Der lange Weg zur quantenresistenten PKI

Hans-Joachim Knobloch (Secorvo)
Noah Freising (Hochschule Mannheim, inzwischen: RUB)

32. DFN-Konferenz „Sicherheit in vernetzten Systemen“

12.02.2025

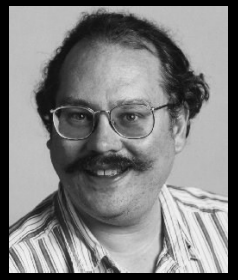
secorvo
security consulting

3. September 1967

Wir schreiben das Jahr 1994….

- Windows 95 soll bald erscheinen
- Es gibt jetzt einen Nachfolger für die 486-CPU namens „Pentium“
- …
- Es wurden gerade DSA und SHA-1 standardisiert
- Der erste Krypto-Smartcard-Chip unterstützt RSA-512
- Mathematiker und Kryptologen untersuchen jetzt etwas, das sich „Elliptische Kurven“ nennt

Wir schreiben das Jahr 1994….



Peter Shor:

Wenn wir mit einer Art von Quantencomputern rechnen könnten, dann kann ich große Zahlen in Primfaktoren zerlegen…

…und nebenbei auch DSA, ECDSA & Co. brechen

Lov Grover (1996):

Dieser Quantencomputer könnte auch schnell in riesigen Datenmengen suchen

AES-256 → AES-128

SHA-512 → SHA-256

usw.

Reaktionen

- Mathematiker:
  Cool
- Physiker:
  Hold my beer…
- Investoren:
  Damit müsste Geld zu machen sein

Viele Forschungsmillionen später…

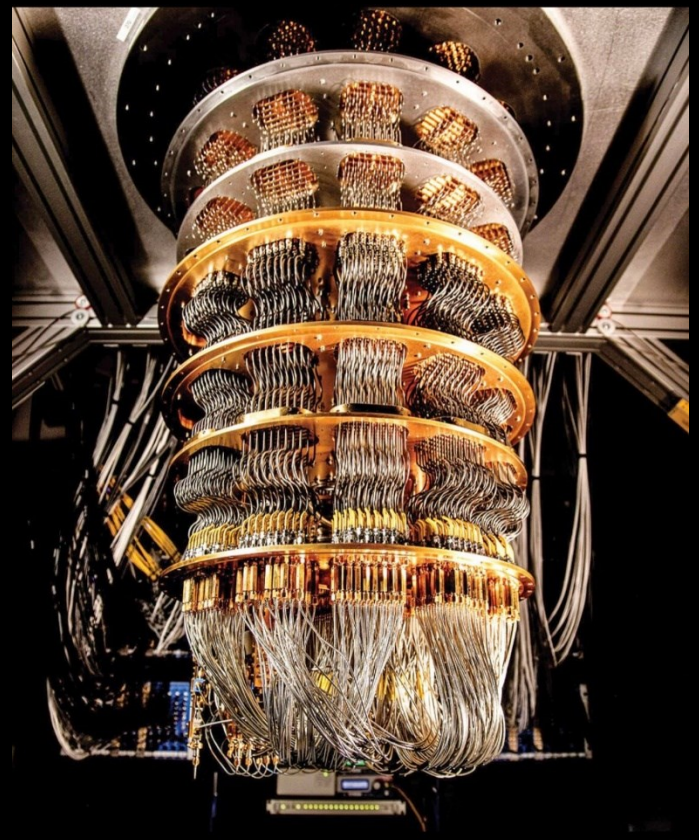


Bild: Google Quantum AI Project

- „Weltrekord“-Faktorisierung mit dem Shor-Algorithmus: 21 = 7*3
- Marketing-Schlagworte: „Quantum Supremacy“, …
- Aber auch immer wieder Fortschritte

Wir brauchen neue „Post-Quantum“ Algorithmen...

- NIST 2016: Wettbewerb!
- NIST 2024: FIPS 203 bis FIPS 205/206

Kyber	→ FIPS 203: ML-KEM
Dilithium	→ FIPS 204: ML-DSA
Sphincs+	→ FIPS 205: SLH-DSA
Falcon	→ *angekündigt für 2025 als FIPS 206: FN-DSA*

Wir brauchen neue „Post-Quantum“ Algorithmen...

- NIST 2016: Wettbewerb!
- NIST 2024: FIPS 203 bis FIPS 205/206

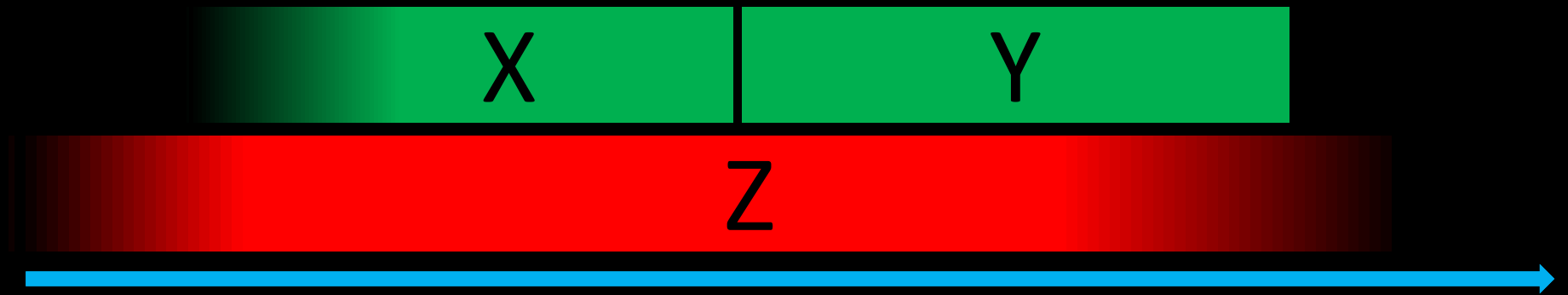
  Kyber → FIPS 203: ML-KEM
  Dilithium → FIPS 204: ML-DSA
  Sphincs+ → FIPS 205: SLH-DSA
  Falcon → *angekündigt für 2025 als FIPS 206: FN-DSA*

- *Wie sicher sind die?*
  - Juli 2022: SIKE ist als heißer Kandidat als KEM in Runde 4 des Wettbewerbs eingezogen
  - August 2022: SIKE gebrochen (mit herkömmlichen Computern)
  - Neu und anders: Schwachstellen und Seitenkanäle bei der Implementierung absehbar
- Daher eher Hybrid („Composite“): ML-DSA mit ECDSA oder RSA kombiniert

Wann kommt also der Quantencomputer raus?

- Michele Mosca 2015:
  „Die Wahrscheinlichkeit, dass eine grundlegende Public-Key-Verschlüsselung bis 2026 durch Quanten geknackt wird, liegt bei 1:7, die Wahrscheinlichkeit, dass dies bis 2031 geschieht, bei 1:2.“
- BSI 2023:
  „mindestens ein Jahrzehnt, wahrscheinlicher zwei, dauern wird - sofern keine Disruptionen stattfinden“ = 2043
- BSI Stand Ende 2024: 16 Jahre statt 20 Jahren = 2040
- *Gegenfrage:*
  Wann kommen produktive Kernfusions-Kraftwerke?
  … seit 40 Jahren möglicherweise in den nächsten 20 Jahren

Aber: Moscas Ungleichung



$$X + Y \leq Z$$

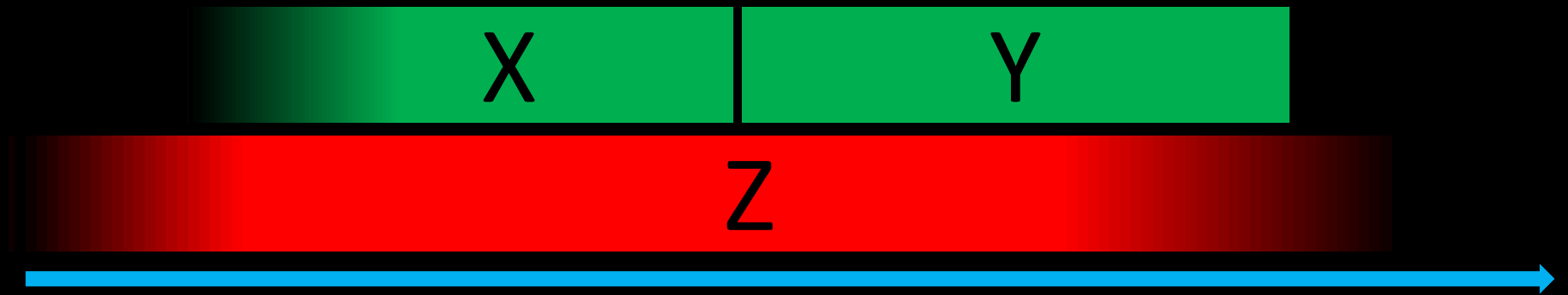
$$X + Y > Z$$

X: Zeit für eine Umstellung auf „quantenresistente“ Kryptoalgorithmen

Y: Zeit, die ein kryptographischer Schlüssel sicher bleiben muss

Z: Zeit, bis ein passender Quantencomputer gebaut wird

Aber: Moscas Ungleichung



$$X + Y \leq Z$$

$$X + Y > Z$$

X: Zeit für eine Umstellung auf „quantenresistente“ Kryptoalgorithmen

Y: Zeit, die ein kryptographischer Schlüssel sicher bleiben muss

Staatsgeheimnisse u. dgl., Firmware-Update-Signaturen, … *Root-CAs*

Z: Zeit, bis ein passender Quantencomputer gebaut wird

Erster Ansatz

Ah,
der Plan

Neue PKI mit PQC-Signaturen und PQC-Schlüsseln

D

Oh,
aber…

Können alle Systeme PQC-Algorithmen verarbeiten?

Zweiter Ansatz

Ah,
der Plan

Zwei PKIs betreiben:

- Legacy-PKI
- PQC-PKI

D

Oh,
aber…

Wer bekommt dann von welcher ein Zertifikat?

Zweiter Ansatz

Einfach

- Legacy-Anwendungen und -Komponenten:

Zertifikate der Legacy-PKI

Einfach

- Neue Anwendungen und Komponenten:

Zertifikate der PQC-PKI

- Kniffliger
- Anwendungen mit Legacy-Komponenten u. neuen Komponenten

?

Zweiter Ansatz: PKI-Anwendungen im Übergang

Ah,
der Plan

Legacy-Systeme bekommen je ein Legacy-Zertifikat

Neue Systeme bekommen zwei Zertifikate, Legacy und PQC

D

Oh,
aber…

Welches ihrer zwei Zertifikate nutzen neue Systeme wann?

Beispiel Webserver mit Legacy- und PQC-Serverzertifikat

1. Will der Browser TLS 1.2 oder älter?
   → Legacy-Serverzertifikat an den Browser schicken (falls überhaupt)
2. Bei TLS 1.3 steht im ClientHello, welche Algorithmen der Browser unterstützt.
   Steht im ClientHello unser PQC-Algorithmus?
   → PQC-Serverzertifikat an den Browser schicken
3. Sonst:
   → Legacy-Serverzertifikat an den Browser schicken
4. Bei Client-Authentifikation: entsprechend dem Serverzertifikat

Zweiter Ansatz: Auswahl Legacy- oder PQC-Zertifikat

Ah,
der Plan

Auswahl treffen ist bei TLS also einfach

Oh,
aber…

Aber was ist mit S/MIME, Signaturen, VPN/IKEv2, PKInit usw.?

Problemverlagerung:
Auswahl Legacy/PQC der Gegenseite überlassen

- Es wird ein Zertifikat an die Gegenstelle geschickt
- Legacy-Komponenten behandeln es als Legacy-Zertifikat
- Neue Komponenten können daraus ein PQC-Zertifikat „bauen“ und nutzen

Kombination Legacy/PQC über nicht-kritische Erweiterungen

Interessiert mich nicht

Legacy-Komponenten:

Ich kenne das nicht,

ich sehe das nicht,

das ist ein Legacy-Zertifikat

Das mag ich

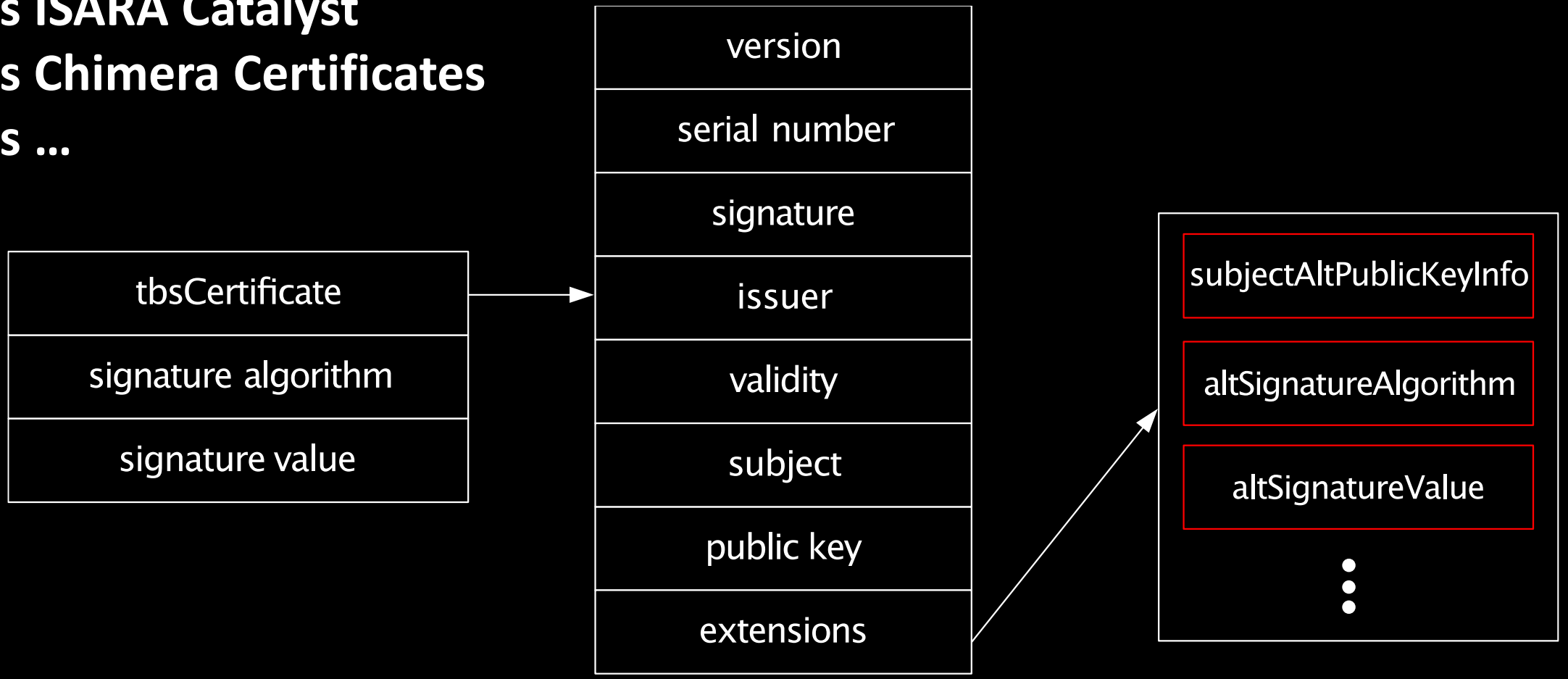
Neue Komponenten:

Ah, da ist die Information, mit der ich das Zertifikat „umbauen“ kann,

das ist ein PQC-Zertifikat

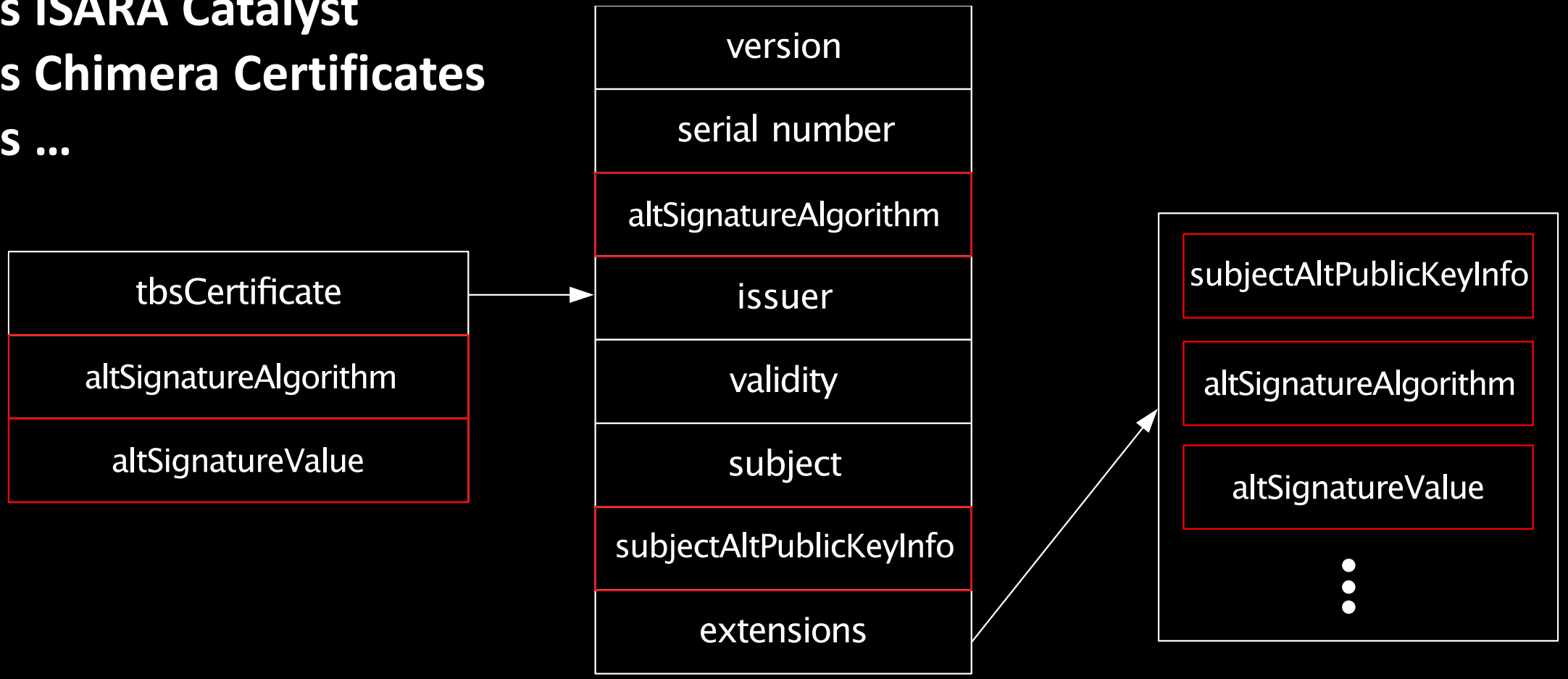
Offiziell bei X.509: Alternative Signaturen/Schlüssel

X.509-2019
alias ISARA Catalyst
alias Chimera Certificates
alias …

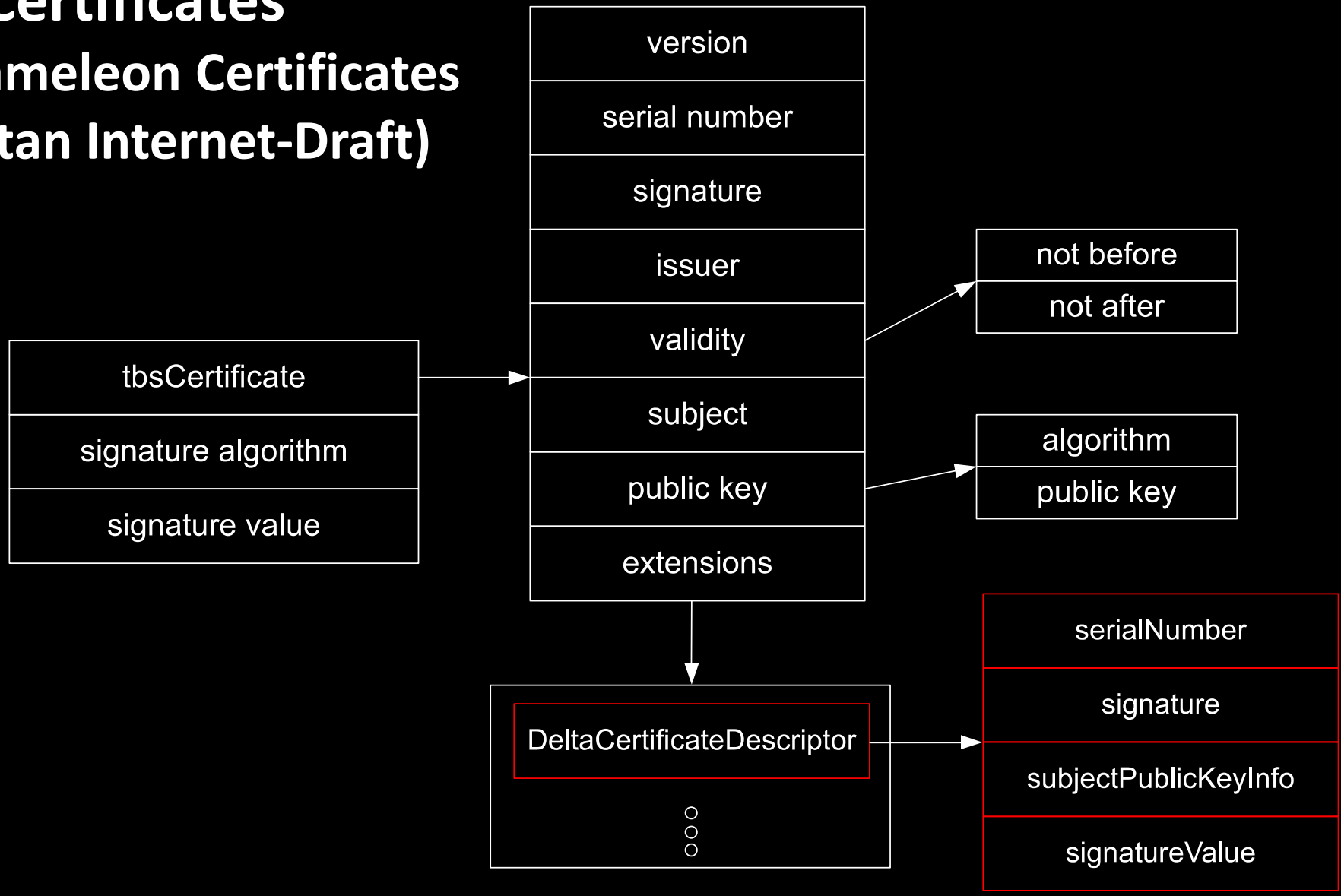


Offiziell bei X.509: Alternative Signaturen/Schlüssel

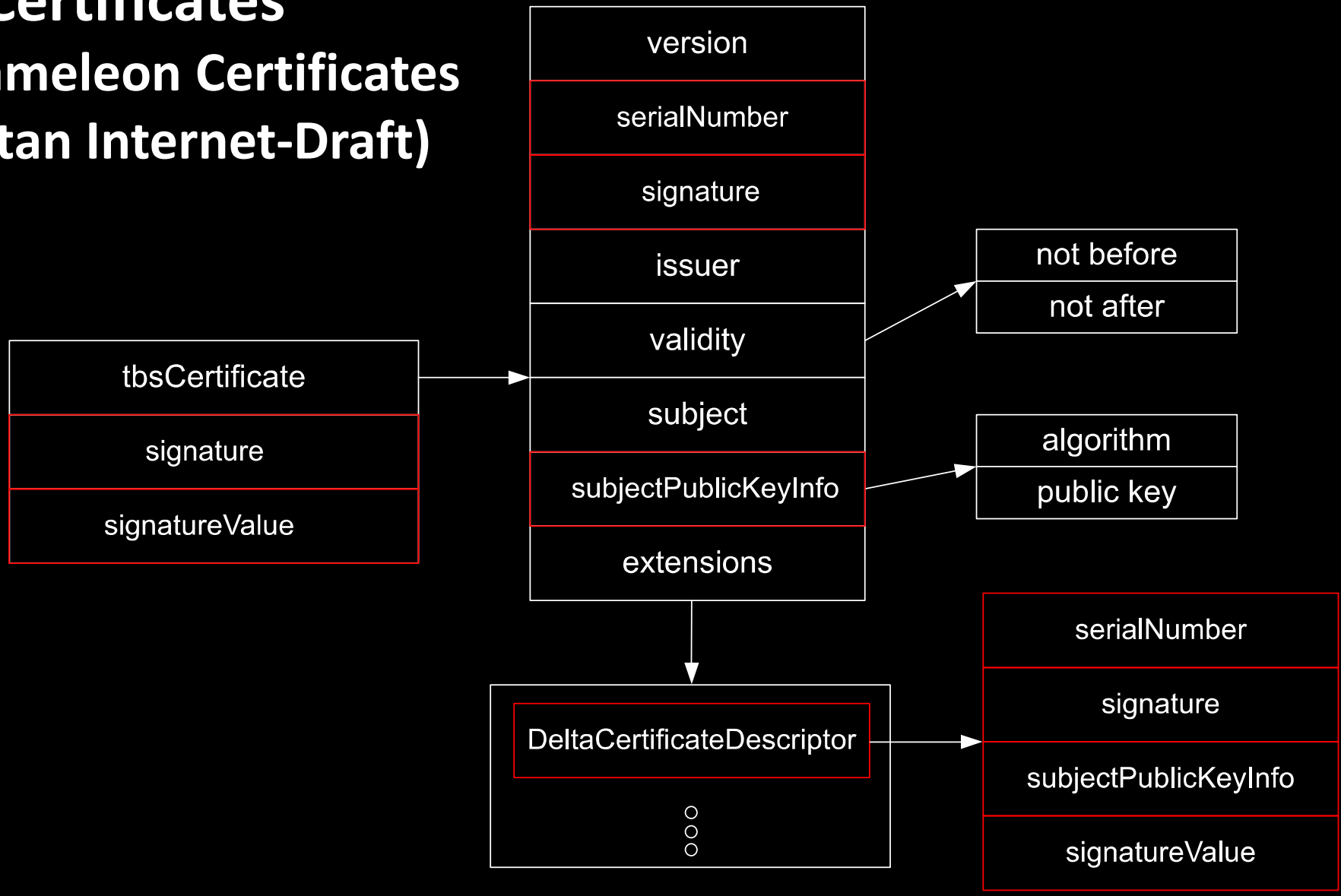
X.509-2019
alias ISARA Catalyst
alias Chimera Certificates
alias …



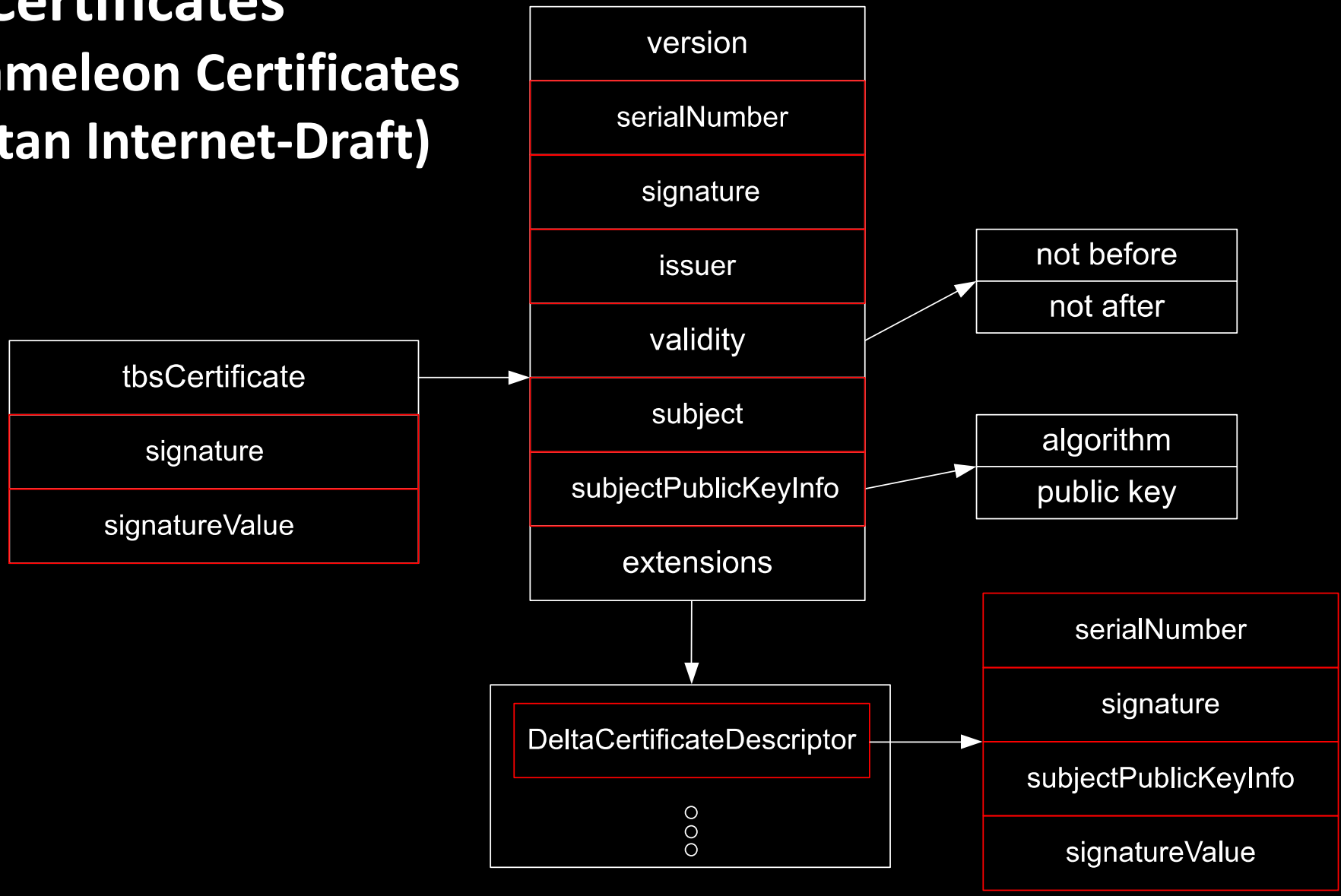
Paired Certificates
alias Chameleon Certificates
(momentan Internet-Draft)



Paired Certificates
alias Chameleon Certificates
(momentan Internet-Draft)



Paired Certificates
alias Chameleon Certificates
(momentan Internet-Draft)



„Wir sind dran… sowas von dran… “

- PQC-Basisalgorithmen standardisiert
- Standardisierung der Anwendungs-Formate und -Protokolle hat begonnen
  - IETF will „Toolbox“ für eine weniger schreckliche PKI-Migration standardisieren
  - … aber die Auswahl der Werkzeuge aus der Toolbox den Herstellern/Anwendern überlassen
- Erste Implementierungen
  - EJBCA Community kann Zertifikate mit ML-DSA-Schlüsseln signieren
  - OpenSSL (Provider) und BouncyCastle implementieren Algorithmen und X.509-Erweiterungen
  - Neueste Firmware mancher HSMs können einige PQC-Algorithmen (eher langsam und wenige Schüssel wg. Speicherplatz)
  - …

Beispiel: Zusammengesetzte Signaturen ML-DSA mit RSA

Bouncy Castle – Signaturalgorithmus

```
SEQUENCE {
  OBJECT IDENTIFIER ’ 1 3 6 1 4 1 …’
    SEQUENCE {
     SEQUENCE {
       OBJECT IDENTIFIER ’1 2 …’
       }
       SEQUENCE {
       OBJECT IDENTIFIER ’1 3 …’
       }
    }
}
```

OpenSSL – Signaturalgorithmus

```
SEQUENCE {
  OBJECT IDENTIFIER ’1 3 9999 2 7 2’
}
```

Beispiel: Zusammengesetzte Signaturen ML-DSA mit RSA

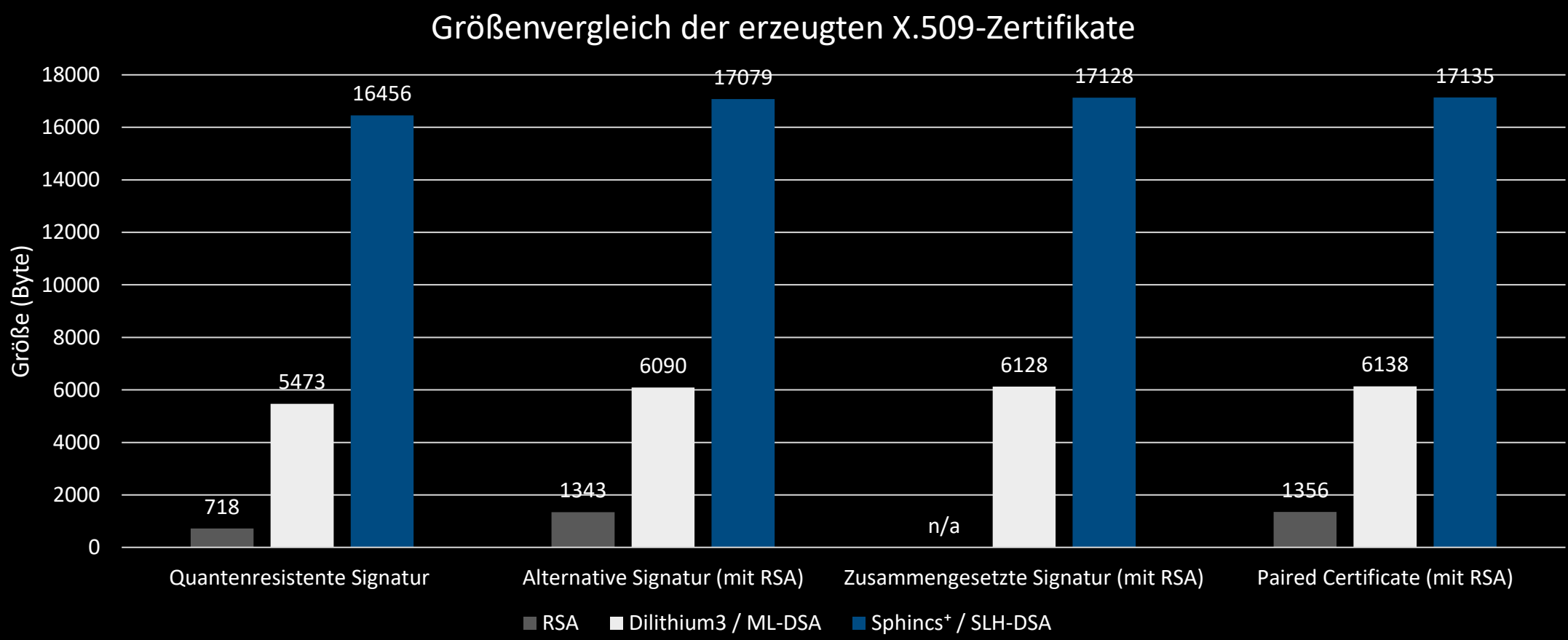
Bouncy Castle – Signatur

```
BIT STRING, encapsulates {
 SEQUENCE {
  BIT STRING
   6B 2C 78 0B 5C 36 11 96 50 8C 04
   7F 64 5F 8B 14 B9 A7 05 84 2C 02
   6D 7B 23 FD 95 D6 B3 06 6E 2E
   [ Another 224 bytes skipped ]
  BIT STRING
   0D B8 A3 CE C4 E2 3E 45 61 13 D5
   86 B2 6B 5C 5D 19 B4 2A A0 30 A7
   7C 04 AF 0D A7 81 CD A8 2F 06
   [ Another 3277 bytes skipped ]
 }
}
```

OpenSSL – Signatur

```
BIT STRING
 00 00 01 80 A1 5D 22 40 24 DA 1D
 DE E8 C3 06 91 8F C3 4F A8 70 B7
 A8 43 2B C7 67 09 AB B1 CE 65 D3
            […]
```

Weiteres Thema: Größe der Zertifikate



Was ist in einer PKI noch betroffen?

- CRLs (sind bei X.509 Alternative Signatures oder Paired Certificate mit betrachtet)
- Die Übertragung von Schlüsseln in PKCS#10 CSR und deren Proof-of-Possession-Signatur
- Die Signatur von OCSP-Responses und optional OCSP-Requests
- Die Verwendung von Public-Key-Hashes als Identifier, insbesondere in Key-Identifier-Erweiterungen und OCSP-Requests
- CRMF als alternatives Antragsformat zu PKCS#10-CSR im CMP-Protokoll
- Signaturen in Zertifikats-Management-Protokollen wie CMC, CMP, SCEP oder ACME
- Signaturen, welche die für viele öffentlich gültige Zertifikate geforderte, korrekte Veröffentlichung in Certificate-Transparency (CT) Logs bestätigen
- Die fehlende Möglichkeit, mit Public-Keys von quantenresistenten reinen Key-Encapsulation-Mechanismen eine Proof-of-Possession-Signatur (zum Nachweis des Besitzes des zugehörigen Private-Keys) für PKCS#10-CSR oder CRMF zu erstellen

Aber die Uhr von Moscas Ungleichung tickt…

NSA: Commercial National Security Algorithm Suite 2.0 = PQC-Algorithmen

„The Commercial National Security Algorithm Suite 2.0 and Quantum Computing FAQ“, Stand April 2024

mode. NSA's current view on timing is as follows:

- **Software- and firmware-signing:** begin transitioning immediately, support and prefer CNSA 2.0 by 2025 where available, *exclusively* use CNSA 2.0 by 2030.
- **Web browsers/servers and cloud services**: support and prefer CNSA 2.0 by 2025, *exclusively*[8] use CNSA 2.0 by 2033.
- **Traditional networking equipment (e.g., virtual private networks, routers):** support and prefer CNSA 2.0 by 2026, *exclusively* use CNSA 2.0 by 2030.
- **Operating systems**: support and prefer CNSA 2.0 by 2027, *exclusively* use CNSA 2.0 by 2033.
- **Niche equipment (e.g., constrained devices, large public-key infrastructure systems)**: support and prefer CNSA 2.0 by 2030, *exclusively* use CNSA 2.0 by 2033.
- **Custom applications and legacy equipment**: update or replace by 2033.

Was tun?

Grundsätzlich

- Nicht ganz unähnlich zum Jahr-2000-Problem - „Y2Q“ ☺
  - Nur der Stichtag steht noch nicht so genau fest
- Situation beobachten
  - U. a. der CNSA-Fahrplan bringt Hersteller unter Druck
  - Hersteller bringen Standardisierungsgremien unter Druck
- Vermeidbare größere PKI-Änderungen bis ca. 2028/2030 zurückstellen, dann entscheiden
  - Neue PQC-PKI
  - Zwei PKIs
  - Eine PKI, die z. B. Paired-Certificates ausstellt
  - …

Was hilft dabei

- Bestmögliche Übersicht über Zertifikats-nutzende Anwendungen und Schlüssel
  - In welchen Anwendungen werden die Zertifikate genutzt?
  - Sind das „eher gutartige“ wie z. B. TLS oder „komplizierte“ wie z. B. Codesignaturen?
  - Welche Anwendungsprodukte und Plattformen werden eingesetzt?
    - In welchen Versionen?
    - Mit welchen Krypto-Libraries bzw. welchem Funktionsumfang?
  - Welche Schlüssel und Schlüssellängen sind im Einsatz?

→ Crypto Bill Of Materials – CBOM, ähnlich SBOM

- Wenn machbar: Einflussnahme auf die Beschaffung
  - „Ausreichende“ PQC-Fähigkeit aus Auswahlkritierium bei einer Neubeschaffung von Systemen und Komponenten
  - Knifflig: Was ist dabei „ausreichend“?


secorvo
security consulting
Ettlinger Str. 12-14
76137 Karlsruhe
Telefon +49 721 255171-0
Telefax +49 721 255171-100
info@secorvo.de
www.secorvo.de