SVA Academy

SVA

24.09.2026

Johannes Weber

Post-Quantum Cryptography PQC

Über mich

Johannes Weber

- Master IT-Security
- Network-Security Consultant
  - Firewalls
  - Wireshark
- IPv6 & Security
- DNS & Security

LinkedIn: https://www.linkedin.com/in/johannes-webernetz/

Blog: https://weberblog.net/

Security-as-a-Podcast https://securityasapodcast.de/

Agenda

01 Motivation

02 Bedrohung Quantencomputer

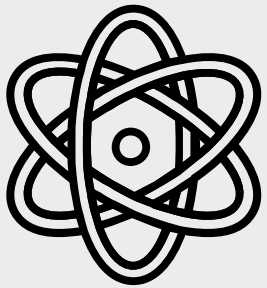
03 Lösungsansätze: QKD & PQC

04 Migrationsstrategien

05 Konkrete Beispiele

TL;DR

- Wenn es Quantencomputer gibt fällt die asymmetrische Kryptografie!
- #TLS #VPN #PKI
- PQC: neue Algorithmen retten!



Bedrohung Quantencomputer

Klassische Welt: Bits

- **Zwei Zustände:**
  Strom aus (0) oder Strom an (1)

- **Rechnen mit Bits: Boolesche Algebra**
  - AND/OR/NOT
  - XOR/NAND/NOR

Quantenwelt: Qubits

- **Überlagerung** von zwei Zuständen

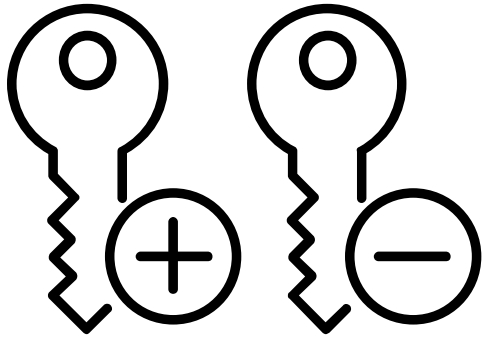
- Vergleich: Münze

Wie funktioniert asymmetrische Kryptographie?

- Grundlage sind mathematische Probleme

- **Eigenschaft:**
  - Eine Lösung ist einfach zu verifizieren
  - Finden einer Lösung ist wiederum schwer

- **Beispiele:**
  - **Primfaktorzerlegung** (RSA)
    - $221 = 13 * 17$
    - $840 = ?$
  - **Diskreter Logarithmus** (ECC, DH, DSA)



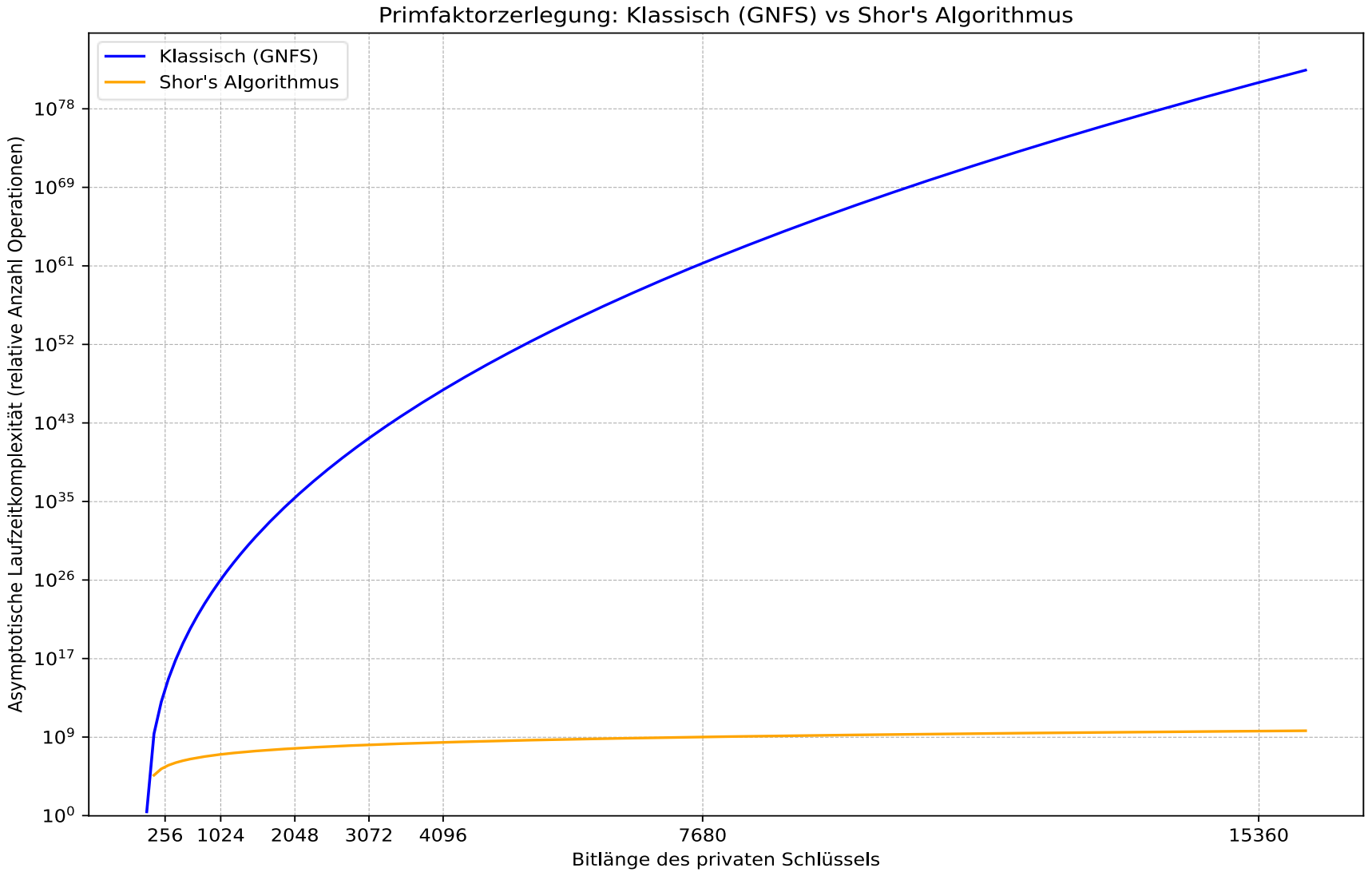
Angriff auf asymmetrische Verfahren: Shor‘s Algorithmus

- 1994 von Peter Shor veröffentlicht
- Benötigt einen Quantencomputer (Quantenalgorithmus)

- **Löst folgende Probleme effizient:**
  - ⇢ Primfaktorzerlegung
  - ⇢ Diskreter Logarithmus

- **Auswirkung (RSA, DSA, DH, ECC):**
  - ⇢ Sind unabhängig von der Schlüsselgröße unsicher

- **Und mit klassischen Computern?**
  - ⇢ RSA-2048: ~300 Billionen Jahre


Primfaktorzerlegung: Klassisch (GNFS) vs Shor's Algorithmus
Klassisch (GNFS)
Shor's Algorithmus
Asymptotische Laufzeitkomplexität (relative Anzahl Operationen)
10^{78}
10^{69}
10^{61}
10^{52}
10^{43}
10^{35}
10^{26}
10^{17}
10^{9}
10^{0}
256
1024
2048
3072
4096
7680
15360
Bitlänge des privaten Schlüssels

Fazit

Kryptographischer Algorithmus	Typ	Einsatzzweck	Einfluss von leistungsfähigen QCs
AES	Symmetrisch	Verschlüsselung	Größere Schlüssel benötigt
SHA-2, SHA-3	Hashfunktion	Prüfsummen	Größere Ausgabe benötigt
RSA	Asymmetrisch (Public Key)	Signaturen, Schlüsselaustausch	**Nicht mehr sicher**
DSA, DH (finite field cryptography)	Asymmetrisch (Public Key)	Signaturen, Schlüsselaustausch	**Nicht mehr sicher**
ECDSA, ECDH (eliptic curve cryptography)	Asymmetrisch (Public Key)	Signaturen, Schlüsselaustausch	**Nicht mehr sicher**

⇢ Alternative für RSA & Co: **PQC und QKD**

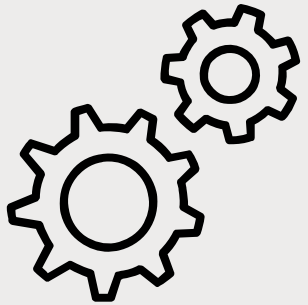
Das Kernproblem

- **Harvest now – decrypt later:** Daten, die heute abgefangen und gespeichert werden, können in der Zukunft entschlüsselt werden (z.B. VPN)

- **Langfristige Systeme:** Systeme mit langen Lebenszyklen müssen bereits jetzt auf die Migration vorbereitet werden (z.B. PKI)

Die Fortschritte in den Jahren 2024–2025 […] deuten aber auf einen kürzeren Zeitraum bis zur Entwicklung eines kryptanalytisch relevanten Quantencomputers hin.
Die kontinuierlichen Verbesserungen der Technik […] lassen das Erreichen des Ziels in **etwa 15 Jahren** realistisch erscheinen.
Neue Entwicklungen […] könnten den Zeitraum sogar noch weiter – **auf ungefähr 10 Jahre** – verkürzen.

Bundesamt für Sicherheit in der Informationstechnik (BSI).
Entwicklungsstand Quantencomputer. Version 2.2, 2025



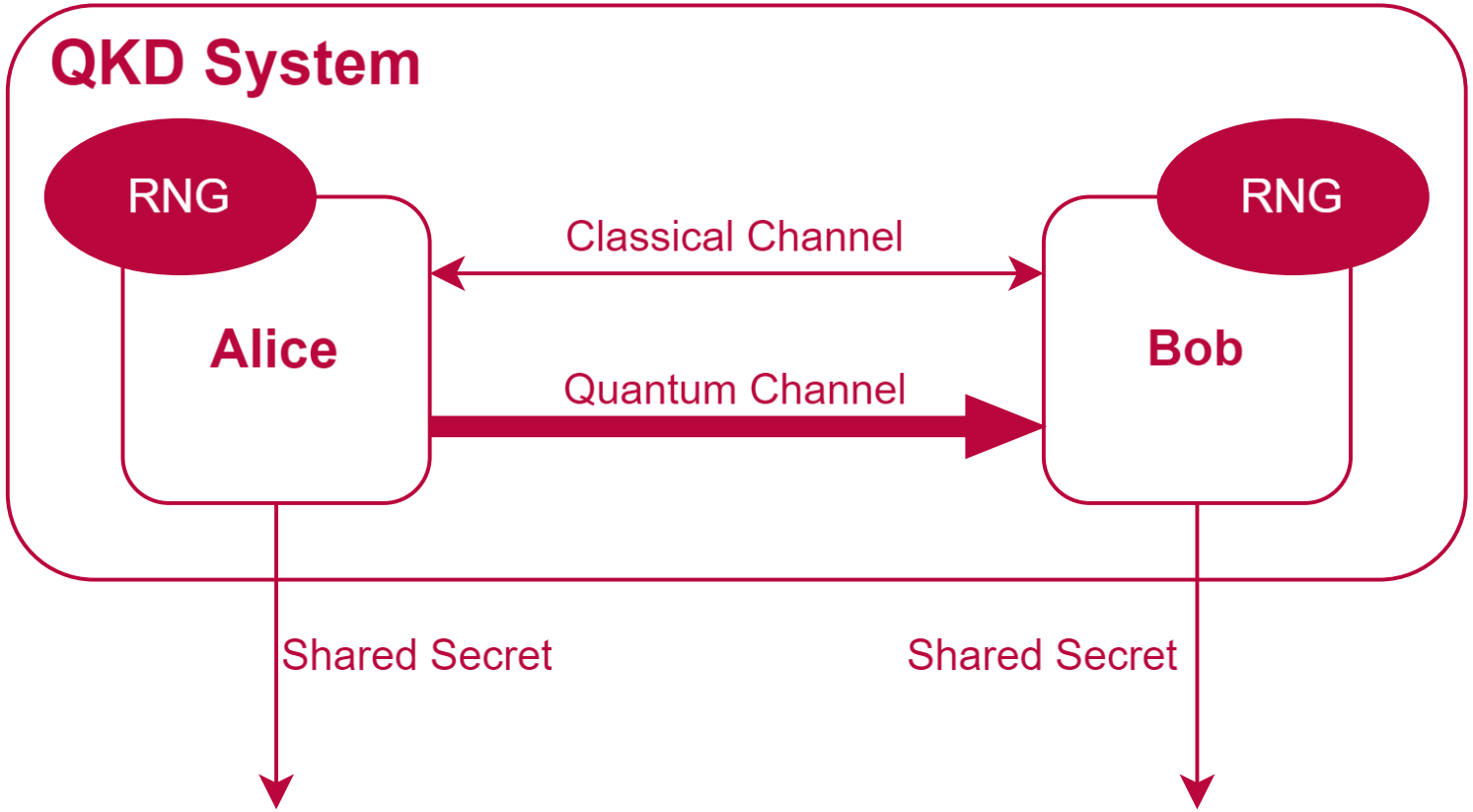
Lösungsansätze

Quantum Key Distribution (QKD)

Schlüsselaustausch durch Quantenphysik

Funktionsweise

- Schlüsselaustausch mithilfe von **Quantenmechanik**
- Austausch und Messung von **Quantenzuständen**
- **Zwei Kommunikationskanäle** werden benötigt



Post Quantum Cryptography (PQC)

Quantensichere asymmetrische Kryptographie

Funktionsweise

- Asymmetrische Kryptosysteme
- Im Gegensatz zu RSA/ECC:
  - **Quantensicher**

Vor- und Nachteile

Vorteile

- Klassische Infrastruktur benutzbar
- Breite Anwendbarkeit
- Bereits erste FIPS/RFC Standards

Nachteile

- (Teilweise) erhöhte Rechenleistung
- Größere Schlüssel/Signaturen
- Admins müssen umstellen!

Empfehlungen und Vorgaben

Die ersten PQC-Standards: NIST FIPS 203, 204 und 205

FIPS 203: ML-KEM

Module-Lattice-Based Key-Encapsulation Mechanism

- Schlüsselaustauschverfahren
- Basiert auf strukturierten Gittern
- Bekannt als „CRYSTALS-KYBER“

FIPS 204: ML-DSA

Module-Lattice-Based Digital Signature Algorithm

- Signaturverfahren
- Basiert auf strukturierten Gittern
- Bekannt als „CRYSTALS-DILITHIUM“

FIPS 205: SLH-DSA

Stateless Hash-Based Digital Signature Algorithm

- Signaturverfahren
- Basiert auf Hash-Funktionen
- Bekannt als „SPHINCS+“

Ausstehende Standards des NIST

FIPS 206: FN-DSA

FFT (fast-Fourier transform) over NTRU-Lattice-Based Digital Signature Algorithm

- Signaturverfahren
- Basiert auf strukturierten Gittern
- Bekannt als „FALCON“
- Standardisierung bis „Ende 2024“

HQC

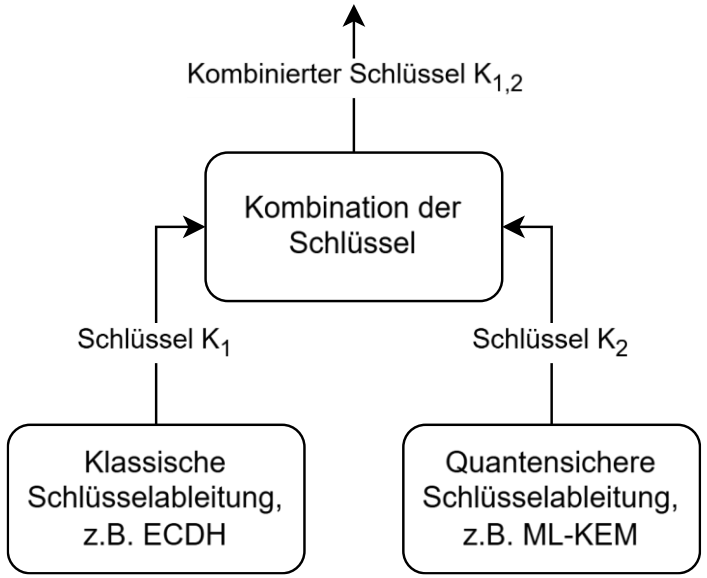
Hamming-Quasi-Cyclic

- Schlüsselaustauschverfahren
- Basiert auf quasi-zyklische Codes
- Auswahl in 03/2025, Standardisierung bis 2027

Kombination der klassischen- und Quantensicherheit

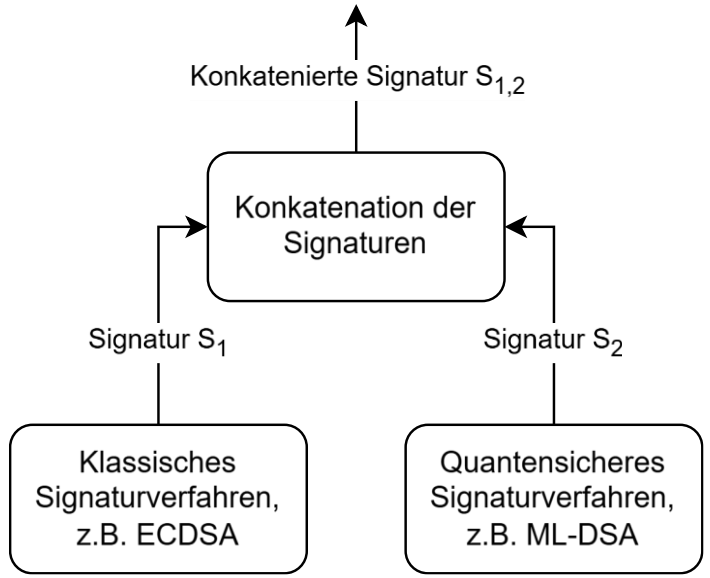
Hybride Schlüsselableitung

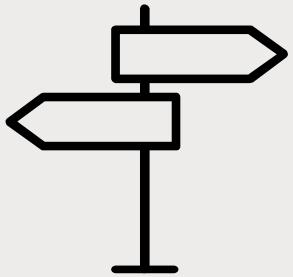
- Kombination eines quantensicheren Verfahrens mit einem klassischen Verfahren.



Hybride Signatur

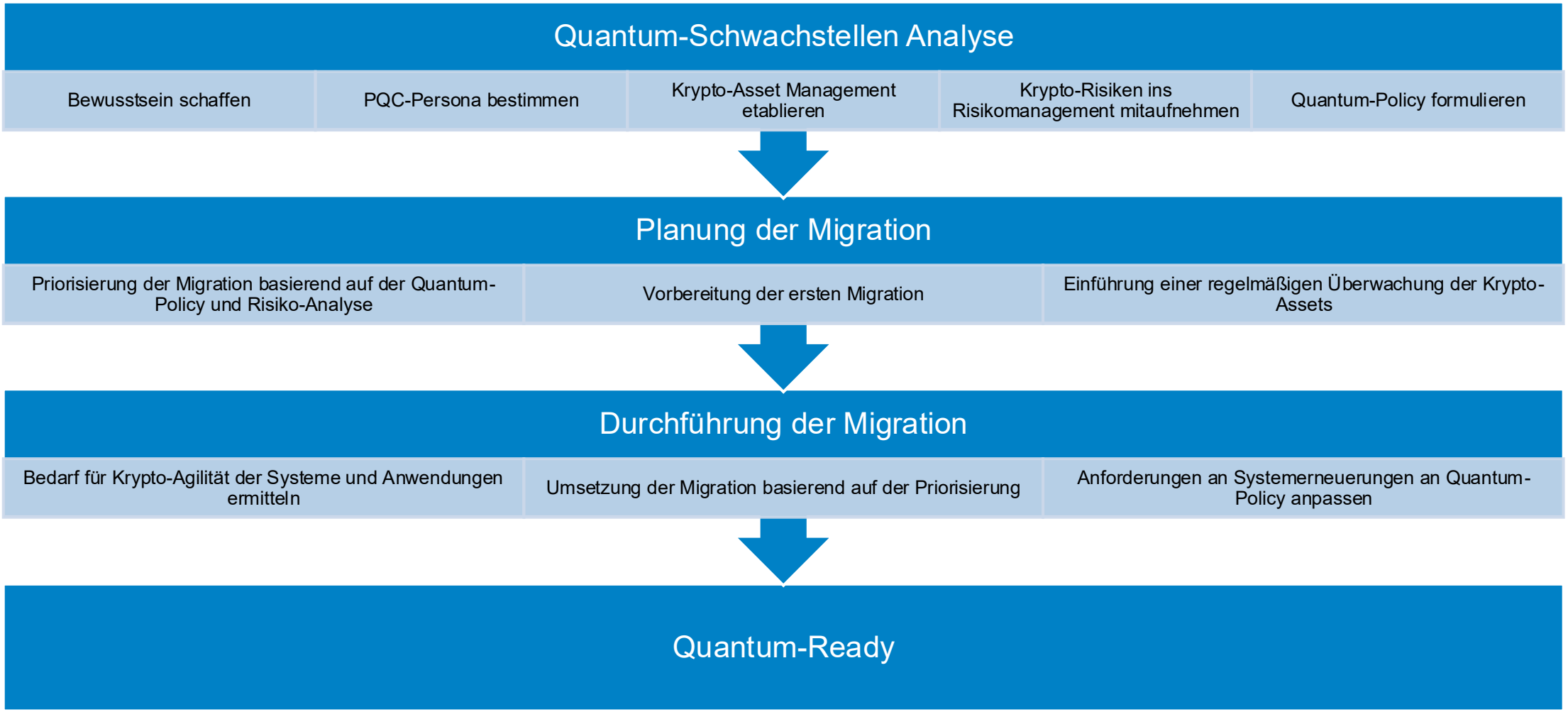
- Konkatenation klassischer und quantensicherer Signatur





Migrationsstrategie

High-Level Roadmap



Krypto-Asset Management – Wo nutze ich Kryptographie?

Netzwerk-Verkehr

- SSH
- X.509
- TLS (HTTPS)
- PGP, S/MIME
- IPsec
- Wireguard
- S/MIME, OpenPGP
- Messenger
- RPKI / BGPsec
- NTS (NTP)

Systeme und Anwendungen

- VPNs
- MFA
- Zertifikate
- Login mit Benutzername/Passwort
- Ver- und Entschlüsselung
- Secure Boot
- Signaturen von Updates

Softwareentwicklung

- Abhängigkeiten von
  - OpenSSL
  - BouncyCastle
  - Libsodium
  - Crypto++
  - wolfCrypt

DNSSEC

- IANA-Algorithmus-Nr. 18: `ML-DSA-44`
- Cloudflares 2606:4700:4700::1111 (1.1.1.1) validiert seit 10.09.2026 ;)
- https://blog.cloudflare.com/post-quantum-dnssec-1111/

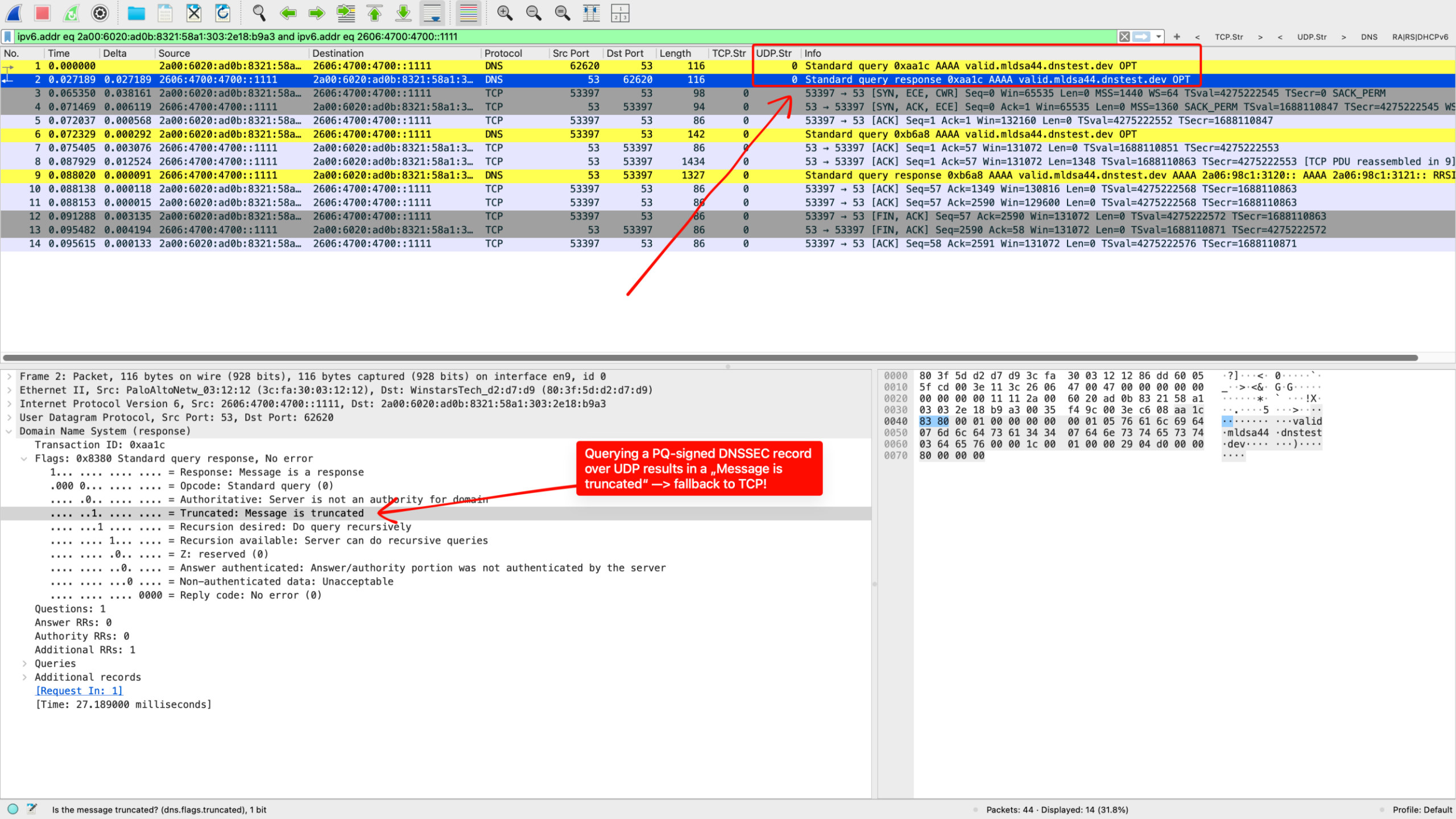
Algorithm	Number	Public key size	Signature size
RSA-2048/SHA-256	8	260 bytes	256 bytes
ECDSA P-256	13	64 bytes	64 bytes
ML-DSA-44	18	1,312 bytes	2,420 bytes

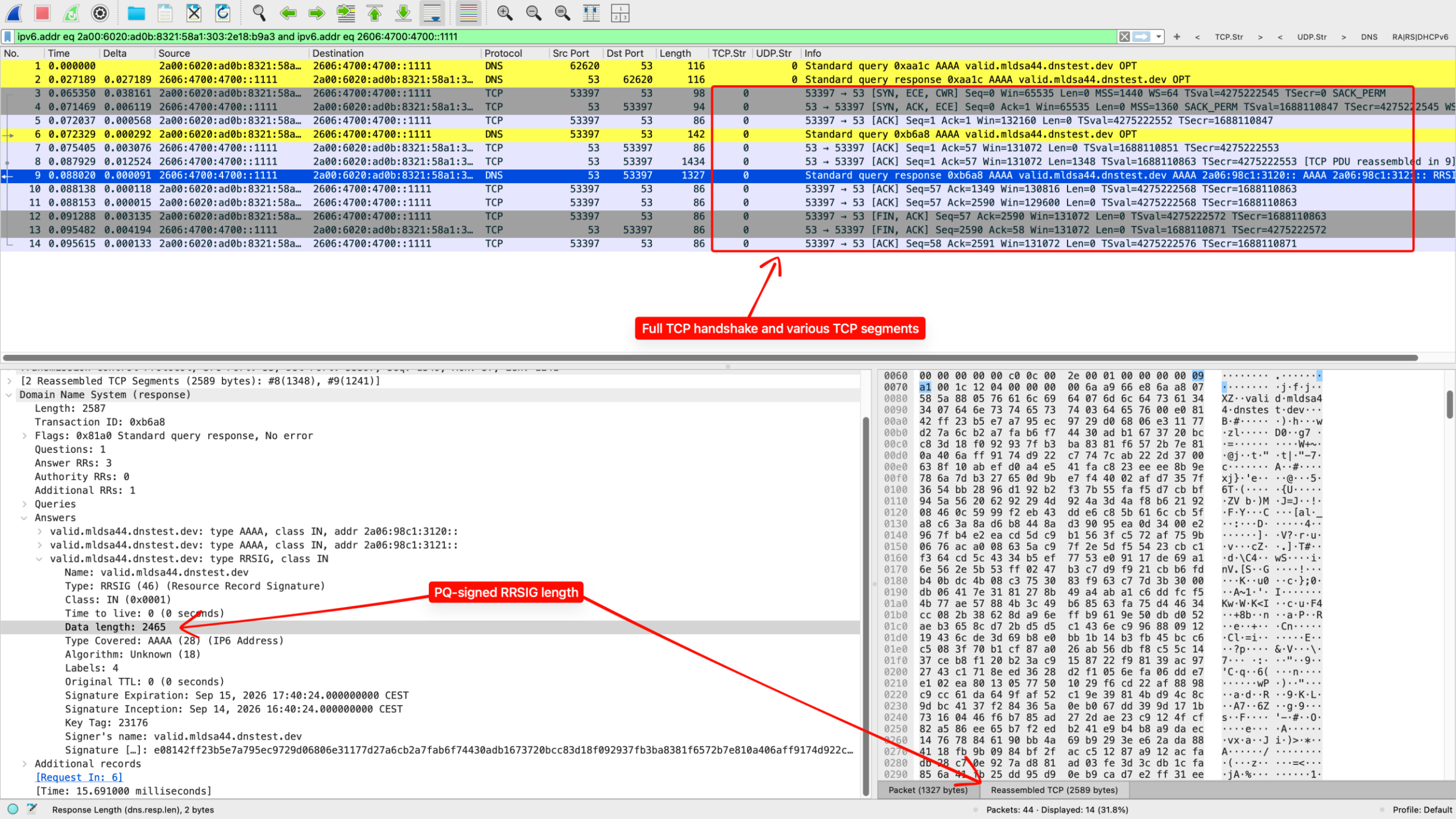
- `dig valid.mldsa44.dnstest.dev rrsig`
- `dig valid.mldsa44.dnstest.dev rrsig @1.1.1.1`

- https://dnstest.dev/

DNSSEC (Wireshark PCAP)

- `dig valid.mldsa44.dnstest.dev @2606:4700:4700::1111 +dnssec`
- `dig valid.mldsa44.dnstest.dev rrsig`


ipv6.addr eq 2a00:6020:ad0b:8321:58a1:303:2e18:b9a3 and ipv6.addr eq 2606:4700:4700::1111
No. Time Delta Source Destination Protocol Src Port Dst Port Length TCP.Str UDP.Str Info
1 0.000000 2a00:6020:ad0b:8321:58a… 2606:4700:4700::1111 DNS 62620 53 116 0 Standard query 0xaa1c AAAA valid.mldsa44.dnstest.dev OPT
2 0.027189 0.027189 2606:4700:4700::1111 2a00:6020:ad0b:8321:58a1:3… DNS 53 62620 116 0 Standard query response 0xaa1c AAAA valid.mldsa44.dnstest.dev OPT
3 0.065350 0.038161 2a00:6020:ad0b:8321:58a… 2606:4700:4700::1111 TCP 53397 53 98 0 53397 → 53 [SYN, ECE, CWR] Seq=0 Win=65535 Len=0 MSS=1440 WS=64 TSval=4275222545 TSecr=0 SACK_PERM
4 0.071469 0.006119 2606:4700:4700::1111 2a00:6020:ad0b:8321:58a1:3… TCP 53 53397 94 0 53 → 53397 [SYN, ACK, ECE] Seq=0 Ack=1 Win=65535 Len=0 MSS=1360 SACK_PERM TSval=1688110847 TSecr=4275222545 WS
5 0.072037 0.000568 2a00:6020:ad0b:8321:58a… 2606:4700:4700::1111 TCP 53397 53 86 0 53397 → 53 [ACK] Seq=1 Ack=1 Win=132160 Len=0 TSval=4275222552 TSecr=1688110847
6 0.072329 0.000292 2a00:6020:ad0b:8321:58a… 2606:4700:4700::1111 DNS 53397 53 142 0 Standard query 0xb6a8 AAAA valid.mldsa44.dnstest.dev OPT
7 0.075405 0.003076 2606:4700:4700::1111 2a00:6020:ad0b:8321:58a1:3… TCP 53 53397 86 0 53 → 53397 [ACK] Seq=1 Ack=57 Win=131072 Len=0 TSval=1688110851 TSecr=4275222553
8 0.087929 0.012524 2606:4700:4700::1111 2a00:6020:ad0b:8321:58a1:3… TCP 53 53397 1434 0 53 → 53397 [ACK] Seq=1 Ack=57 Win=131072 Len=1348 TSval=1688110863 TSecr=4275222553 [TCP PDU reassembled in 9]
9 0.088020 0.000091 2606:4700:4700::1111 2a00:6020:ad0b:8321:58a1:3… DNS 53 53397 1327 0 Standard query response 0xb6a8 AAAA valid.mldsa44.dnstest.dev AAAA 2a06:98c1:3120:: AAAA 2a06:98c1:3121:: RRSI
10 0.088138 0.000118 2a00:6020:ad0b:8321:58a… 2606:4700:4700::1111 TCP 53397 53 86 0 53397 → 53 [ACK] Seq=57 Ack=1349 Win=130816 Len=0 TSval=4275222568 TSecr=1688110863
11 0.088153 0.000015 2a00:6020:ad0b:8321:58a… 2606:4700:4700::1111 TCP 53397 53 86 0 53397 → 53 [ACK] Seq=57 Ack=2590 Win=129600 Len=0 TSval=4275222568 TSecr=1688110863
12 0.091288 0.003135 2a00:6020:ad0b:8321:58a… 2606:4700:4700::1111 TCP 53397 53 86 0 53397 → 53 [FIN, ACK] Seq=57 Ack=2590 Win=131072 Len=0 TSval=4275222572 TSecr=1688110863
13 0.095482 0.004194 2606:4700:4700::1111 2a00:6020:ad0b:8321:58a1:3… TCP 53 53397 86 0 53 → 53397 [FIN, ACK] Seq=2590 Ack=58 Win=131072 Len=0 TSval=1688110871 TSecr=4275222572
14 0.095615 0.000133 2a00:6020:ad0b:8321:58a… 2606:4700:4700::1111 TCP 53397 53 86 0 53397 → 53 [ACK] Seq=58 Ack=2591 Win=131072 Len=0 TSval=4275222576 TSecr=1688110871
Frame 2: Packet, 116 bytes on wire (928 bits), 116 bytes captured (928 bits) on interface en9, id 0
Ethernet II, Src: PaloAltoNetw_03:12:12 (3c:fa:30:03:12:12), Dst: WinstarsTech_d2:d7:d9 (80:3f:5d:d2:d7:d9)
Internet Protocol Version 6, Src: 2606:4700:4700::1111, Dst: 2a00:6020:ad0b:8321:58a1:303:2e18:b9a3
User Datagram Protocol, Src Port: 53, Dst Port: 62620
Domain Name System (response)
Transaction ID: 0xaa1c
Flags: 0x8380 Standard query response, No error
1... .... = Response: Message is a response
.000 0... .... = Opcode: Standard query (0)
.... .0.. .... = Authoritative: Server is not an authority for domain
.... ..1. .... = Truncated: Message is truncated
....1 .... = Recursion desired: Do query recursively
.... 1... .... = Recursion available: Server can do recursive queries
.... .0.. .... = Z: reserved (0)
....0. .... = Answer authenticated: Answer/authority portion was not authenticated by the server
....0 .... = Non-authenticated data: Unacceptable
.... 0000 = Reply code: No error (0)
Questions: 1
Answer RRs: 0
Authority RRs: 0
Additional RRs: 1
Queries
Additional records
[Request In: 1]
[Time: 27.189000 milliseconds]
Querying a PQ-signed DNSSEC record over UDP results in a „Message is truncated“ —> fallback to TCP!
0000 80 3f 5d d2 d7 d9 3c fa 30 03 12 12 86 dd 60 05
0010 5f cd 00 3e 11 3c 26 06 47 00 47 00 00 00 00 00
0020 00 00 00 00 11 11 2a 00 60 20 ad 0b 83 21 58 a1
0030 03 03 2e 18 b9 a3 00 35 f4 9c 00 3e c6 08 aa 1c
0040 83 80 00 01 00 00 00 00 00 01 05 76 61 6c 69 64
0050 07 6d 6c 64 73 61 34 34 07 64 6e 73 74 65 73 74
0060 03 64 65 76 00 00 1c 00 01 00 00 29 04 d0 00 00
0070 80 00 00 00
Is the message truncated? (dns.flags.truncated), 1 bit
Packets: 44 · Displayed: 14 (31.8%)
Profile: Default

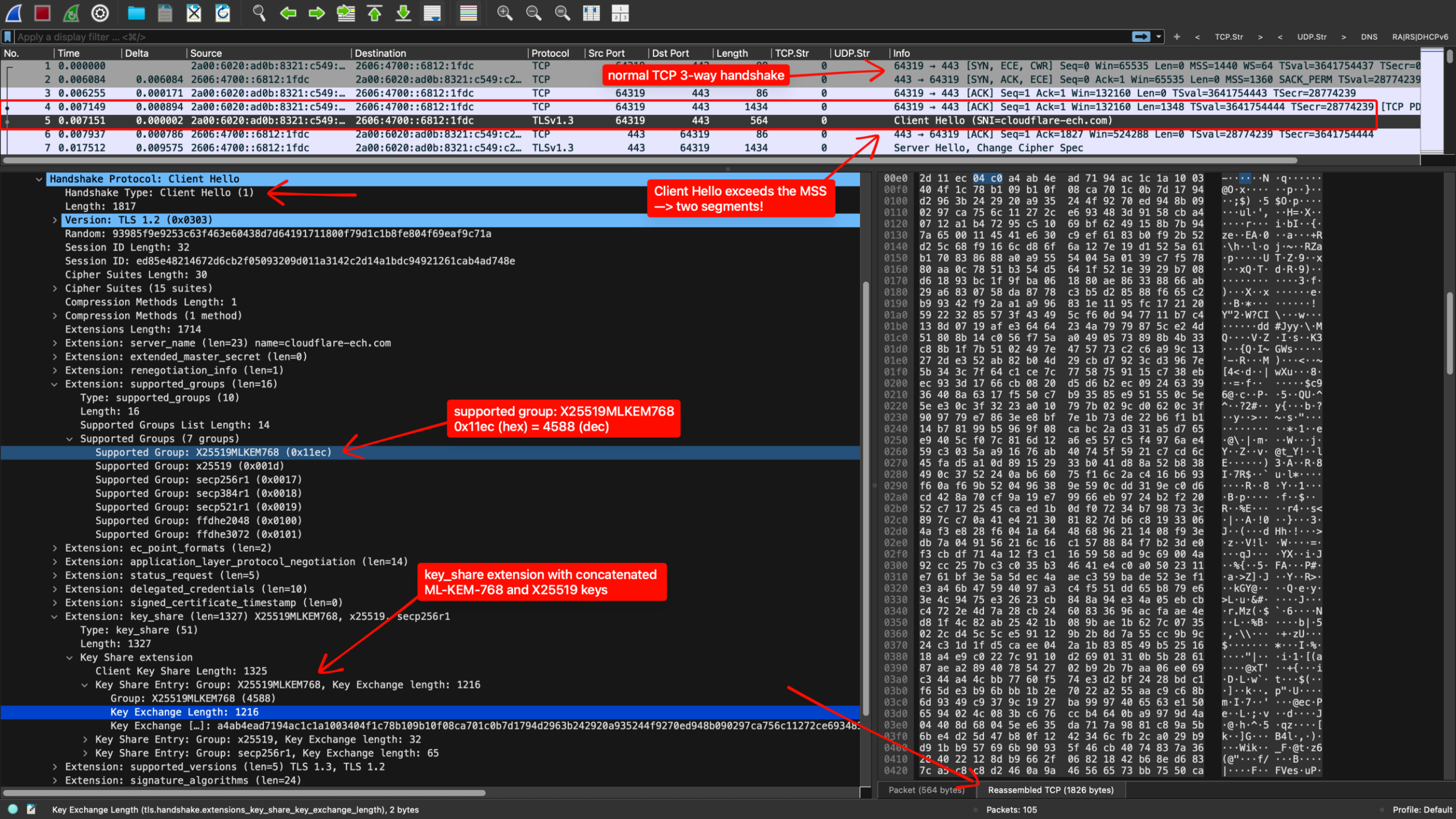

ipv6.addr eq 2a00:6020:ad0b:8321:58a1:303:2e18:b9a3 and ipv6.addr eq 2606:4700:4700::1111
TCP.Str
UDP.Str
DNS
RA|RS|DHCPv6
No. Time Delta Source Destination Protocol Src Port Dst Port Length TCP.Str UDP.Str Info
1 0.000000 2a00:6020:ad0b:8321:58a… 2606:4700:4700::1111 DNS 62620 53 116 0 Standard query 0xaa1c AAAA valid.mldsa44.dnstest.dev OPT
2 0.027189 0.027189 2606:4700:4700::1111 2a00:6020:ad0b:8321:58a1:3… DNS 53 62620 116 0 Standard query response 0xaa1c AAAA valid.mldsa44.dnstest.dev OPT
3 0.065350 0.038161 2a00:6020:ad0b:8321:58a… 2606:4700:4700::1111 TCP 53397 53 98 0 53397 → 53 [SYN, ECE, CWR] Seq=0 Win=65535 Len=0 MSS=1440 WS=64 TSval=4275222545 TSecr=0 SACK_PERM
4 0.071469 0.006119 2606:4700:4700::1111 2a00:6020:ad0b:8321:58a1:3… TCP 53 53397 94 0 53 → 53397 [SYN, ACK, ECE] Seq=0 Ack=1 Win=65535 Len=0 MSS=1360 SACK_PERM TSval=1688110847 TSecr=4275222545 WS
5 0.072037 0.000568 2a00:6020:ad0b:8321:58a… 2606:4700:4700::1111 TCP 53397 53 86 0 53397 → 53 [ACK] Seq=1 Ack=1 Win=132160 Len=0 TSval=4275222552 TSecr=1688110847
6 0.072329 0.000292 2a00:6020:ad0b:8321:58a… 2606:4700:4700::1111 DNS 53397 53 142 0 Standard query 0xb6a8 AAAA valid.mldsa44.dnstest.dev OPT
7 0.075405 0.003076 2606:4700:4700::1111 2a00:6020:ad0b:8321:58a1:3… TCP 53 53397 86 0 53 → 53397 [ACK] Seq=1 Ack=57 Win=131072 Len=0 TSval=1688110851 TSecr=4275222553
8 0.087929 0.012524 2606:4700:4700::1111 2a00:6020:ad0b:8321:58a1:3… TCP 53 53397 1434 0 53 → 53397 [ACK] Seq=1 Ack=57 Win=131072 Len=1348 TSval=1688110863 TSecr=4275222553 [TCP PDU reassembled in 9]
9 0.088020 0.000091 2606:4700:4700::1111 2a00:6020:ad0b:8321:58a1:3… DNS 53 53397 1327 0 Standard query response 0xb6a8 AAAA valid.mldsa44.dnstest.dev AAAA 2a06:98c1:3120:: AAAA 2a06:98c1:3121:: RRSI
10 0.088138 0.000118 2a00:6020:ad0b:8321:58a… 2606:4700:4700::1111 TCP 53397 53 86 0 53397 → 53 [ACK] Seq=57 Ack=1349 Win=130816 Len=0 TSval=4275222568 TSecr=1688110863
11 0.088153 0.000015 2a00:6020:ad0b:8321:58a… 2606:4700:4700::1111 TCP 53397 53 86 0 53397 → 53 [ACK] Seq=57 Ack=2590 Win=129600 Len=0 TSval=4275222568 TSecr=1688110863
12 0.091288 0.003135 2a00:6020:ad0b:8321:58a… 2606:4700:4700::1111 TCP 53397 53 86 0 53397 → 53 [FIN, ACK] Seq=57 Ack=2590 Win=131072 Len=0 TSval=4275222572 TSecr=1688110863
13 0.095482 0.004194 2606:4700:4700::1111 2a00:6020:ad0b:8321:58a1:3… TCP 53 53397 86 0 53 → 53397 [FIN, ACK] Seq=2590 Ack=58 Win=131072 Len=0 TSval=1688110871 TSecr=4275222572
14 0.095615 0.000133 2a00:6020:ad0b:8321:58a… 2606:4700:4700::1111 TCP 53397 53 86 0 53397 → 53 [ACK] Seq=58 Ack=2591 Win=131072 Len=0 TSval=4275222576 TSecr=1688110871
Full TCP handshake and various TCP segments
[2 Reassembled TCP Segments (2589 bytes): #8(1348), #9(1241)]
Domain Name System (response)
Length: 2587
Transaction ID: 0xb6a8
Flags: 0x81a0 Standard query response, No error
Questions: 1
Answer RRs: 3
Authority RRs: 0
Additional RRs: 1
Queries
Answers
valid.mldsa44.dnstest.dev: type AAAA, class IN, addr 2a06:98c1:3120::
valid.mldsa44.dnstest.dev: type AAAA, class IN, addr 2a06:98c1:3121::
valid.mldsa44.dnstest.dev: type RRSIG, class IN
Name: valid.mldsa44.dnstest.dev
Type: RRSIG (46) (Resource Record Signature)
Class: IN (0x0001)
Time to live: 0 (0 seconds)
Data length: 2465
PQ-signed RRSIG length
Type Covered: AAAA (28) (IP6 Address)
Algorithm: Unknown (18)
Labels: 4
Original TTL: 0 (0 seconds)
Signature Expiration: Sep 15, 2026 17:40:24.000000000 CEST
Signature Inception: Sep 14, 2026 16:40:24.000000000 CEST
Key Tag: 23176
Signer's name: valid.mldsa44.dnstest.dev
Signature […]: e08142ff23b5e7a795ec9729d06806e31177d27a6cb2a7fab6f74430adb1673720bcc83d18f092937fb3ba8381f6572b7e810a406aff9174d922c…
Additional records
[Request In: 6]
[Time: 15.691000 milliseconds]
0060 00 00 00 00 00 c0 0c 00 2e 00 01 00 00 00 00 09
0070 a1 00 1c 12 04 00 00 00 00 6a a9 66 e8 6a a8 07
0080 58 5a 88 05 76 61 6c 69 64 07 6d 6c 64 73 61 34
0090 34 07 64 6e 73 74 65 73 74 03 64 65 76 00 e0 81
00a0 42 ff 23 b5 e7 a7 95 ec 97 29 d0 68 06 e3 11 77
00b0 d2 7a 6c b2 a7 fa b6 f7 44 30 ad b1 67 37 20 bc
00c0 c8 3d 18 f0 92 93 7f b3 ba 83 81 f6 57 2b 7e 81
00d0 0a 40 6a ff 91 74 d9 22 c7 74 7c ab 22 2d 37 00
00e0 63 8f 10 ab ef d0 a4 e5 41 fa c8 23 ee ee 8b 9e
00f0 78 6a 7d b3 27 65 0d 9b e7 f4 40 02 af d7 35 7f
0100 36 54 bb 28 96 d1 92 b2 f3 7b 55 fa f5 d7 cb bf
0110 94 5a 56 20 62 92 29 4d 92 4a 3d 4a f8 b6 21 92
0120 08 46 0c 59 99 f2 eb 43 dd e6 c8 5b 61 6c cb 5f
0130 a8 c6 3a 8a d6 b8 44 8a d3 90 95 ea 0d 34 00 e2
0140 96 7f b4 e2 ea cd 5d c9 b1 56 3f c5 72 af 75 9b
0150 06 76 ac a0 08 63 5a c9 7f 2e 5d f5 54 23 cb c1
0160 f3 64 cd 5c 43 34 b5 ef 77 53 e0 91 17 de 69 a1
0170 6e 56 2e 5b 53 ff 02 47 b3 c7 d9 f9 21 cb b6 fd
0180 b4 0b dc 4b 08 c3 75 30 83 f9 63 c7 7d 3b 30 00
0190 db 06 41 7e 31 81 27 8b 49 a4 ab a1 c6 dd fc f5
01a0 4b 77 ae 57 88 4b 3c 49 b6 85 63 fa 75 d4 46 34
01b0 cc 08 2b 38 62 8d a9 6e ff b9 61 9e 50 db d0 52
01c0 ae b3 65 8c d7 2b d5 d5 c1 43 6e c9 96 88 09 12
01d0 19 43 6c de 3d 69 b8 e0 bb 1b 14 b3 fb 45 bc c6
01e0 c5 08 3f 70 b1 cf 87 a0 26 ab 56 db f8 c5 5c 14
01f0 37 ce b8 f1 20 b2 3a c9 15 87 22 f9 81 39 ac 97
0200 27 43 c1 71 8e ed 36 28 d2 f1 05 6e fa 06 dd e7
0210 e1 02 ea 80 13 05 77 50 10 29 f6 cd 22 af 88 98
0220 c9 cc 61 da 64 9f af 52 c1 9e 39 81 4b d9 4c 8c
0230 9d bc 41 37 f2 84 36 5a 0e b0 67 dd 39 9d 17 1b
0240 73 16 04 46 f6 b7 85 ad 27 2d ae 23 c9 12 4f cf
0250 82 a5 86 ee 65 b7 f2 ed b2 41 e9 b4 b8 a9 da ec
0260 14 76 78 84 61 90 bb 4a 69 b9 29 3e e6 2a da 88
0270 41 18 fb 9b 09 84 bf 2f ac c5 12 87 a9 12 ac fa
0280 db 28 c7 0e 92 7a d8 81 ad 03 fe 3d 3c db 1c fa
0290 85 6a 41 fb 25 dd 95 d9 0e b9 ca d7 e2 ff 31 ee
Packet (1327 bytes)
Reassembled TCP (2589 bytes)
Response Length (dns.resp.len), 2 bytes
Packets: 44 · Displayed: 14 (31.8%)
Profile: Default

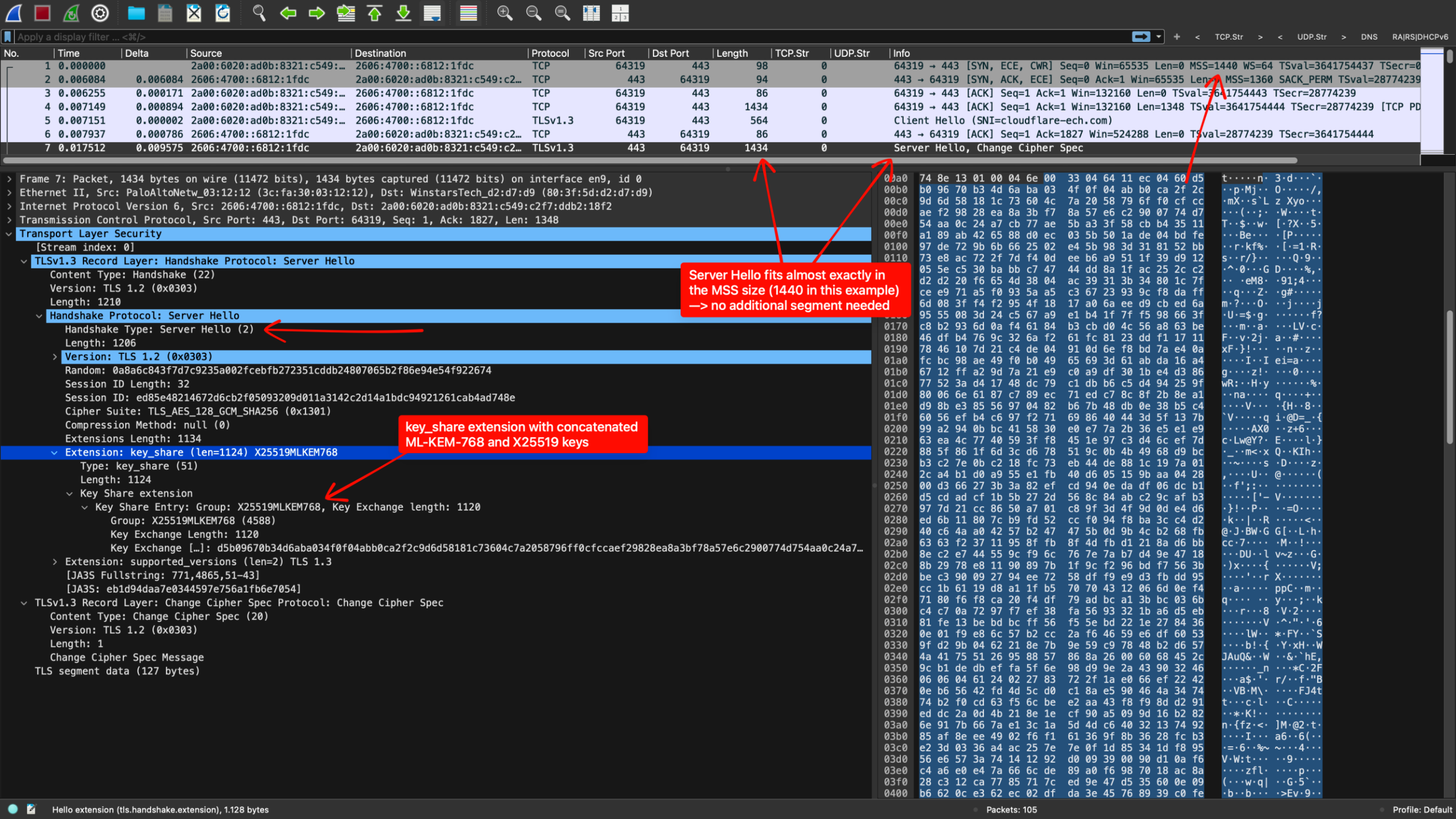
TLS (HTTPS)

- Analyse
- Algorithmen Server- & Clientseitig
- TLS-Proxies

- RFC 10024 (August 2026), https://www.rfc-editor.org/info/rfc10024/
- three hybrid key agreement mechanisms for TLS 1.3:
  - X25519MLKEM768
  - SecP256r1MLKEM768
  - SecP384r1MLKEM1024

- https://pq.cloudflareresearch.com/
- https://test.openquantumsafe.org/


normal TCP 3-way handshake
Client Hello exceeds the MSS
—> two segments!
supported group: X25519MLKEM768
0x11ec (hex) = 4588 (dec)
key_share extension with concatenated
ML-KEM-768 and X25519 keys

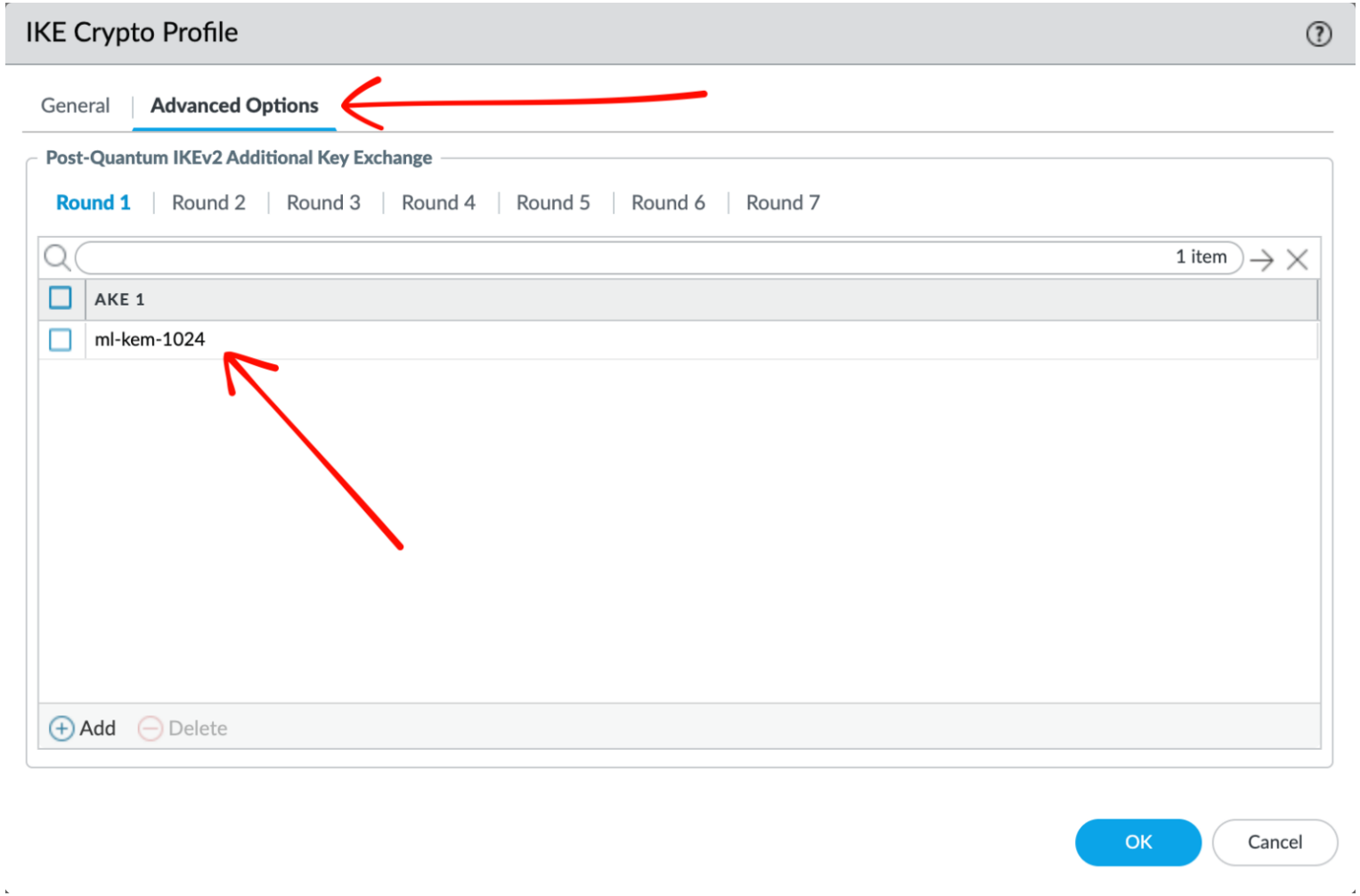

Apply a display filter ... <⌘/>
TCP.Str
UDP.Str
DNS
RA|RS|DHCPv6
No. | Time | Delta | Source | Destination | Protocol | Src Port | Dst Port | Length | TCP.Str | UDP.Str | Info
1 0.000000 2a00:6020:ad0b:8321:c549:… 2606:4700::6812:1fdc TCP 64319 443 98 0 64319 → 443 [SYN, ECE, CWR] Seq=0 Win=65535 Len=0 MSS=1440 WS=64 TSval=3641754437 TSecr=0
2 0.006084 0.006084 2606:4700::6812:1fdc 2a00:6020:ad0b:8321:c549:c2… TCP 443 64319 94 0 443 → 64319 [SYN, ACK, ECE] Seq=0 Ack=1 Win=65535 Len=0 MSS=1360 SACK_PERM TSval=28774239
3 0.006255 0.000171 2a00:6020:ad0b:8321:c549:… 2606:4700::6812:1fdc TCP 64319 443 86 0 64319 → 443 [ACK] Seq=1 Ack=1 Win=132160 Len=0 TSval=3641754443 TSecr=28774239
4 0.007149 0.000894 2a00:6020:ad0b:8321:c549:… 2606:4700::6812:1fdc TCP 64319 443 1434 0 64319 → 443 [ACK] Seq=1 Ack=1 Win=132160 Len=1348 TSval=3641754444 TSecr=28774239 [TCP PD
5 0.007151 0.000002 2a00:6020:ad0b:8321:c549:… 2606:4700::6812:1fdc TLSv1.3 64319 443 564 0 Client Hello (SNI=cloudflare-ech.com)
6 0.007937 0.000786 2606:4700::6812:1fdc 2a00:6020:ad0b:8321:c549:c2… TCP 443 64319 86 0 443 → 64319 [ACK] Seq=1 Ack=1827 Win=524288 Len=0 TSval=28774239 TSecr=3641754444
7 0.017512 0.009575 2606:4700::6812:1fdc 2a00:6020:ad0b:8321:c549:c2… TLSv1.3 443 64319 1434 0 Server Hello, Change Cipher Spec
Frame 7: Packet, 1434 bytes on wire (11472 bits), 1434 bytes captured (11472 bits) on interface en9, id 0
Ethernet II, Src: PaloAltoNetw_03:12:12 (3c:fa:30:03:12:12), Dst: WinstarsTech_d2:d7:d9 (80:3f:5d:d2:d7:d9)
Internet Protocol Version 6, Src: 2606:4700::6812:1fdc, Dst: 2a00:6020:ad0b:8321:c549:c2f7:ddb2:18f2
Transmission Control Protocol, Src Port: 443, Dst Port: 64319, Seq: 1, Ack: 1827, Len: 1348
Transport Layer Security
[Stream index: 0]
TLSv1.3 Record Layer: Handshake Protocol: Server Hello
Content Type: Handshake (22)
Version: TLS 1.2 (0x0303)
Length: 1210
Handshake Protocol: Server Hello
Handshake Type: Server Hello (2)
Length: 1206
Version: TLS 1.2 (0x0303)
Random: 0a8a6c843f7d7c9235a002fcebfb272351cddb24807065b2f86e94e54f922674
Session ID Length: 32
Session ID: ed85e48214672d6cb2f05093209d011a3142c2d14a1bdc94921261cab4ad748e
Cipher Suite: TLS_AES_128_GCM_SHA256 (0x1301)
Compression Method: null (0)
Extensions Length: 1134
Extension: key_share (len=1124) X25519MLKEM768
Type: key_share (51)
Length: 1124
Key Share extension
Key Share Entry: Group: X25519MLKEM768, Key Exchange length: 1120
Group: X25519MLKEM768 (4588)
Key Exchange Length: 1120
Key Exchange […]: d5b09670b34d6aba034f0f04abb0ca2f2c9d6d58181c73604c7a2058796ff0cfccaef29828ea8a3bf78a57e6c2900774d754aa0c24a7…
Extension: supported_versions (len=2) TLS 1.3
[JA3S Fullstring: 771,4865,51-43]
[JA3S: eb1d94daa7e0344597e756a1fb6e7054]
TLSv1.3 Record Layer: Change Cipher Spec Protocol: Change Cipher Spec
Content Type: Change Cipher Spec (20)
Version: TLS 1.2 (0x0303)
Length: 1
Change Cipher Spec Message
TLS segment data (127 bytes)
Server Hello fits almost exactly in the MSS size (1440 in this example) —> no additional segment needed
key_share extension with concatenated ML-KEM-768 and X25519 keys
00a0 74 8e 13 01 00 04 6e 00 33 04 64 11 ec 04 60 d5 t·····n· 3·d···`·
00b0 b0 96 70 b3 4d 6a ba 03 4f 0f 04 ab b0 ca 2f 2c ··p·Mj·· O·····/,
00c0 9d 6d 58 18 1c 73 60 4c 7a 20 58 79 6f f0 cf cc ·mX··s`L z Xyo···
00d0 ae f2 98 28 ea 8a 3b f7 8a 57 e6 c2 90 07 74 d7 ···(··;· ·W····t·
00e0 54 aa 0c 24 a7 cb 77 ae 5b a3 3f 58 cb b4 35 11 T··$··w· [·?X··5·
00f0 a1 89 ab 42 65 88 d0 ec 03 5b 50 1a de 04 bd fe ···Be··· ·[P·····
0100 97 de 72 9b 6b 66 25 02 e4 5b 98 3d 31 81 52 bb ··r·kf%· ·[·=1·R·
0110 73 e8 ac 72 2f 7d f4 0d ee b6 a9 51 1f 39 d9 12 s··r/}·· ···Q·9··
05 5e c5 30 ba bb c7 47 44 dd 8a 1f ac 25 2c c2 ·^·0···G D····%,·
d2 d2 20 f6 65 4d 38 04 ac 39 31 3b 34 80 1c 7f ·· ·eM8· ·91;4···
ce e9 71 a5 f0 93 5a a5 c3 67 23 93 9c f8 da ff ··q···Z· ·g#·····
6d 08 3f f4 f2 95 4f 18 17 a0 6a ee d9 cb ed 6a m·?···O· ··j····j
95 55 08 3d 24 c5 67 a9 e1 b4 1f 7f f5 98 66 3f ·U·=$·g· ·····f?
0170 c8 b2 93 6d 0a f4 61 84 b3 cb d0 4c 56 a8 63 be ···m··a· ···LV·c·
0180 46 df b4 76 9c 32 6a f2 61 fc 81 23 dd f1 17 11 F··v·2j· a··#····
0190 78 46 10 7d 21 c4 de 04 91 0d 6e f8 bd 7a e4 0a xF·}!··· ··n··z··
01a0 fc bc 98 ae 49 f0 b0 49 65 69 3d 61 ab da 16 a4 ····I··I ei=a····
01b0 67 12 ff a2 9d 7a 21 e9 c0 a9 df 30 1b e4 d3 86 g····z!· ···0····
01c0 77 52 3a d4 17 48 dc 79 c1 db b6 c5 d4 94 25 9f wR:··H·y ·····%·
01d0 80 06 6e 61 87 c7 89 ec 71 ed c7 8c 8f 2b 8e a1 ··na···· q····+··
01e0 d9 8b e3 85 56 97 04 82 b6 7b 48 db 0e 38 b5 c4 ····V··· ·{H··8··
01f0 60 56 ef b4 c6 97 f2 71 69 86 40 44 3d 5f 13 7b `V·····q i·@D=_·{
0200 99 a2 94 0b bc 41 58 30 e0 e7 7a 2b 36 e5 e1 e9 ·····AX0 ··z+6···
0210 63 ea 4c 77 40 59 3f f8 45 1e 97 c3 d4 6c ef 7d c·Lw@Y?· E····l·}
0220 88 5f 86 1f 6d 3c d6 78 51 9c 0b 4b 49 68 d9 bc ·_··m<·x Q··KIh··
0230 b3 c2 7e 0b c2 18 fc 73 eb 44 de 88 1c 19 7a 01 ··~····s ·D····z·
0240 2c a4 b1 d0 a9 55 e1 fb 40 d6 05 15 9b aa 04 28 ,····U·· @·····(
0250 00 d3 66 27 3b 3a 82 ef cd 94 0e da df 06 dc b1 ··f';:·· ·····
0260 d5 cd ad cf 1b 5b 27 2d 56 8c 84 ab c2 9c af b3 ·····['- V·····
0270 97 7d 21 cc 86 50 a7 01 c8 9f 3d 4f 9d 0d e4 d6 ·}!··P·· ··=O····
0280 ed 6b 11 80 7c b9 fd 52 cc f0 94 f8 ba 3c c4 d2 ·k··|··R ·····<··
0290 40 c6 4a a0 42 57 b2 47 47 5b 0d 9b 4c b2 68 fb @·J·BW·G G[··L·h·
02a0 63 63 f2 37 11 95 8f fb 8f 4d fb d1 21 8a d6 bb cc·7···· ·M··!···
02b0 8e c2 e7 44 55 9c f9 6c 76 7e 7a b7 d4 9e 47 18 ···DU··l v~z···G·
02c0 8b 29 78 e8 11 90 89 7b 1f 9c f2 96 bd f7 56 3b ·)x····{ ·····V;
02d0 be c3 90 09 27 94 ee 72 58 df f9 e9 d3 fb dd 95 ····'··r X·····
02e0 cc 1b 61 19 d8 a1 1f b5 70 70 43 12 06 6d 0e f4 ··a····· ppC··m··
02f0 71 80 f6 f8 ca 20 f4 df 79 ad bc a1 3b bc 03 6b q···· ·· y···;··k
0300 c4 c7 0a 72 97 f7 ef 38 fa 56 93 32 1b a6 d5 eb ···r···8 ·V·2····
0310 81 fe 13 be bd bc ff 56 f5 5e bd 22 1e 27 84 36 ·····V ·^·"·'·6
0320 0e 01 f9 e8 6c 57 b2 cc 2a f6 46 59 e6 df 60 53 ····lW·· *·FY··`S
0330 9f d2 9b 04 62 21 8e 7b 9e 59 c9 78 48 b2 d6 57 ····b!·{ ·Y·xH··W
0340 4a 41 75 51 26 95 88 57 86 8a 26 00 60 68 45 2c JAuQ&··W ··&·`hE,
0350 9c b1 de db ef fa 5f 6e 98 d9 9e 2a 43 90 32 46 ·····_n ···*C·2F
0360 06 06 04 61 24 02 27 83 72 2f 1a e0 66 ef 22 42 ···a$·'· r/··f·"B
0370 0e b6 56 42 fd 4d 5c d0 c1 8a e5 90 46 4a 34 74 ··VB·M\· ····FJ4t
0380 74 b2 f0 cd 63 f5 6c be e2 aa 43 f8 f9 8d d2 91 t···c·l· ··C·····
0390 ed dc 2a 0d 4b 21 8e 1e cf 90 a5 09 9d 16 b2 82 ··*·K!·· ········
03a0 6e 91 7b 66 7a e1 3c 1a 5d 4d c6 40 32 13 74 92 n·{fz·<·]M·@2·t·
03b0 85 af 8e ee 49 02 f6 f1 61 36 9f 8b 36 28 fc b3 ····I··· a6··6(··
03c0 e2 3d 03 36 a4 ac 25 7e 7e 0f 1d 85 34 1d f8 95 ·=·6··%~ ~···4···
03d0 56 e6 57 3a 74 14 12 92 d0 09 39 00 90 d1 0a f6 V·W:t··· ··9·····
03e0 c4 a6 e0 e4 7a 66 6c de 89 a0 f6 98 70 18 ac 8a ····zfl· ····p···
03f0 28 c3 12 ca 77 85 71 7c ed 9e 47 d5 35 60 0e 09 (···w·q| ··G·5`··
0400 b6 62 0c e3 62 ec 02 df da 3e 45 76 89 39 c0 fe ·b··b··· ·>Ev·9··
Hello extension (tls.handshake.extension), 1.128 bytes
Packets: 105
Profile: Default

IPsec/IKEv2

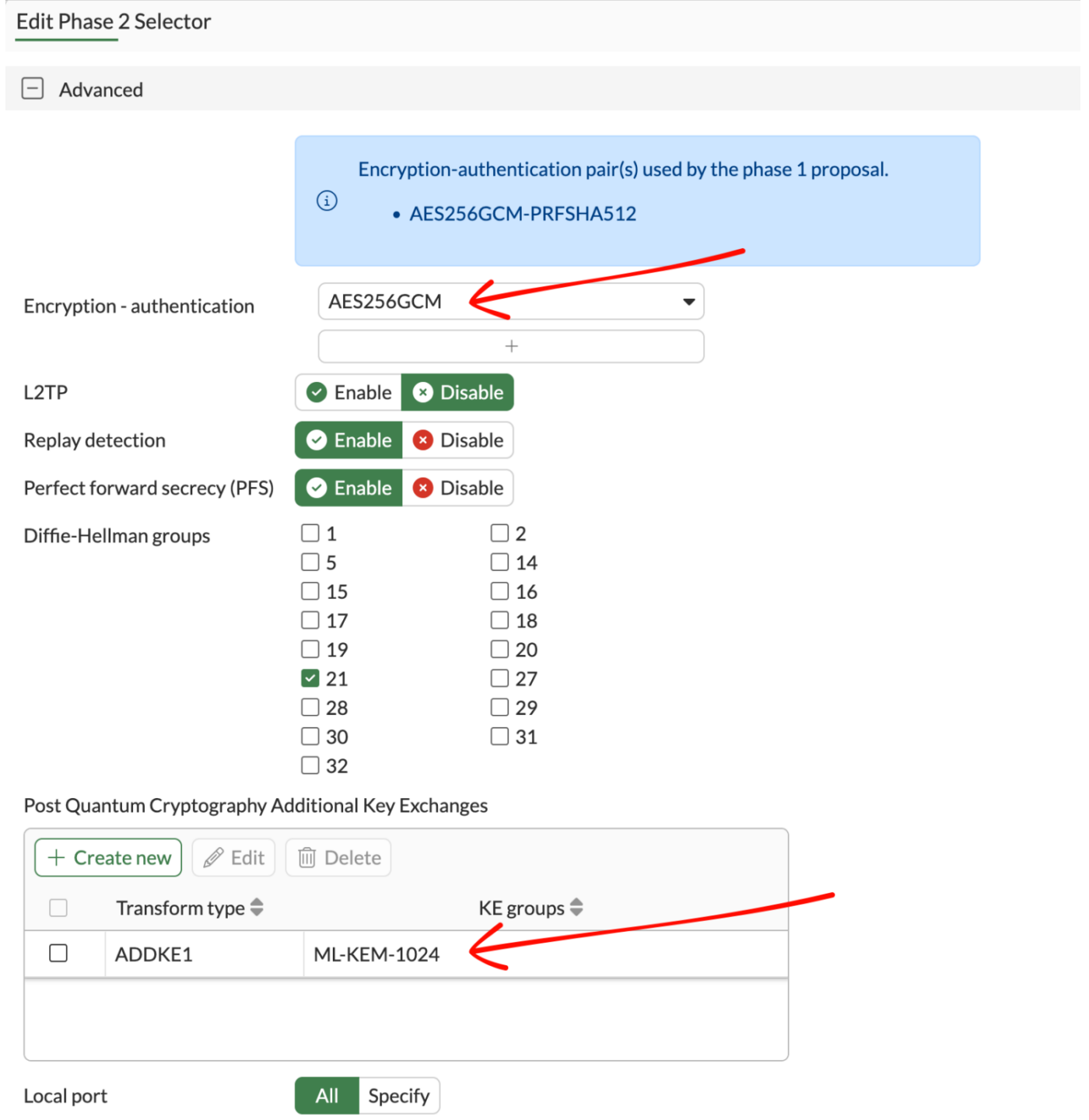
- hybrid modes (ECDH + ML-KEM)
- IKEv2 (phase1) and IPsec (phase2)

- https://weberblog.net/pqc-vpn-tunnel-with-palo/
- https://weberblog.net/pqc-vpn-tunnel-between-palo-alto-fortigate/
- https://weberblog.net/packet-capture-of-a-post-quantum-site-to-site-vpn/

IPsec/IKEv2: Palo Alto Networks



IPsec/IKEv2: FortiGate



PQC VPN Palo-Forti 02 hybrid group21 mlkem.pcapng — Johannes Weber - Weberblog.net

Apply a display filter ... <⌘/>

No.	Time	Delta	Source	Destination	Protocol	Src Port	Dst Port	Length	Comment	Info
1	0.000000000		2a00:6020:ad0b:8303::9	2a00:6020:ad0b:8303::2	ISAKMP	500	500	330	Start: IKEv2…	IKE_SA_INIT MID=00 Initiator Request
2	12.020092000	12.020092000	2a00:6020:ad0b:8303::9	2a00:6020:ad0b:8303::2	ISAKMP	500	500	330		IKE_SA_INIT MID=00 Initiator Request
3	21.980342000	9.960250000	2a00:6020:ad0b:8303::9	2a00:6020:ad0b:8303::2	ISAKMP	500	500	330		IKE_SA_INIT MID=00 Initiator Request
4	24.990211000	3.009869000	2a00:6020:ad0b:8303::9	2a00:6020:ad0b:8303::2	ISAKMP	500	500	330		IKE_SA_INIT MID=00 Initiator Request
5	31.000216000	6.010005000	2a00:6020:ad0b:8303::9	2a00:6020:ad0b:8303::2	ISAKMP	500	500	330		IKE_SA_INIT MID=00 Initiator Request
6	37.766680000	6.766464000	2a00:6020:ad0b:8303::2	2a00:6020:ad0b:8303::9	ISAKMP	500	500	387		IKE_SA_INIT MID=00 Initiator Request
7	37.786489000	0.019809000	2a00:6020:ad0b:8303::9	2a00:6020:ad0b:8303::2	ISAKMP	500	500	362		IKE_SA_INIT MID=00 Responder Response
8	37.810114000	0.023625000	2a00:6020:ad0b:8303::2	2a00:6020:ad0b:8303::9	ISAKMP	500	500	1306		IKE_INTERMEDIATE MID=01 Initiator Request (fragment 1/2)
9	37.810142000	0.000028000	2a00:6020:ad0b:8303::2	2a00:6020:ad0b:8303::9	ISAKMP	500	500	522		IKE_INTERMEDIATE MID=01 Initiator Request (fragment 2/2)
10	37.813543000	0.003401000	2a00:6020:ad0b:8303::9	2a00:6020:ad0b:8303::2	ISAKMP	500	500	1188		IKE_INTERMEDIATE MID=01 Responder Response (fragment 1/2)
11	37.813546000	0.000003000	2a00:6020:ad0b:8303::9	2a00:6020:ad0b:8303::2	ISAKMP	500	500	650		IKE_INTERMEDIATE MID=01 Responder Response (fragment 2/2)
12	37.815927000	0.002381000	2a00:6020:ad0b:8303::2	2a00:6020:ad0b:8303::9	ISAKMP	500	500	390		IKE_AUTH MID=02 Initiator Request
13	37.817223000	0.001296000	2a00:6020:ad0b:8303::9	2a00:6020:ad0b:8303::2	ISAKMP	500	500	355		IKE_AUTH MID=02 Responder Response
14	40.766077000	2.948854000	2a00:6020:ad0b:8303::2	2a00:6020:ad0b:8303::9	ESP			206		ESP (SPI=0xbea130a5)
15	43.020297000	2.254220000	2a00:6020:ad0b:8303::9	2a00:6020:ad0b:8303::2	ISAKMP	500	500	330		IKE_SA_INIT MID=00 Initiator Request
16	43.027405000	0.007108000	2a00:6020:ad0b:8303::2	2a00:6020:ad0b:8303::9	ISAKMP	500	500	339		IKE_SA_INIT MID=00 Responder Response
17	43.044296000	0.016891000	2a00:6020:ad0b:8303::2	2a00:6020:ad0b:8303::9	ISAKMP	500	500	134		INFORMATIONAL MID=03 Initiator Request
18	43.044517000	0.000221000	2a00:6020:ad0b:8303::9	2a00:6020:ad0b:8303::2	ISAKMP	500	500	127		INFORMATIONAL MID=03 Responder Response
19	43.047450000	0.002933000	2a00:6020:ad0b:8303::9	2a00:6020:ad0b:8303::2	ISAKMP	500	500	1188		IKE_INTERMEDIATE MID=01 Initiator Request (fragment 1/2)
20	43.047451000	0.000001000	2a00:6020:ad0b:8303::9	2a00:6020:ad0b:8303::2	ISAKMP	500	500	650		IKE_INTERMEDIATE MID=01 Initiator Request (fragment 2/2)
21	43.053051000	0.005600000	2a00:6020:ad0b:8303::2	2a00:6020:ad0b:8303::9	ISAKMP	500	500	1306		IKE_INTERMEDIATE MID=01 Responder Response (fragment 1/2)
22	43.053052000	0.000001000	2a00:6020:ad0b:8303::2	2a00:6020:ad0b:8303::9	ISAKMP	500	500	522		IKE_INTERMEDIATE MID=01 Responder Response (fragment 2/2)

```
Frame 6: Packet, 387 bytes on wire (3096 bits), 387 bytes captured (3096 bits) on interface Allegro interface 4, id 3
Ethernet II, Src: PaloAltoNetw_04:91:10 (3c:fa:30:04:91:10), Dst: Fortinet_51:43:06 (94:f3:92:51:43:06)
Internet Protocol Version 6, Src: 2a00:6020:ad0b:8303::2, Dst: 2a00:6020:ad0b:8303::9
User Datagram Protocol, Src Port: 500, Dst Port: 500
Internet Security Association and Key Management Protocol
    Initiator SPI: 9371eda156662819
    Responder SPI: 0000000000000000
    Next payload: Security Association (33)
  > Version: 2.0
    Exchange type: IKE_SA_INIT (34)
  > Flags: 0x08 (Initiator, No higher version, Request)
    Message ID: 0x00000000
    Length: 325
  > Payload: Security Association (33)
  v Payload: Key Exchange (34)
      Next payload: Nonce (40)
      0... .... = Critical Bit: Not critical
      .000 0000 = Reserved: 0x00
      Payload length: 140
      Key Exchange Method: 521-bit random ECP group (21)
      Reserved: 0000
      Key Exchange Data […]: 01a2317efd725eea22cc77698016f8f0b3a3434a71102c3c75c77feb6513123f2da7108da095becddef2c974c1d6ce02b9ef8342bf620…
  > Payload: Nonce (40)
  > Payload: Notify (41) - INTERMEDIATE_EXCHANGE_SUPPORTED
  > Payload: Notify (41) - IKEV2_FRAGMENTATION_SUPPORTED
  > Payload: Notify (41) - Private Use - STATUS TYPES
```

hybrid (classical + PQC) VPN:
still DH group 21 in the IKE_SA_INIT

but asking for INTERMEDIATE_EXCHANGE
and IKEV2_FRAGMENTATION support

```
0000  94 f3 92 51 43 06 3c fa  30 04 91 10 86 dd 60 00   ···QC·<· 0·····`·
0010  65 1d 01 4d 11 3f 2a 00  60 20 ad 0b 83 03 00 00   e··M·?*· ` ·····
0020  00 00 00 00 00 00 02 2a  00 60 20 ad 0b 83 03 00   ·····*· ` ·····
0030  00 00 00 00 00 09 01 f4  01 f4 01 4d fd 76 93 71   ···········M·v·q
0040  ed a1 56 66 28 19 00 00  00 00 00 00 00 00 21 20   ··Vf(··· ·····!
0050  22 08 00 00 00 00 00 00  01 45 22 00 00 60 00 00   "······ ·E"··`··
0060  00 5c 01 01 00 0a 03 00  00 0c 01 00 00 14 80 0e   ·\····· ········
0070  01 00 03 00 00 08 02 00  00 07 03 00 00 08 04 00   ········ ········
0080  00 15 03 00 00 08 06 00  00 25 03 00 00 08 07 00   ········ ·%······
0090  00 00 03 00 00 08 08 00  00 00 03 00 00 08 09 00   ········ ········
00a0  00 00 03 00 00 08 0a 00  00 00 03 00 00 08 0b 00   ········ ········
00b0  00 00 00 00 00 08 0c 00  00 00 28 00 00 8c 00 15   ········ ··(·····
00c0  00 00 01 a2 31 7e fd 72  5e ea 22 cc 77 69 80 16   ····1~·r ^·"·wi··
00d0  f8 f0 b3 a3 43 4a 71 10  2c 3c 75 c7 7f eb 65 13   ····CJq· ,<u···e·
00e0  12 3f 2d a7 10 8d a0 95  be cd de f2 c9 74 c1 d6   ·?-····· ·····t··
00f0  ce 02 b9 ef 83 42 bf 62  09 0f c2 41 b7 d1 66 fa   ·····B·b ···A··f·
0100  f5 28 24 ca 01 f3 02 0f  1f c1 31 a3 97 de f3 35   ·($····· ··1····5
0110  54 ee 5f 24 0d c8 4f c6  a5 60 f7 b3 71 ec 44 39   T·_$··O· ·`··q·D9
0120  19 80 dd 83 61 75 e5 51  34 af d0 61 e3 41 f3 3c   ····au·Q 4··a·A·<
0130  44 0e 86 71 be 45 e4 2f  ec ba 0d 95 96 3f 2b 09   D··q·E·/ ·····?+·
0140  d4 5a c5 78 47 44 29 00  00 24 b0 c7 24 31 7a 13   ·Z·xGD)· ·$··$1z·
0150  79 33 3a 5a 97 54 04 3a  14 7c c1 94 b6 ee 4c 45   y3:Z·T·: ·|····LE
0160  d6 ea 54 bf 01 88 af af  09 df 29 00 00 09 00 00   ··T····· ··)·····
0170  40 36 00 29 00 00 08 00  00 40 2e 00 00 00 08 00   @6·)···· ·@.·····
0180  00 a0 02                                          ···
```

PQC VPN Palo-Forti 02 hybrid group21 mlkem.pcapng — Johannes Weber - Weberblog.net

Apply a display filter ... <⌘/>

No.	Time	Delta	Source	Destination	Protocol	Src Port	Dst Port	Length	Comment	Info
1	0.000000000		2a00:6020:ad0b:8303::9	2a00:6020:ad0b:8303::2	ISAKMP	500	500	330	Start: IKEv2…	IKE_SA_INIT MID=00 Initiator Request
2	12.020092000	12.020092000	2a00:6020:ad0b:8303::9	2a00:6020:ad0b:8303::2	ISAKMP	500	500	330		IKE_SA_INIT MID=00 Initiator Request
3	21.980342000	9.960250000	2a00:6020:ad0b:8303::9	2a00:6020:ad0b:8303::2	ISAKMP	500	500	330		IKE_SA_INIT MID=00 Initiator Request
4	24.990211000	3.009869000	2a00:6020:ad0b:8303::9	2a00:6020:ad0b:8303::2	ISAKMP	500	500	330		IKE_SA_INIT MID=00 Initiator Request
5	31.000216000	6.010005000	2a00:6020:ad0b:8303::9	2a00:6020:ad0b:8303::2	ISAKMP	500	500	330		IKE_SA_INIT MID=00 Initiator Request
6	37.766680000	6.766464000	2a00:6020:ad0b:8303::2	2a00:6020:ad0b:8303::9	ISAKMP	500	500	387		IKE_SA_INIT MID=00 Initiator Request
7	37.786489000	0.019809000	2a00:6020:ad0b:8303::9	2a00:6020:ad0b:8303::2	ISAKMP	500	500	362		IKE_SA_INIT MID=00 Responder Response
8	37.810114000	0.023625000	2a00:6020:ad0b:8303::2	2a00:6020:ad0b:8303::9	ISAKMP	500	500	1306		IKE_INTERMEDIATE MID=01 Initiator Request (fragment 1/2)
9	37.810142000	0.000028000	2a00:6020:ad0b:8303::2	2a00:6020:ad0b:8303::9	ISAKMP	500	500	522		IKE_INTERMEDIATE MID=01 Initiator Request (fragment 2/2)
10	37.813543000	0.003401000	2a00:6020:ad0b:8303::9	2a00:6020:ad0b:8303::2	ISAKMP	500	500	1188		IKE_INTERMEDIATE MID=01 Responder Response (fragment 1/2)
11	37.813546000	0.000003000	2a00:6020:ad0b:8303::9	2a00:6020:ad0b:8303::2	ISAKMP	500	500	650		IKE_INTERMEDIATE MID=01 Responder Response (fragment 2/2)
12	37.815927000	0.002381000	2a00:6020:ad0b:8303::2	2a00:6020:ad0b:8303::9	ISAKMP	500	500	1306		IKE_AUTH MID=02 Initiator Request
13	37.817223000	0.001296000	2a00:6020:ad0b:8303::9	2a00:6020:ad0b:8303::2	ISAKMP	500	500	355		IKE_AUTH MID=02 Responder Response
14	40.766077000	2.948854000	2a00:6020:ad0b:8303::2	2a00:6020:ad0b:8303::9	ESP			206		ESP (SPI=0xbea130a5)
15	43.020297000	2.254220000	2a00:6020:ad0b:8303::9	2a00:6020:ad0b:8303::2	ISAKMP	500	500	330		IKE_SA_INIT MID=00 Initiator Request
16	43.027405000	0.007108000	2a00:6020:ad0b:8303::2	2a00:6020:ad0b:8303::9	ISAKMP	500	500	339		IKE_SA_INIT MID=00 Responder Response
17	43.044296000	0.016891000	2a00:6020:ad0b:8303::2	2a00:6020:ad0b:8303::9	ISAKMP	500	500	134		INFORMATIONAL MID=03 Initiator Request
18	43.044517000	0.000221000	2a00:6020:ad0b:8303::9	2a00:6020:ad0b:8303::2	ISAKMP	500	500	127		INFORMATIONAL MID=03 Responder Response
19	43.047450000	0.002933000	2a00:6020:ad0b:8303::9	2a00:6020:ad0b:8303::2	ISAKMP	500	500	1188		IKE_INTERMEDIATE MID=01 Initiator Request (fragment 1/2)
20	43.047451000	0.000001000	2a00:6020:ad0b:8303::9	2a00:6020:ad0b:8303::2	ISAKMP	500	500	650		IKE_INTERMEDIATE MID=01 Initiator Request (fragment 2/2)
21	43.053051000	0.005600000	2a00:6020:ad0b:8303::2	2a00:6020:ad0b:8303::9	ISAKMP	500	500	1306		IKE_INTERMEDIATE MID=01 Responder Response (fragment 1/2)
22	43.053052000	0.000001000	2a00:6020:ad0b:8303::2	2a00:6020:ad0b:8303::9	ISAKMP	500	500	522		IKE_INTERMEDIATE MID=01 Responder Response (fragment 2/2)

followed by two fragments (!) of IKE_INTERMEDIATE

```
> Frame 8: Packet, 1306 bytes on wire (10448 bits), 1306 bytes captured (10448 bits) on interface Allegro interface 4, id 3
> Ethernet II, Src: PaloAltoNetw_04:91:10 (3c:fa:30:04:91:10), Dst: Fortinet_51:43:06 (94:f3:92:51:43:06)
> Internet Protocol Version 6, Src: 2a00:6020:ad0b:8303::2, Dst: 2a00:6020:ad0b:8303::9
> User Datagram Protocol, Src Port: 500, Dst Port: 500
v Internet Security Association and Key Management Protocol
    Initiator SPI: 9371eda156662819
    Responder SPI: 563203ba62c2309c
    Next payload: Encrypted and Authenticated Fragment (53)
  > Version: 2.0
    Exchange type: IKE_INTERMEDIATE (43)
  > Flags: 0x08 (Initiator, No higher version, Request)
    Message ID: 0x00000001
    Length: 1244
  v Payload: Encrypted and Authenticated Fragment (53)
      Next payload: Key Exchange (34)
      0... .... = Critical Bit: Not critical
      .000 0000 = Reserved: 0x00
      Payload length: 1216
      Fragment Number: 1
      Total Fragments: 2
```

additional stuff for ML-KEM key exhange

```
0050  2b 08 00 00 00 01 00 00  04 dc 22 00 04 c0 00 01   +·····  ··"·····
0060  00 02 a5 34 cb ed 81 28  a5 b7 e8 70 fa 7a 5f a0   ···4···(  ···p·z_·
0070  73 75 1b 88 a5 56 ba 42  e5 36 0a ff 0d e1 dd 92   su···V·B  ·6·····
0080  fe b6 7a 84 16 f7 98 d2  d9 b2 95 d3 8b 38 c2 a1   ··z·····  ·····8··
0090  55 8e 84 37 51 29 82 f9  1e b3 19 d7 0c b6 ef 9c   U··7Q)··  ········
00a0  45 41 95 e1 9e 1c c3 16  eb a2 33 e4 bd 70 25 79   EA·····  ··3··p%y
00b0  2d e1 87 a0 cd 0a 61 00  0a 0f 15 64 01 29 7a 11   −·····a·  ···d·)z·
00c0  a7 ba 80 42 e4 82 45 65  50 5e e5 6e 86 ee a8 5a   ···B··Ee  P^·n···Z
00d0  36 3c 86 b3 eb 50 b1 3d  a6 44 84 93 de fd db d9   6<···P·=  ·D·····
00e0  3a 00 fb 44 a6 cd 89 28  dd 75 64 86 c7 f6 4a a4   :··D···(  ·ud·|·J·
00f0  b0 05 4d ea 30 3b 6c 67  b2 da 5f a4 b2 33 48 24   ··M·0;lg  ··_··3H$
0100  59 3c 8f 8f ea 5d 4b 4f  1d 87 a2 1d 8d 0f 82 1d   Y<···]KO  ·····
0110  c0 1f 94 45 7c 10 98 8a  e6 ec 29 10 3e 89 8d 07   ···E|···  ··)·>···
0120  2b 39 aa 5b 7c 96 26 c8  1e af 73 c2 6b 39 f5 15   +9·[|·&·  ··s·k9··
0130  8a de 91 a0 7d b9 55 33  4e 20 24 59 b9 d7 bf cb   ····}·U3  N $Y····
0140  51 c4 70 80 4d aa b7 65  5d 06 9b ec fd f8 f7 29   Q·p·M··e  ]·····)
0150  56 db 9e 4f 0c d6 fa e2  f3 7e 47 67 f1 e1 1d e4   V··O····  ·~Gg····
0160  82 dc 48 fc 25 5d 84 2c  a1 c4 17 2e ed e0 1c 0c   ··H·%]·,  ···.····
0170  39 ed 8e 83 a0 1b e5 19  6b 37 a9 ee e9 44 15 5f   9·······  k7···D·_
0180  63 27 41 a9 9a fa c8 86  12 4e 4f ac c6 bf 49 04   c'A·····  ·NO···I·
0190  d5 30 5e c7 9c 09 e4 2c  14 07 78 d2 07 32 6d ea   ·0^····,  ··x··2m·
01a0  e3 ff 32 07 1c c0 9b dd  2a ab 0a c2 28 a5 81 69   ··2·····  *···(··i
01b0  19 c8 ad 40 e9 78 cf da  96 01 39 c1 3c 26 29 bc   ···@·x··  ··9·<&)·
01c0  ca da 54 77 0b 7e 1d 9a  26 3c 6d 07 8d 4d d6 bf   ··Tw·~··  &<m··M··
01d0  16 7a f7 e1 19 9a 5f cf  12 0b b9 1f e7 98 30 6f   ·z····_·  ·····0o
01e0  79 a3 73 6c 5a 96 94 b9  4e 60 82 0a eb 31 3b 04   y·slZ···  N`···1;·
01f0  67 cb ca d7 27 6b 2c c8  ad 4e d7 4e a5 bf 52 22   g···'k,·  ·N·N··R"
0200  f6 25 b2 48 c7 2d a9 8e  6d 59 25 35 51 d7 b0 24   ·%·H·−··  mY%5Q··$
0210  c3 58 0c a3 74 59 eb 15  f3 65 57 a6 66 74 0d eb   ·X··tY··  ·eW·ft··
0220  a3 d2 32 94 f2 ab 30 06  cb a5 38 64 1f e6 30 6d   ··2···0·  ··8d··0m
0230  3c fb e1 14 27 4b 13 d7  1e 3c f9 2d a5 7b 98 0f   <···'K··  ·<·−·{··
0240  e0 84 1f c7 cc 1c 34 d7  fc 09 f1 ff fc 6a 67 7e   ·····4·  ·····jg~
0250  b4 9a 64 4a b3 6a ed db  d9 8d aa 1c 0d e4 0a ad   ··dJ·j··  ········
```

ISAKMP Payload Type (isakmp.typepayload), 1.216 bytes

Packets: 298 · Comments: 2

Profile: Default

Security-as-a-Podcast #07 – PQC – Post-Quantum Cryptography

/ Ansprechpartner

Kontaktieren Sie uns

Johannes Weber
Senior IT-Security Consultant

Mobil: +49 151 19598770
E-Mail: johannes.weber@sva.de

SVA System Vertrieb Alexander GmbH
Borsigstraße 26
65205 Wiesbaden

www.sva.de