...	EAPOL...		170	Key Server, Live Peer List, MACsec SAK Use, ICV Indicator
142	111.2667838...	0.143118188	aa:c1:ab:6e:91:a9	Nearest-non-TPMR-B...	EAPOL...		182	Live Peer List, MACsec SAK Use, XPN, ICV Indicator
143	111.7235352...	0.456751369	aa:c1:ab:31:74:d4	aa:c1:ab:92:ca:4b	MACSEC	31	134	MACsec frame [UNVERIFIED]
144	112.7250290...	1.001493762	aa:c1:ab:31:74:d4	aa:c1:ab:92:ca:4b	MACSEC	32	134	MACsec frame [UNVERIFIED]
145	113.1420144...	0.416985478	aa:c1:ab:1d:d3:cc	Nearest-non-TPMR-B...	EAPOL...		170	Key Server, Live Peer List, MACsec SAK Use, ICV Indicator
146	113.2854685...	0.143454060	aa:c1:ab:6e:91:a9	Nearest-non-TPMR-B...	EAPOL...		182	Live Peer List, MACsec SAK Use, XPN, ICV Indicator
147	113.7271843...	0.441715835	aa:c1:ab:31:74:d4	aa:c1:ab:92:ca:4b	MACSEC	33	134	MACsec frame [UNVERIFIED]
148	114.7338503...	1.006665963	aa:c1:ab:31:74:d4	aa:c1:ab:92:ca:4b	MACSEC	34	134	MACsec frame [UNVERIFIED]
149	115.1632003...	0.429350032	aa:c1:ab:1d:d3:cc	Nearest-non-TPMR-B...	EAPOL...		170	Key Server, Live Peer List, MACsec SAK Use, ICV Indicator
150	115.3079082...	0.144707875	aa:c1:ab:6e:91:a9	Nearest-non-TPMR-B...	EAPOL...		182	Live Peer List, MACsec SAK Use, XPN, ICV Indicator
151	115.7303435...	0.422435263	aa:c1:ab:31:74:d4	aa:c1:ab:92:ca:4b	MACSEC	35	134	MACsec frame [UNVERIFIED]
152	116.7320523...	1.001708871	aa:c1:ab:31:74:d4	aa:c1:ab:92:ca:4b	MACSEC	36	134	MACsec frame [UNVERIFIED]
153	117.1830572...	0.451004832	aa:c1:ab:1d:d3:cc	Nearest-non-TPMR-B...	EAPOL...		170	Key Server, Live Peer List, MACsec SAK Use, ICV Indicator
154	117.3307254...	0.147668235	aa:c1:ab:6e:91:a9	Nearest-non-TPMR-B...	EAPOL...		182	Live Peer List, MACsec SAK Use, XPN, ICV Indicator
155	117.7329811...	0.402255733	aa:c1:ab:31:74:d4	aa:c1:ab:92:ca:4b	MACSEC	37	134	MACsec frame [UNVERIFIED]
156	118.7347696...	1.001788422	aa:c1:ab:31:74:d4	aa:c1:ab:92:ca:4b	MACSEC	38	134	MACsec frame [UNVERIFIED]
157	119.2020160...	0.469246440	aa:c1:ab:1d:d3:cc	Nearest-non-TPMR-B...	EAPOL...		170	Key Server, Live Peer List, MACsec SAK Use, ICV Indicator

> Frame 147: Packet. 134 bytes on wire (1072 bits). 134 bytes captured (1072 bits) on interface e1-1-c1-1, id 0

✓ Ethernet II, Src: aa:c1:ab:31:74:d4 (aa:c1:ab:31:74:d4), Dst: aa:c1:ab:92:ca:4b (aa:c1:ab:92:ca:4b)

> Destination: aa:c1:ab:92:ca:4b (aa:c1:ab:92:ca:4b)

> Source: aa:c1:ab:31:74:d4 (aa:c1:ab:31:74:d4)

Type: 802.1Q Virtual LAN (0x8100)

[Stream index: 3]

> 802.1Q Virtual LAN, PRI: 0, DEI: 0, ID: 28

✓ 802.1AE Security Tag

> 0010 11.. = TCI: 0x0b, VER: 0x0, SC, E, C

.... ..00 = AN: 0x0

Short length: 0

Packet number: 33

System Identifier: aa:c1:ab:1d:d3:cc (aa:c1:ab:1d:d3:cc)

Port Identifier: 1

ICV: 535f14e94be66716bed0f39462c5bb0f

> [Verification Info]

> Data (86 bytes)

Verschlüsselte
ICMP-Übertragung

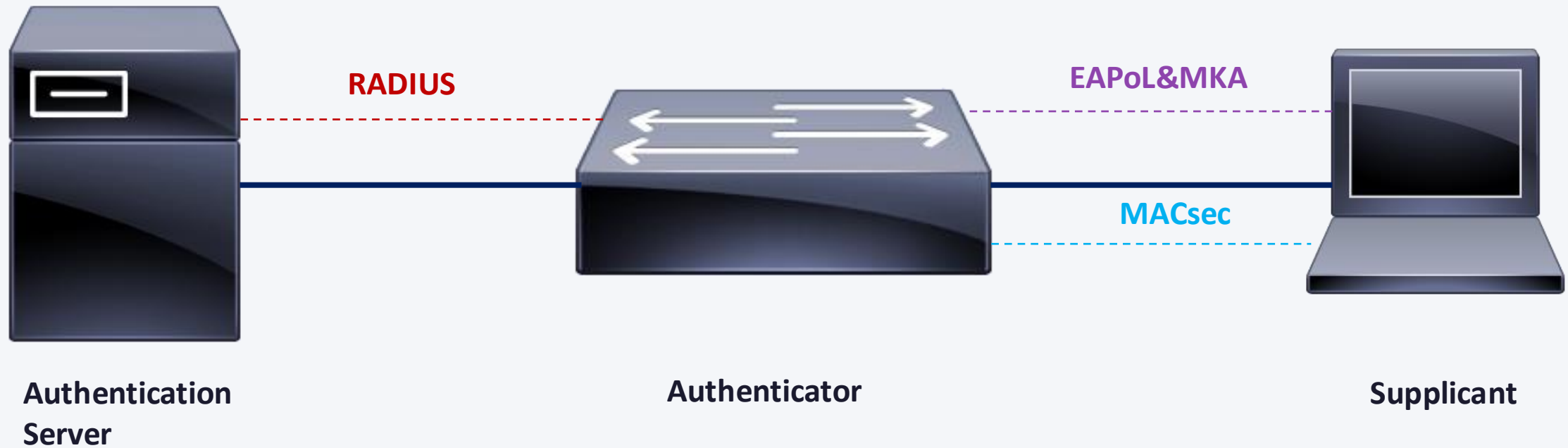
Unverschlüsselter
Ethernet- und
802.1Q Header im
Clear Mode

Verschlüsselter
MACsec-Header,
ICV Trailer und
Nutzdaten

Anwendungsszenarien

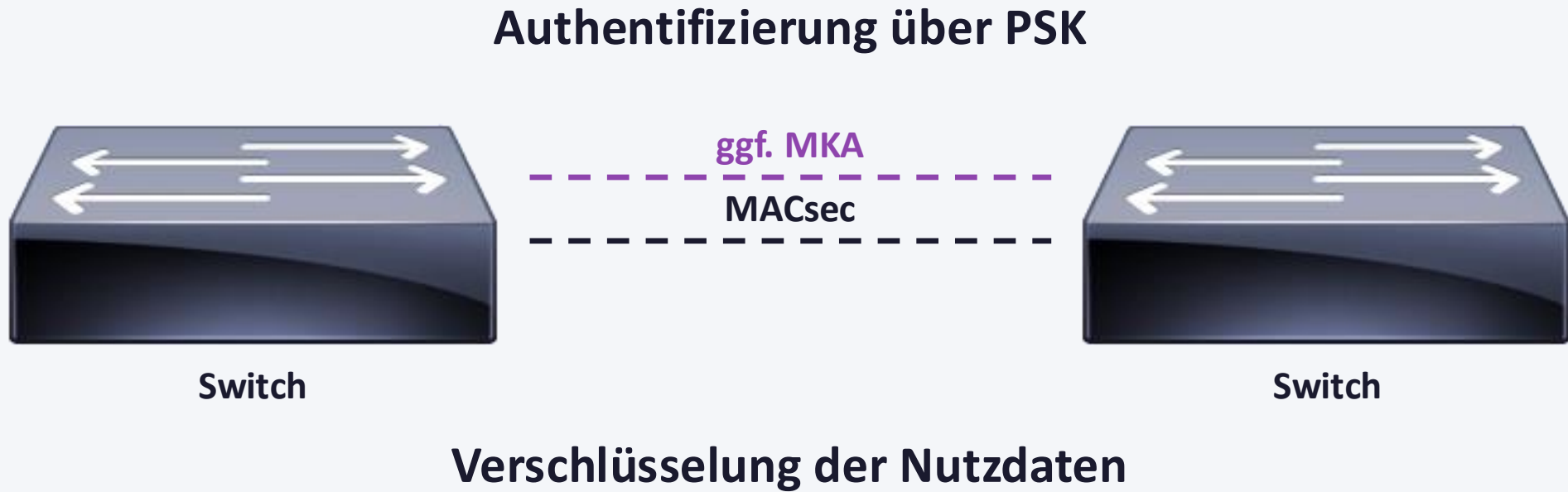


Switch <-> Endgerät





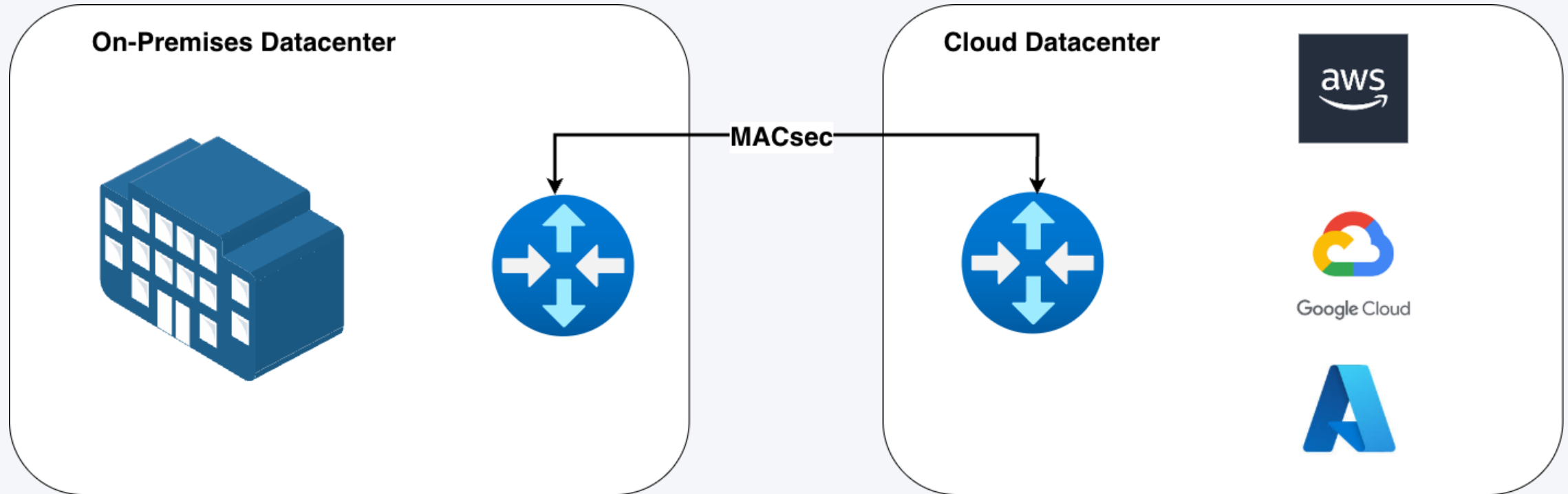
Switch <-> Switch



Anwendungsszenarien



Anbindung Cloud-Provider



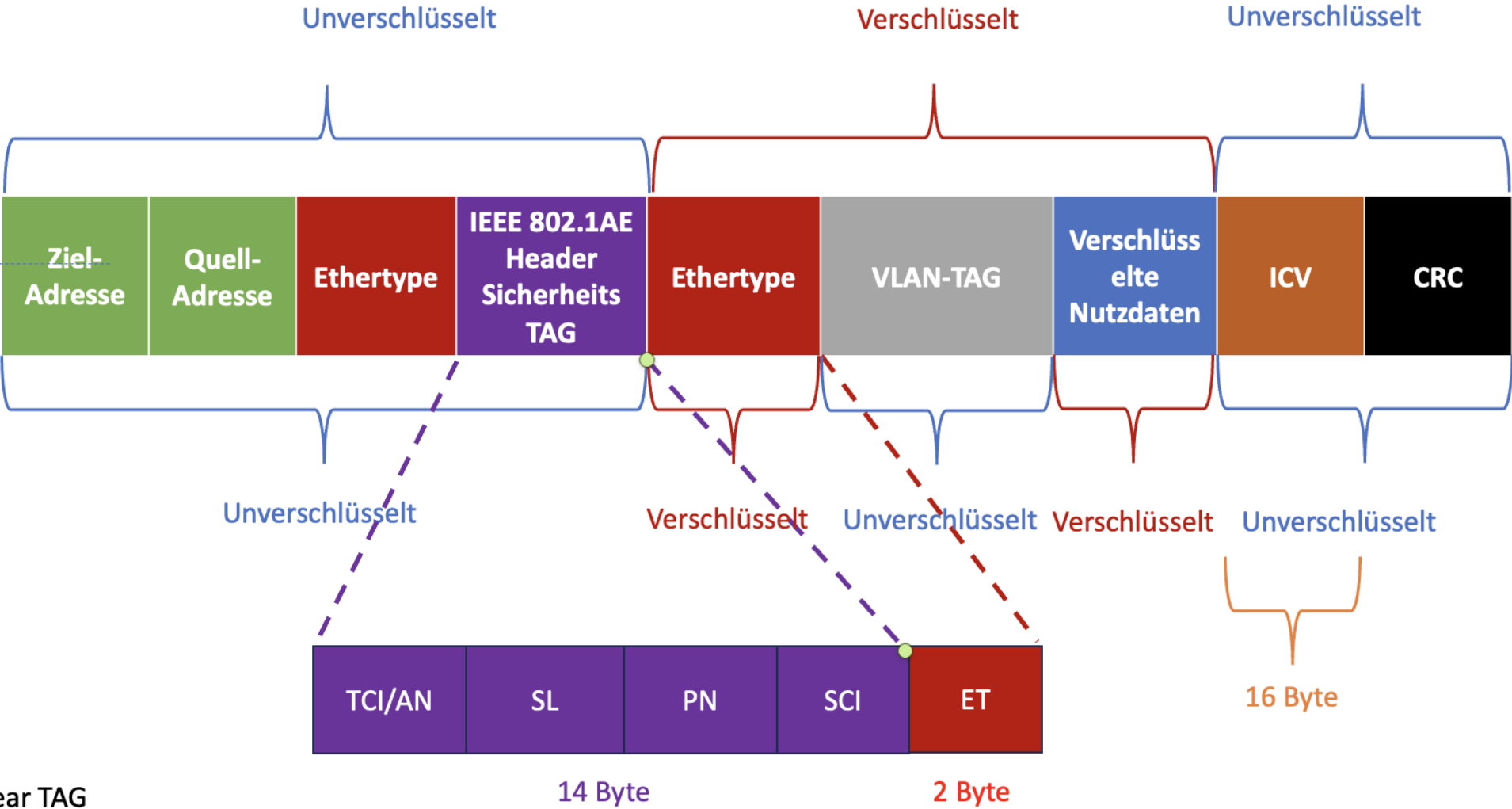
Frame-Aufbau



Frame-Aufbau

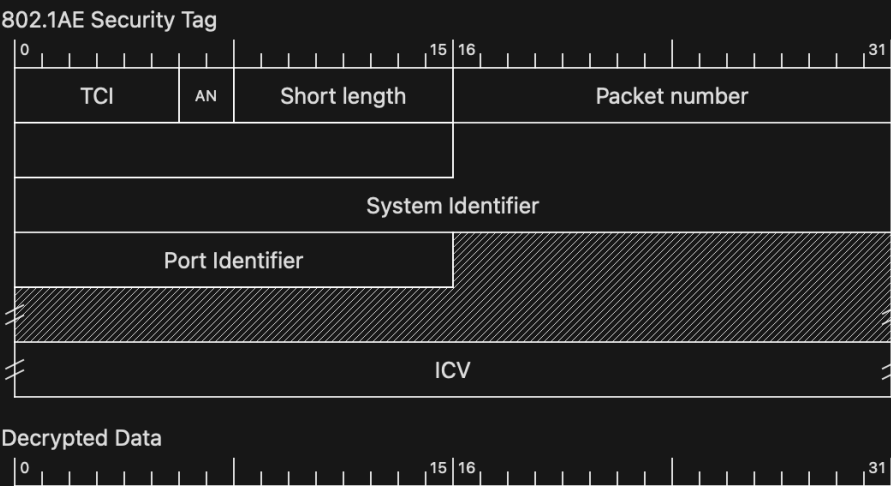


Default





```
> Frame 103: Packet, 134 bytes on wire (1072 bits), 134 bytes captured (1072 bits) on interface
> Ethernet II, Src: aa:c1:ab:31:74:d4 (aa:c1:ab:31:74:d4), Dst: aa:c1:ab:92:ca:4b (aa:c1:ab:92:
> 802.1Q Virtual LAN, PRI: 0, DEI: 0, ID: 28
< 802.1AE Security Tag
  > 0010 11.. = TCI: 0x0b, VER: 0x0, SC, E, C
    .... ..00 = AN: 0x0
    Short length: 0
    Packet number: 11
    System Identifier: aa:c1:ab:1d:d3:cc (aa:c1:ab:1d:d3:cc)
    Port Identifier: 1
    Ethertype: IPv4 (0x0800)
    ICV: 0e79bda1a54cb43961971292ac83ae16
  > [Verification Info]
  Decrypted Data: 0800450000548345000040019b3eac110202ac1102010000d898000b000755a8bd69000000005
> Internet Protocol Version 4, Src: 172.17.2.2, Dst: 172.17.2.1
> Internet Control Message Protocol
```



Wichtige Begrifflichkeiten



Begrifflichkeit	Beschreibung
MKA	MACsec Key Agreement: Schlüsseleinigungsprotokoll, um MACsec Peers aufzufinden, Schlüssel zu generieren, zu erneuern und auszutauschen.
CKN	Connectivity Association Key Name: Dient als Rahmen für den CAK. Die Peers übertragen diesen untereinander zur Validierung im Klartext.
CAK	Connectivity Association Key: Schlüssel der Control-Plane, von dem der Sessionschlüssel abgeleitet wird.
SAK	Security Association Key: Sessionschlüssel, der vom CAK abgeleitet wurde und zur Verschlüsselung zwischen zwei MACsec Peers Verwendung findet.
MSK	Master Session Key: Wird innerhalb EAP-Austausch generiert. Supplicant- und Authentifizierungsserver verwenden MSK, um CAK zu generieren.

Schlüsselverteilung & Analyse



- Was können wir allgemein analysieren?
 - Validieren ob verschlüsselt
 - Fehler im MKA
 - Fehler Übertragung EAPoL-Frames
 - Key Server-Auswahl
 - CAK-Namen
 - Confidentiality Offset
 - SAK-Verteilung
 - ICV-Fehler durch Manipulation oder Übertragungsfehler
 - Paketverlust anhand Paketnummer
 - Latenz mit Paketnummer





Schlüsselaustausch	Beschreibung	Szenario
Statischer SAK	Manuelle Konfiguration des symmetrischen Sitzungsschlüssels	Switch-zu-Switch Host-zu-Host
Statischer CAK	Manuelle Konfiguration des CAK und CKN und Nutzung MKA für Austausch SAK	Switch-zu-Switch
Dynamisch CAK MSK Verteilung via RADIUS und EAP-TLS	Nutzt dynamisches MKA und verteilt MSK im Rahmen von EAP-TLS um CAK zu ermitteln	Host-zu-Switch



■ Statisch SAK

- Statische Hinterlegung Schlüssel-ID und Schlüssel
- Beispiel Ubuntu mit iproute2

```
231 ip link set ens160 down
232 ip link add link ens160 macsec0 type macsec encrypt on
233 ip macsec add macsec0 tx sa 0 pn 1 on key AAAA 01234567012345670123456701234567
234 ip macsec add macsec0 rx address 00:0c:29:ef:7c:66 port 1
235 ip macsec add macsec0 rx address 00:0c:29:ef:7c:66 port 1 sa 0 pn 1 on key AAAA 01234567012345670123456701234567
236 ip addr add 192.168.203.2/24 dev macsec0
237 ip link set ens160 up
238 ip link set macsec0 up
```



MACsec_Linux_Static_SAK.pcapng — ceos1: eth1

macsec or eth.type == 0x88e5

No.

Absolute Time

Time

Delta

Source

Destination

Protocol

Length

Info

1	2026-01-20 23:20:31.756329	0.000000		VMware_55:9b:4b	IPv6mcast_02	MACSEC	102	MACsec frame [UNVERIFIED]
2	2026-01-20 23:20:42.900306	11.143977	11.1439...	VMware_ef:7c:66	IPv6mcast_02	MACSEC	102	MACsec frame [UNVERIFIED]
3	2026-01-20 23:21:06.930066	35.173737	24.0297...	VMware_55:9b:4b	VMware_ef:7c:66	MACSEC	130	MACsec frame [UNVERIFIED]
4	2026-01-20 23:21:06.930450	35.174121	0.000384	VMware_ef:7c:66	VMware_55:9b:4b	MACSEC	130	MACsec frame [UNVERIFIED]
5	2026-01-20 23:21:07.932194	36.175865	1.001744	VMware_55:9b:4b	VMware_ef:7c:66	MACSEC	130	MACsec frame [UNVERIFIED]
6	2026-01-20 23:21:07.932928	36.176599	0.000734	VMware_ef:7c:66	VMware_55:9b:4b	MACSEC	130	MACsec frame [UNVERIFIED]
7	2026-01-20 23:21:08.934904	37.178575	1.001976	VMware_55:9b:4b	VMware_ef:7c:66	MACSEC	130	MACsec frame [UNVERIFIED]
8	2026-01-20 23:21:08.935387	37.179058	0.000483	VMware_ef:7c:66	VMware_55:9b:4b	MACSEC	130	MACsec frame [UNVERIFIED]
9	2026-01-20 23:21:09.937111	38.180782	1.001724	VMware_55:9b:4b	VMware_ef:7c:66	MACSEC	130	MACsec frame [UNVERIFIED]
10	2026-01-20 23:21:09.937460	38.181131	0.000349	VMware_ef:7c:66	VMware_55:9b:4b	MACSEC	130	MACsec frame [UNVERIFIED]
11	2026-01-20 23:21:10.938940	39.182611	1.001480	VMware_55:9b:4b	VMware_ef:7c:66	MACSEC	130	MACsec frame [UNVERIFIED]
12	2026-01-20 23:21:10.939585	39.183256	0.000645	VMware_ef:7c:66	VMware_55:9b:4b	MACSEC	130	MACsec frame [UNVERIFIED]
13	2026-01-20 23:21:11.950767	40.194438	1.011182	VMware_55:9b:4b	VMware_ef:7c:66	MACSEC	74	MACsec frame [UNVERIFIED]
14	2026-01-20 23:21:11.951494	40.195165	0.000727	VMware_ef:7c:66	VMware_55:9b:4b	MACSEC	74	MACsec frame [UNVERIFIED]
15	2026-01-20 23:21:12.084563	40.328234	0.133069	VMware_ef:7c:66	VMware_55:9b:4b	MACSEC	74	MACsec frame [UNVERIFIED]
16	2026-01-20 23:21:12.084752	40.328423	0.000189	VMware_55:9b:4b	VMware_ef:7c:66	MACSEC	74	MACsec frame [UNVERIFIED]

> Frame 3: Packet, 130 bytes on wire (1040 bits), 130 bytes captured (1040 bits) on interface vmenet3, id 0

> Ethernet II, Src: VMware_55:9b:4b (00:0c:29:55:9b:4b), Dst: VMware_ef:7c:66 (00:0c:29:ef:7c:66)

> 802.1AE Security Tag

> 0010 11.. = TCI: 0x0b, VER: 0x0, SC, E, C

>00 = AN: 0x0

Short length: 0

Packet number: 17

System Identifier: VMware_55:9b:4b (00:0c:29:55:9b:4b)

Port Identifier: 1

ICV: 63595b682602b4e7f1f07d7494c8d649

> [Verification Info]

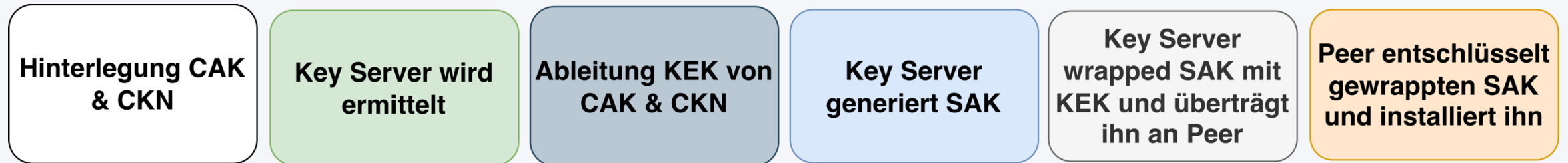
> Data (86 bytes)

Data: 32d5ca83290bbcb63be8ac621ac33bd9667ca8b2f7e0b19ca1ce3f6e8aacd93d0bddb512c622ef6c556fc362571eabe4c88840ab50c005333e1a787ff68d7c4a51e5982a3afd5e57e9a54f03d2d109cf4c3b4cc5234e

[Length: 86]



■ Statisch CAK





■ Statisch CAK

- Hinterlegung CKN und CAK
- Key-Server

```
ceos1#sh run | sec mac security
mac security
  profile mka
    cipher aes256-gcm
    key 0202020202020202020202020202020202020202020202020202020202020202 7 075F731C1C594B55454259
5C567A79747A6367724157445353060B0801045C534A460B0805030005065B0956550805544156560B59565D711E1E5B495
747405B5E
    mka key-server priority 15
    mka session rekey-period 600
    traffic unprotected drop
interface Ethernet1
  mac security profile mka
```



EAPoL MKA

No.	Time	Delta	Source	Destination	Protocol	Length	Info
8	9.686986667s		aa:c1:ab:ea:02:3d	Nearest-non-TPM...	EAPOL-MKA	94	Key Server, XPN
9	10.501125324s	0...	aa:c1:ab:03:d3:81	Nearest-non-TPM...	EAPOL-MKA	114	Key Server, Potential Peer List, XPN
10	11.793064591s	1...	aa:c1:ab:ea:02:3d	Nearest-non-TPM...	EAPOL-MKA	114	Key Server, Live Peer List, XPN
11	12.599381955s	0...	aa:c1:ab:03:d3:81	Nearest-non-TPM...	EAPOL-MKA	114	Live Peer List, XPN
15	16.502724384s	3...	aa:c1:ab:ea:02:3d	Nearest-non-TPM...	EAPOL-MKA	170	Key Server, Live Peer List, Distributed SAK, XPN
16	16.504829843s	0...	aa:c1:ab:ea:02:3d	Nearest-non-TPM...	EAPOL-MKA	214	Key Server, Live Peer List, MACsec SAK Use, Distributed SAK, XPN

Key Server Aushandlung & Peer Discovery

Aushandlung Verschlüsselungsparameter und Verteilung Session Key



EAPoL MKA

MACsec_Arista_Static_CAK_Encrypted.pcapng — ceos1: eth1

eth.type == 0x888e and mka.param_set_type == 4

No.	Absolute Time	Time	Delta	Source	Destination	Protocol	Length	Info
15	2026-03-12 01:20:39.337204617	16.502724384		aa:c1:ab:ea:02:3d	Nearest-non-TPMR-Bridge	EAPoL-MKA	170	Key Server, Live Peer List, Distributed SAK, XPN
16	2026-03-12 01:20:39.339310076	16.504829843	0.00210...	aa:c1:ab:ea:02:3d	Nearest-non-TPMR-Bridge	EAPoL-MKA	214	Key Server, Live Peer List, MACsec SAK Use, Distributed SAK...

> Frame 15: Packet, 170 bytes on wire (1360 bits), 170 bytes captured (1360 bits) on interface eth1, id 0

> Ethernet II, Src: aa:c1:ab:ea:02:3d (aa:c1:ab:ea:02:3d), Dst: Nearest-non-TPMR-Bridge (01:80:c2:00:00:03)

> 802.1X Authentication

▼ MACsec Key Agreement

- ▼ Basic Parameter set
 - MKA Version Identifier: 2
 - Key Server Priority: 10
 - 1... = Key Server: True
 - .1.. = MACsec Desired: True
 - ..10 = MACsec Capability: MACsec Integrity with/without confidentiality, no confidentiality offset (2)
 - 0000 0010 1100 = Parameter set body length: 44
 - SCI: aac1abea023d0001
 - Actor Member Identifier: 192b390775f4dd5dae367e46
 - Actor Message Number: 00000006
 - Algorithm Agility: IEEE Std 802.1X-2010 (0x0080c201)
 - CAK Name: 01234567890123456789012345678912
 - [CAK Name Info: 0001]
- > Live Peer List Parameter set
- ▼ Distributed SAK parameter set
 - Parameter set type: Distributed SAK (4)
 - 00.. = Distributed AN: 0
 - ..01 = Confidentiality Offset: No confidentiality offset (1)
 - 0000 0011 0100 = Parameter set body length: 52
 - Key Number: 00000001
 - MACsec Cipher Suite: GCM-AES-256 (0x0080c20001000002)
 - AES Key Wrap of SAK: b711957f12c3ac757dd4ea3fbd2c91a943110a59d6f383cfc47d743ab70cb5c1782b25480630c110
 - Unwrapped SAK: 565f261e492fb86709fed2a1b615f4cd7b2a55bad8342f019f6ee53881acab87
- > Extended Packet Numbering set
 - Integrity Check Value: 71d4fab3b0a568e2518ef5e791bdeeb9



Dynamic CAK



Schlüsselverteilung



Dynamic CAK

MACsec_Dynamic_CAK.pcapng

Apply a display filter ... <=>

No.	Time	Delta	Source	Destination	Protocol	Length	Packet number	Info
5	9.700126	0.299905	AlcatelLucen_6b:34:65	RaspberryPi_b4:41:49	EAP	60		Request, Protected EAP (EAP-PEAP)
6	9.700143	0.000017	RaspberryPi_b4:41:49	Nearest-non-TPMR-Bridge	EAP	60		Response, Legacy Nak (Response Only)
7	9.800065	0.099922	AlcatelLucen_6b:34:65	RaspberryPi_b4:41:49	EAP	60		Request, TLS EAP (EAP-TLS)
8	9.800087	0.000022	RaspberryPi_b4:41:49	Nearest-non-TPMR-Bridge	TLSv1.2	223		Client Hello
9	10.000075	0.199988	AlcatelLucen_6b:34:65	RaspberryPi_b4:41:49	EAP	1042		Request, TLS EAP (EAP-TLS)
10	10.000099	0.000024	RaspberryPi_b4:41:49	Nearest-non-TPMR-Bridge	EAP	60		Response, TLS EAP (EAP-TLS)
11	10.100140	0.100041	AlcatelLucen_6b:34:65	RaspberryPi_b4:41:49	EAP	1042		Request, TLS EAP (EAP-TLS)
12	10.100143	0.000003	RaspberryPi_b4:41:49	Nearest-non-TPMR-Bridge	EAP	60		Response, TLS EAP (EAP-TLS)
13	10.300135	0.199992	AlcatelLucen_6b:34:65	RaspberryPi_b4:41:49	EAP	1042		Request, TLS EAP (EAP-TLS)
14	10.300156	0.000021	RaspberryPi_b4:41:49	Nearest-non-TPMR-Bridge	EAP	60		Response, TLS EAP (EAP-TLS)
15	10.400141	0.099985	AlcatelLucen_6b:34:65	RaspberryPi_b4:41:49	TLSv1.2	361		Server Hello, Certificate, Server Key Exchange, Certificate Request, Server Hello Do
16	10.500129	0.099988	RaspberryPi_b4:41:49	Nearest-non-TPMR-Bridge	EAP	1426		Response, TLS EAP (EAP-TLS)
17	10.599899	0.099770	AlcatelLucen_6b:34:65	RaspberryPi_b4:41:49	EAP	60		Request, TLS EAP (EAP-TLS)
18	10.599901	0.000002	RaspberryPi_b4:41:49	Nearest-non-TPMR-Bridge	EAP	1422		Response, TLS EAP (EAP-TLS)
19	10.800067	0.200166	AlcatelLucen_6b:34:65	RaspberryPi_b4:41:49	EAP	60		Request, TLS EAP (EAP-TLS)
20	10.800070	0.000003	RaspberryPi_b4:41:49	Nearest-non-TPMR-Bridge	TLSv1.2	464		Certificate, Client Key Exchange, Certificate Verify, Change Cipher Spec, Encrypted
21	10.900131	0.100061	AlcatelLucen_6b:34:65	RaspberryPi_b4:41:49	TLSv1.2	79		Change Cipher Spec, Encrypted Handshake Message
22	10.900152	0.000021	RaspberryPi_b4:41:49	Nearest-non-TPMR-Bridge	EAP	60		Response, TLS EAP (EAP-TLS)
23	11.099968	0.199816	AlcatelLucen_6b:34:65	RaspberryPi_b4:41:49	EAP	60		Success
24	11.200147	0.100179	RaspberryPi_b4:41:49	Nearest-non-TPMR-Bridge	EAPOL-M...	82		
25	12.000127	0.799980	AlcatelLucen_6b:34:65	Nearest-non-TPMR-Bridge	EAPOL-M...	102		Key Server, Potential Peer List
26	12.700161	0.700034	fe80::2cfc:67ff:feb4:4149	ff02::2	ICMPv6	70		Router Solicitation from 2c:cf:67:b4:41:49
27	13.200053	0.499892	RaspberryPi_b4:41:49	Nearest-non-TPMR-Bridge	EAPOL-M...	102		Live Peer List
28	14.000192	0.800139	AlcatelLucen_6b:34:65	Nearest-non-TPMR-Bridge	EAPOL-M...	134		Key Server, Live Peer List, Distributed SAK
29	14.000218	0.000026	RaspberryPi_b4:41:49	Nearest-non-TPMR-Bridge	EAPOL-M...	146		Live Peer List, MACsec SAK Use

> Frame 32: Packet, 122 bytes on wire (976 bits), 122 bytes captured (976 bits) on interface en15, id 0
> Ethernet II, Src: RaspberryPi_b4:41:49 (2c:cf:67:b4:41:49), Dst: IPv6mcast_16 (33:33:00:00:00:16)
> 802.1AE Security Tag
> Data (78 bytes)

Ethernet
0 15 16 31
Destination

Bildquellen



■ Pexels <https://www.pexels.com/de-de/>

■ Unsplash <https://unsplash.com/de>

Vielen Dank!

WIRESHARK

Benjamin Pfister

[linkedin.com/in/benjamin-pfister-90136b298](https://www.linkedin.com/in/benjamin-pfister-90136b298)

