TEMET
end-to-end IT security

X.509v4
Quantum-Safe Certificates

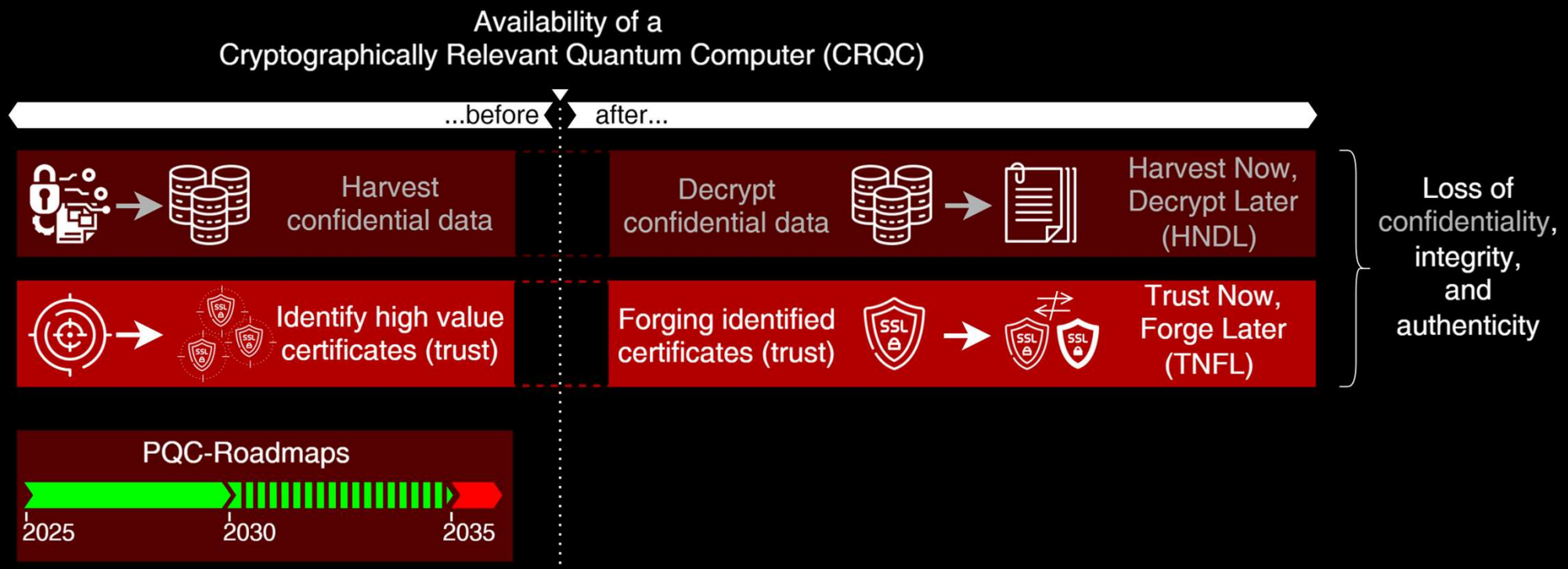
...do we need an update to the current X.509v3?

André Clerc, TEMET AG | 12.03.2026, Zurich

TEMET
end-to-end IT security

Potential Risk for Traditional Certificates

Potential Risk



TEMET
end-to-end IT security

Problem Statement – Digital Signatures

1. Trust Now - Forge Later (TNFL)
   Does a digital signature or ID still need to be valid in 7 years?
2. PQC-Agnostic Archiving (PAA)
   How do I prove in 2032 that a signature was valid in 2026?
3. Cryptanalytic Maturity Gap (CMG)
   Trust gap between classical and Post-Quantum Cryptography (Algorithms)
4. Resource Constraints (RC)
   Significantly larger signatures and certificate chains (up to a factor of 10–50; 10-15 packages)
5. Migration Deadline (MD)
   Compliance or regulatory cut-off for RSA/ECC algorithms
6. Backward Compatibility (BC)
   Is it necessary for my application/service to handle classic and PQC methods?

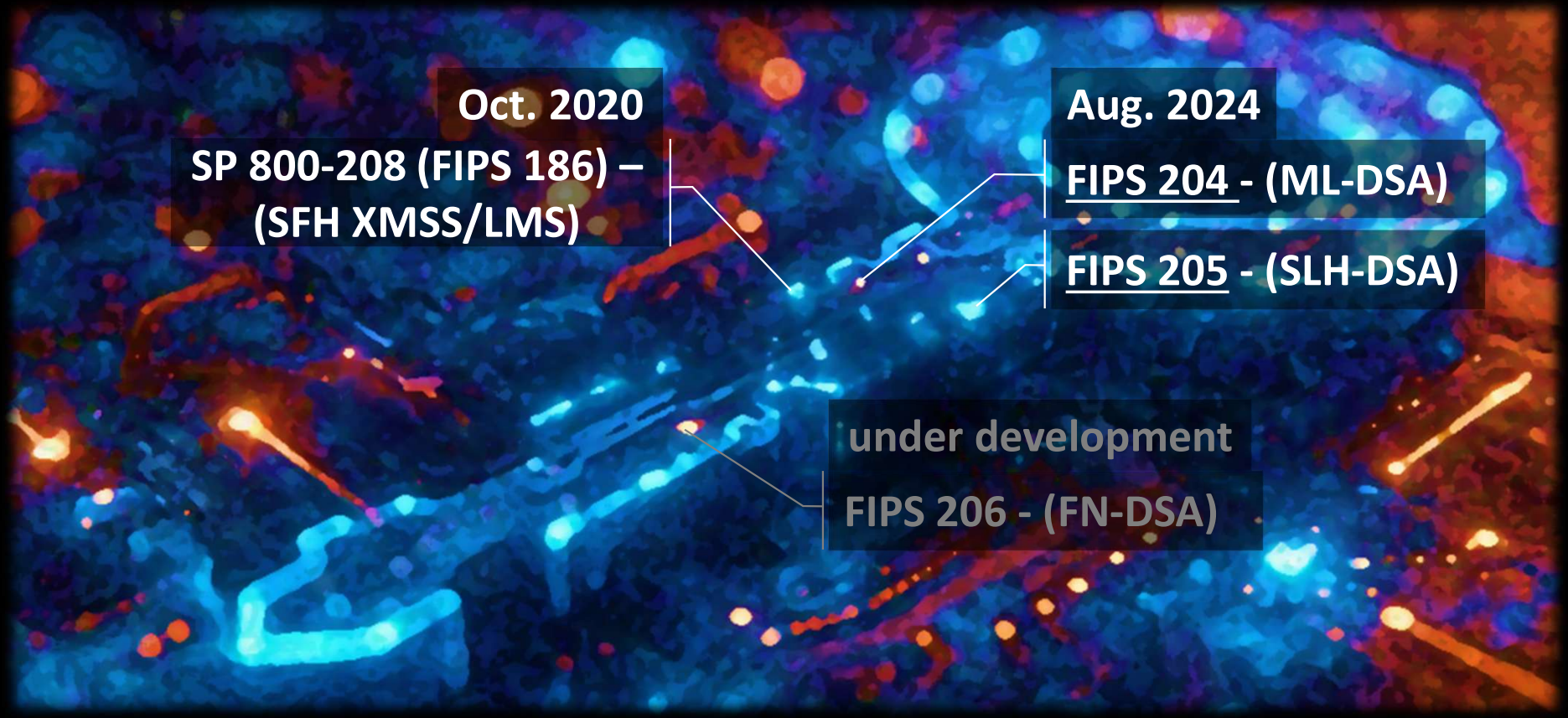
Vulnerable Data - Areas of Action

1. Identity & Access
   User/Device Auth, IoT, mTLS, Mobile ID
2. Documents & Legal
   Signed Contracts, Tax-Documents EPD, E-Prescriptions
3. Critical Infrastructure & Telemetry
   Sensors & Actuators, OTA-Updates, Smart Meters, Vehicle-to-Everything (V2X)
4. Life-Critical Systems (IoMT)
   Pacemakers, Insulin Pumps, or Neurostimulators
5. Trust Anchor & Third Party (Supply Chain) Integrity
   - **PKI**: CAs, RA, VA (CRLs/OCSP), Trust Stores, HSMs, TPM, Smart Cards
   - **Software & Data**: OS Packages, Firmware Updates, Code Signing, S/CBOM
   - **Integrity Persistence**: Trusted Timestamps, Evidence Records (ERS)
   - **Security-Feeds**: Virus Signatures, Blocklists, Configuration-Templates (IaC)

TEMET
end-to-end IT security

Standardised PQC Signing Algorithms

Available PQC-Standards



TEMET
end-to-end IT security

X.509v3 Background

X.509v3 Background

- Version 3 of X.509 was standardized in 1996
  (as part of ITU-T Recommendation X.509 | ISO/IEC 9594-8)
  - Syntax-Framework (ASN.1-Structur)
- **Goal**: Create a flexible framework so that the basic format of the certificate no longer needs to be changed
  - Core data format (external ASN.1 structure) remains unchanged
- Evolution without structural change
  - Adjustments to **semantics**, **interoperability**, and **policy**
    (PKIX-Profil - Public Key Infrastructure X.509; IETF, CA/B Forum)
    - 1999 → RFC 2459
    - 2002 → RFC 3280
    - 2008 → RFC 5280

X.509v3 Background

- X.509 Profiles Updates (see RFC Editor)
  - PQC conversion → IETF working group **LAMPS**
    (Limited Additional Mechanisms for PKI and S/MIME)
  - RFC 9935 (Mar. 2026) → Algorithm Identifiers **ML-KEM**
  - RFC 9925 (Feb. 2026) → Algorithm Identifiers **Unsigned Certificate**
  - RFC 9909 (Dec. 2025) → Algorithm Identifiers **SLH-DSA**
  - RFC 9881 (Oct. 2025) → Algorithm Identifiers **ML-DSA**
  - RFC 9882 (Oct. 2025) → **ML-DSA** Signature for CMS
  - RFC 9629 (Aug. 2024) → **KEM** in CMS
  - RFC 9618 (Aug. 2024) → Updates to X.509 Policy Validation
  - RFC 9608 (Jun. 2024) → **No Revocation Available** for X.509 Certificates

TEMET
end-to-end IT security

Post-Quantum X.509v3 Certificates

PQC Integration in X.509v3

1. Pure PQC Certificates
   Direct implementation PQC without any legacy cryptographic fallback

2. Merkle Tree Certificates (MTC)
   Hash-based structures to aggregate certificates to reduce bandwidth overhead (PQC chains)

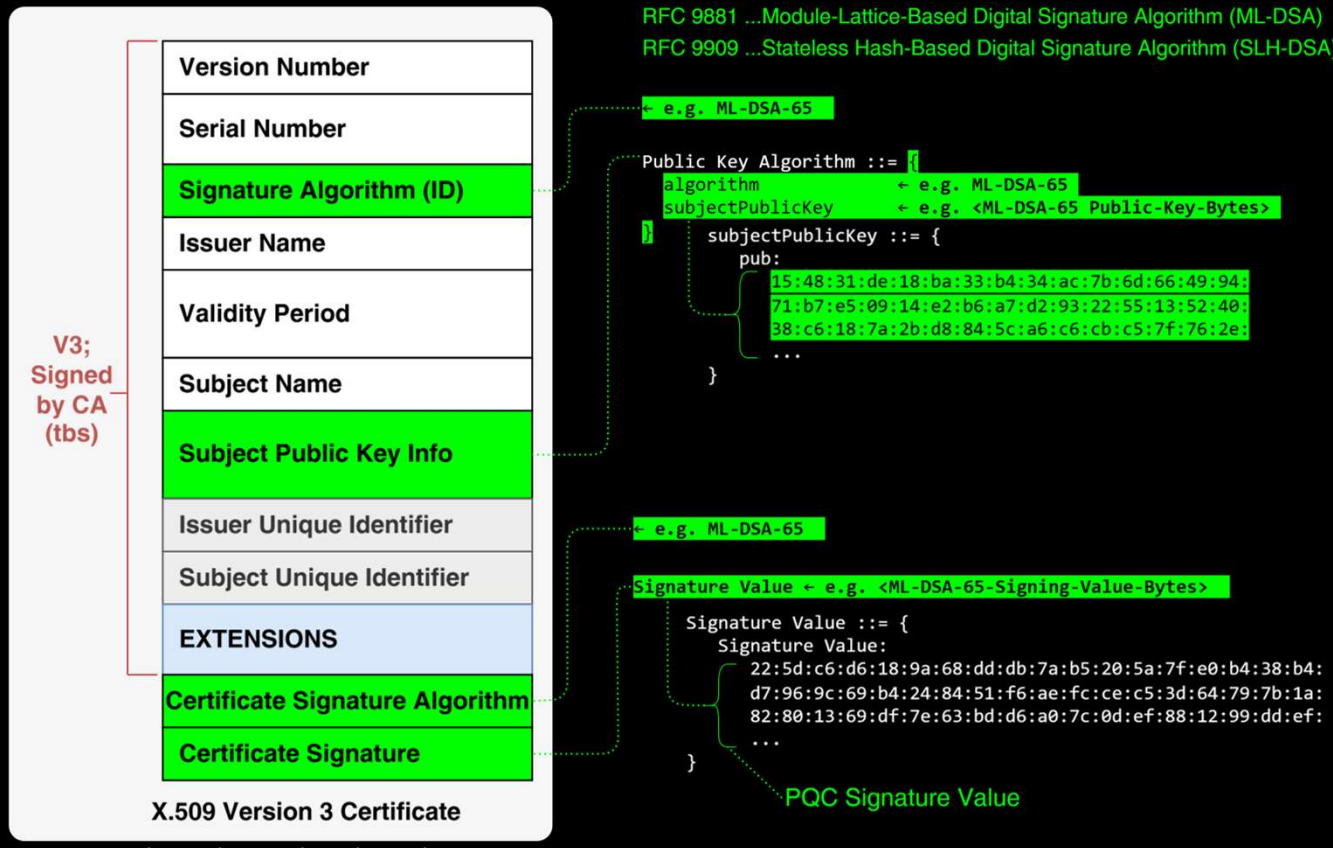
3. Chimera/Catalyst Certificates/MAB (ASA)
   Hybrid method where a traditional certificate is augmented with a secondary PQC signature to provide backward compatibility

4. Chameleon Certificates
   Evolution of the hybrid approach that allows "morphing" a classical certificate into a PQC-compliant

5. Composite Certificates
   Both classical & PQC keys & signatures are tightly bound into a single, inseparable data structure

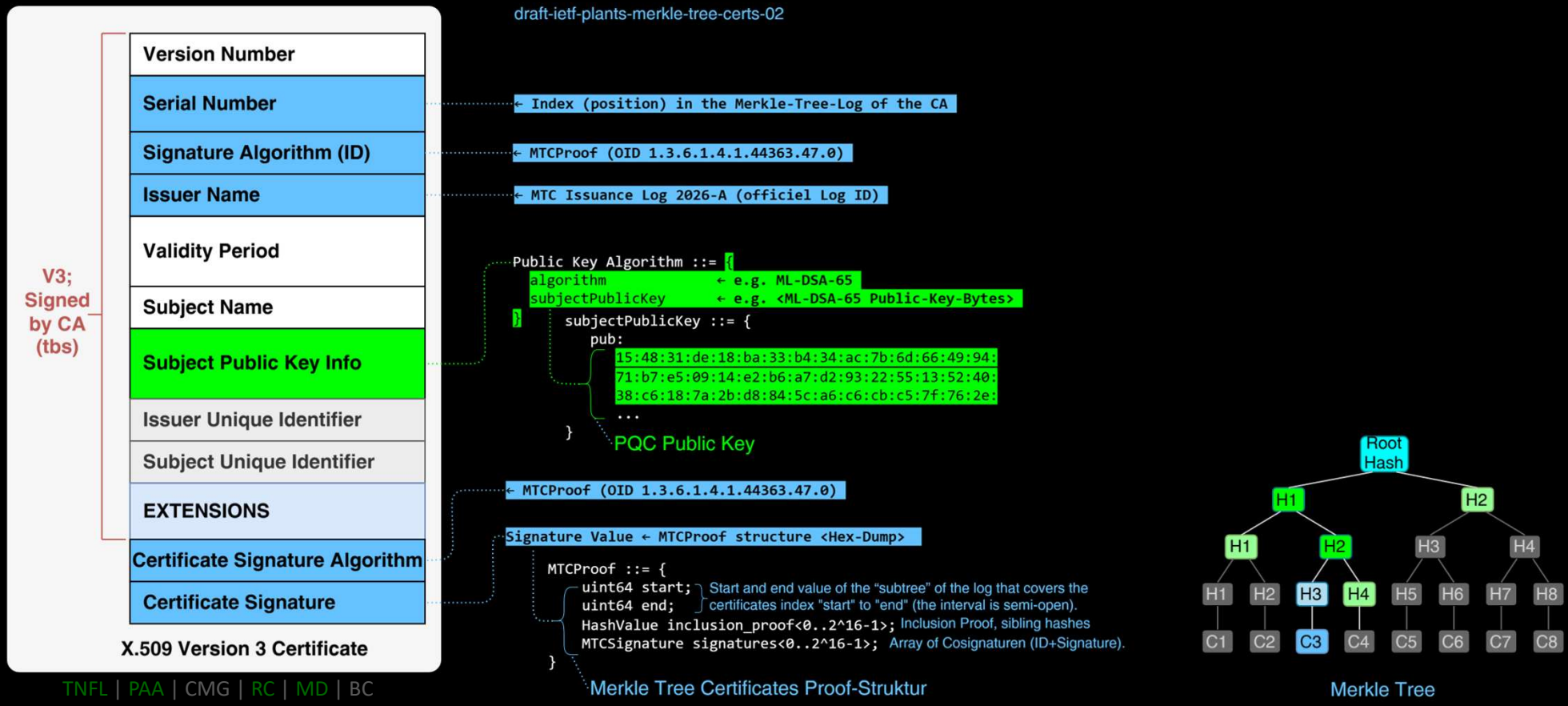
6. KEM-Based Certificates
   Changes the logic of a certificate from “I sign something” to “I encrypt something for you”

X.509v3 – Pure PQC Certificates



TNFL | PAA | CMG | RC | MD | BC

X.509v3 – Merkle Tree Certificates (MTC)



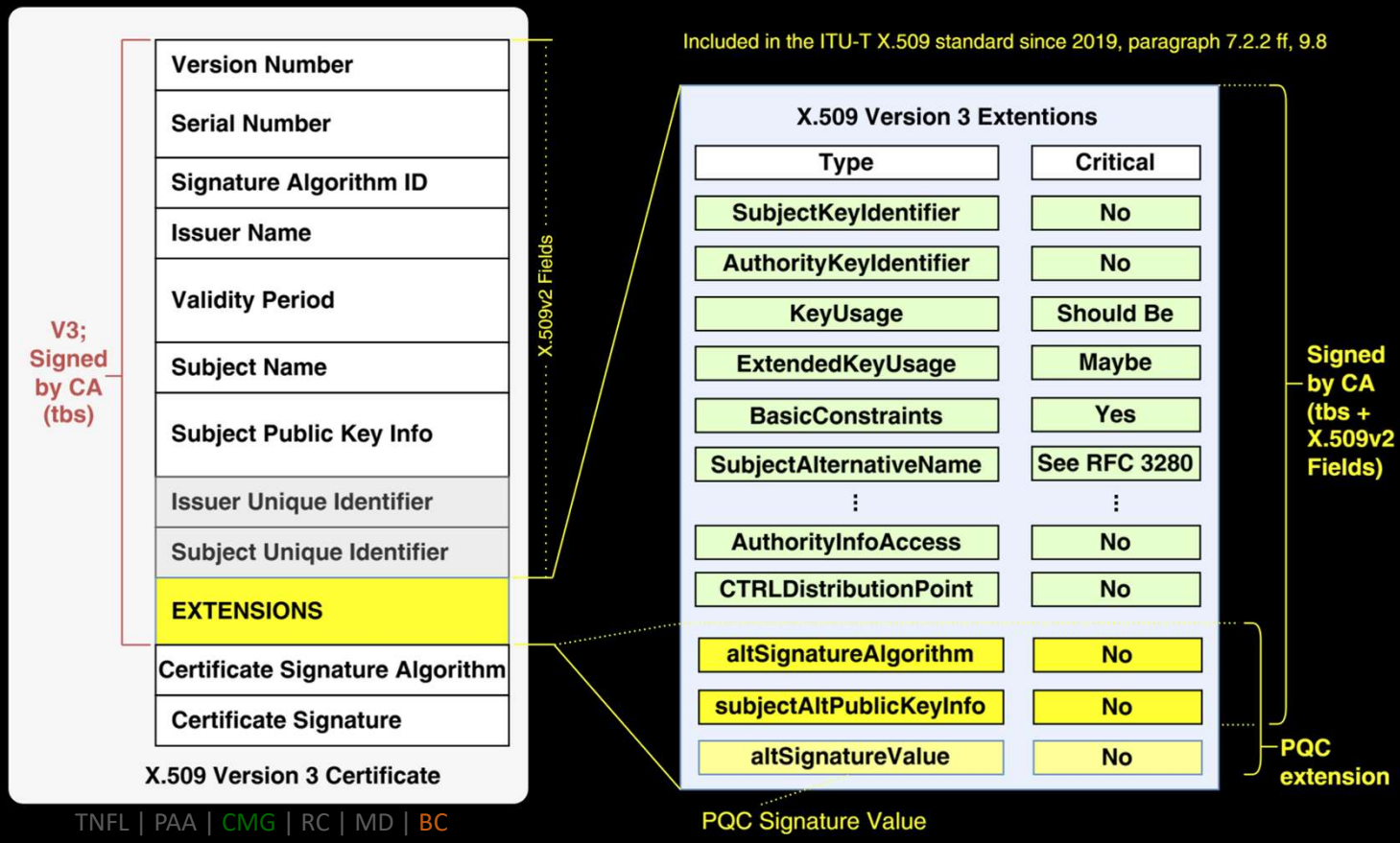
TNFL | PAA | CMG | RC | MD | BC

TEMET
end-to-end IT security

Hybrid Certificates

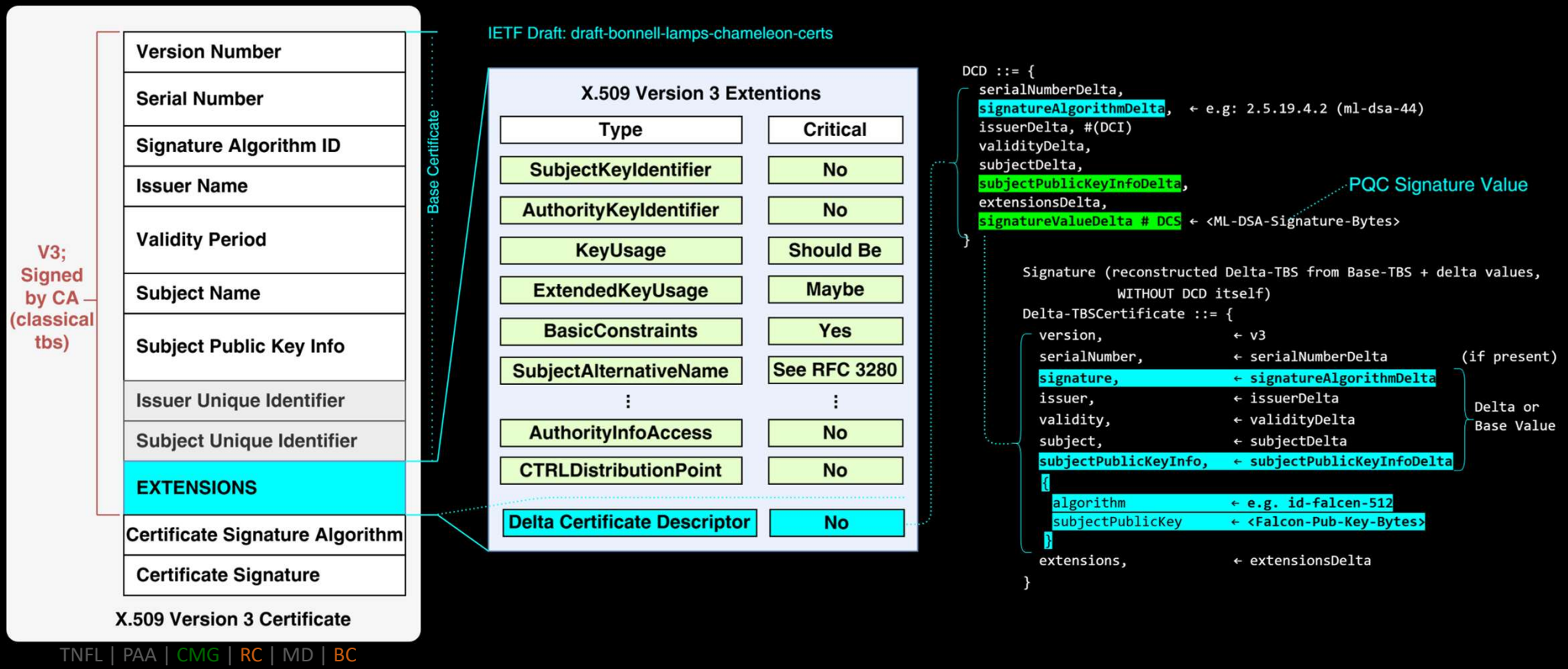
TEMET
end-to-end IT security

X.509v3 – Chimera/Catalyst Certificates (ASA)



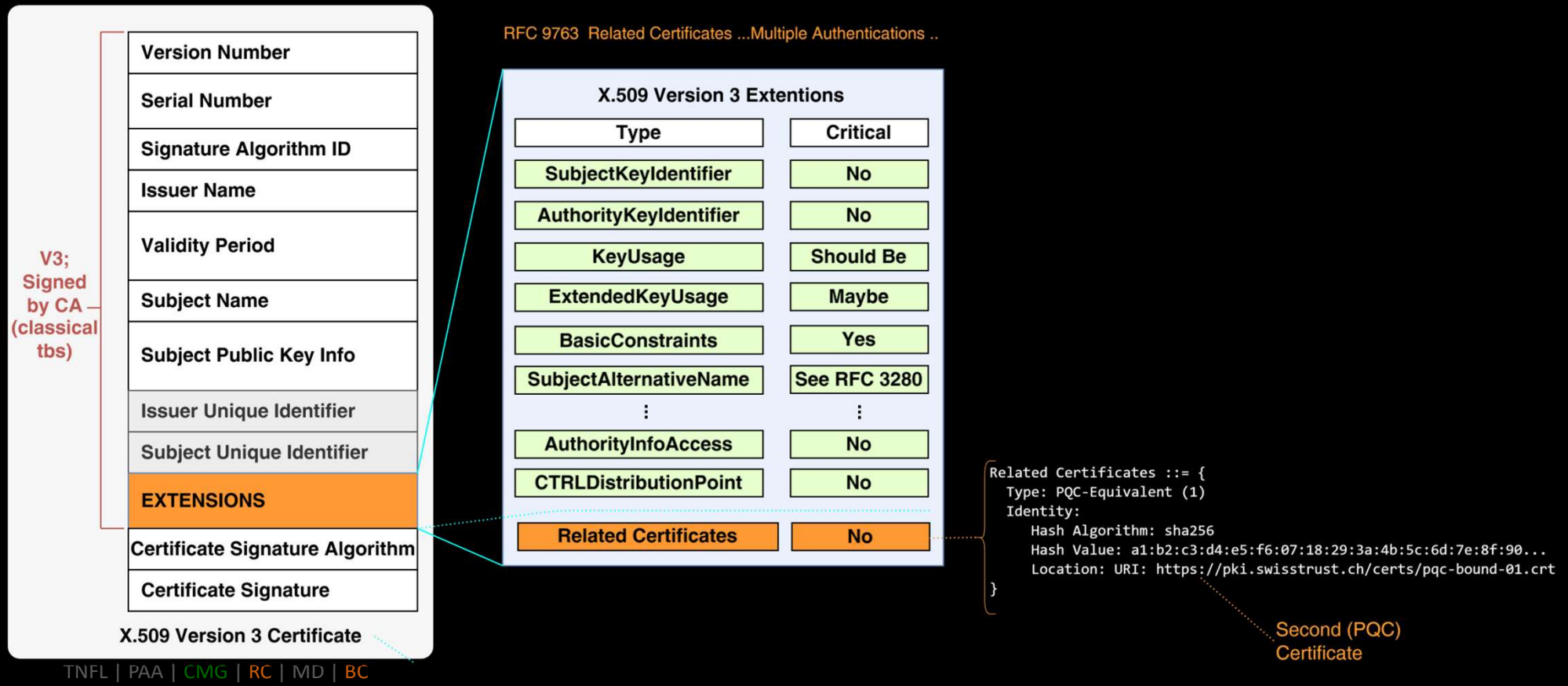
TNFL | PAA | CMG | RC | MD | BC

X.509v3 – Chameleon Certificates



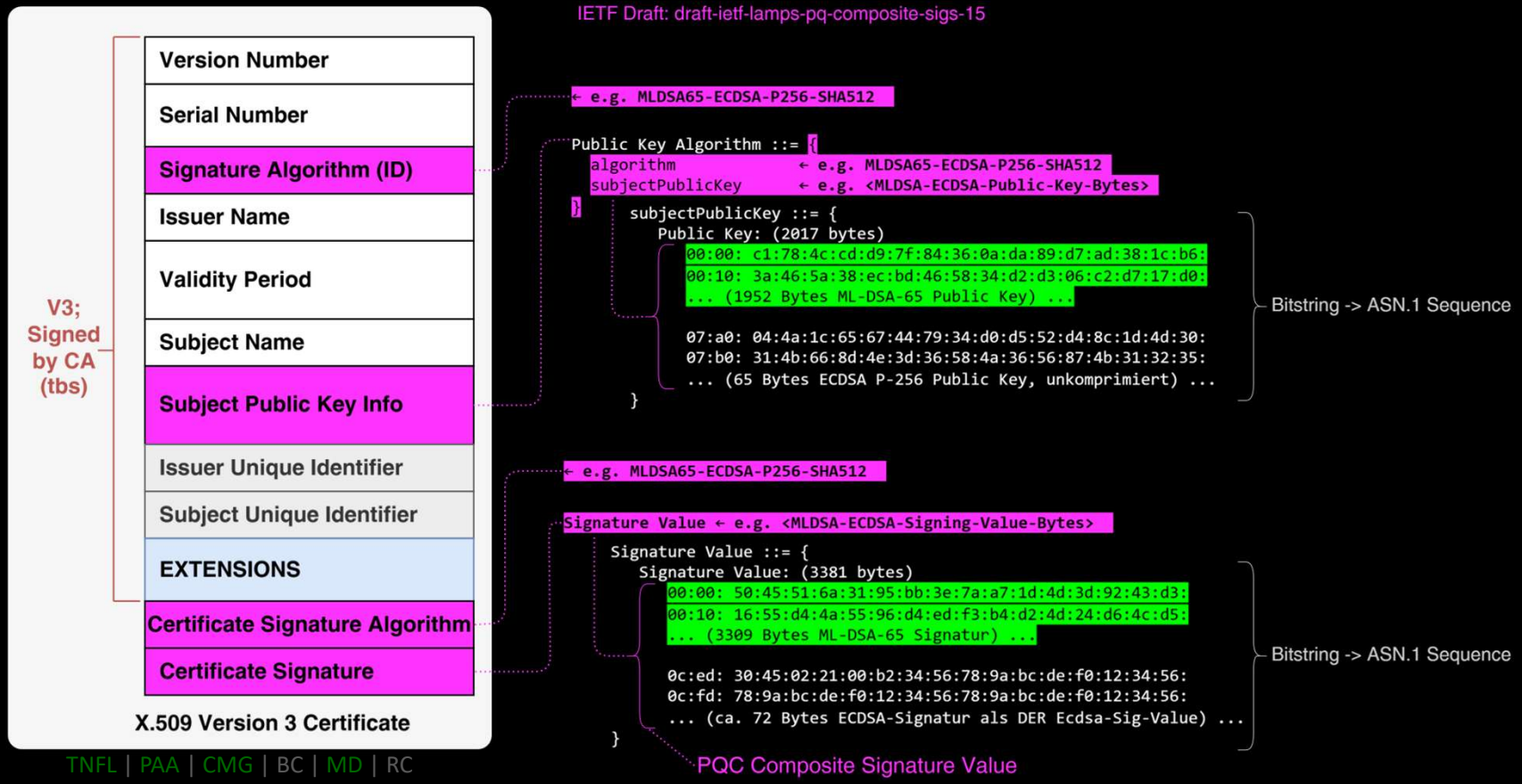
TNFL | PAA | CMG | RC | MD | BC

X.509v3 – Multi-Auth Binding Certificates



TNFL | PAA | CMG | RC | MD | BC

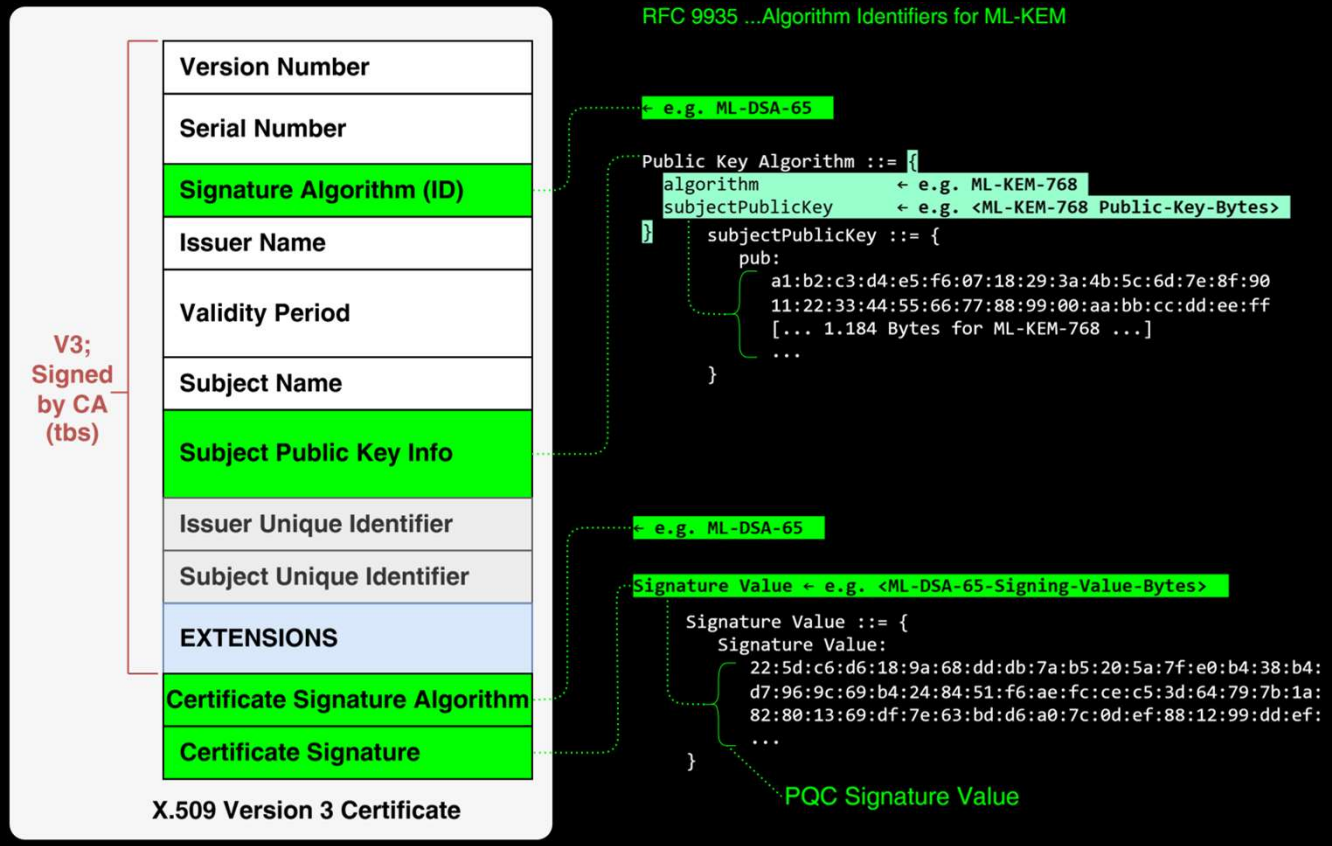
X.509v3 – Composite Certificates



TNFL | PAA | CMG | BC | MD | RC

KEM-Based Certificate

X.509v3 – KEM-Based Certificates



TNFL | PAA | CMG | RC | MD | BC

PQC Certificate Integrations

Technologie	Pure PQC	Composite	Chimera/Chameleon/ Multi-Auth Binding	Merkle Tree Certs	KEM-Certs
BoringSSL	Yes	No	No	Tests are runing	No
OpenSSL 3.5+	Yes	Yes (OQS)	No	Draft	No
WolfSSL	Yes (FIPS-Focus)	No	Yes (Chimera)	Draft	No
Go (crypto)	Yes	Yes (CIRCL)	No	In Progress	No
Java, Kotlin	Yes (BC)	Yes (BC)	Yes (BC)	No	No
C# (.NET)	Yes	Yes	No	No	No
Rust (rustls)	Yes	Yes	No	No	No

X.509v3 PQC – Conclusion

- **Pure PQC Certificates**
  Vulnerable to algorithmic and implementation weaknesses.
- **Chimera & Chameleon Certificates**
  Suggests PQC security, but this can often be undermined by downgrade options. → *Backward compatibility*
- **Composite Certificates**
  These certificates address the TNFL, PAC-AA, MG and MD problem statements.
- **Merkle Tree Certificates (MTC)**
  In combination with the composite approach, these certificates have the potential to become a key technology.
- **KEM-Based Certificates**
  Can only be used for authentication

TEMET
end-to-end IT security

Do we need an X.509v4?

X.509v3 Issues

1. Version Number
   TLS stacks, web servers, & browsers expect certificate versions 1, 2, or 3
2. Obsolete Fields
   We have certificate fields that are now obsolete or have never been utilized
3. Missing Fields
   Important fields are missing in modern digitisation
4. Error-Prone ASN.1 Parser
   ASN.1 parsing can become very complex and error-prone
5. CRQC Relevance
   A CRQC was considered to be a theoretical prospect
6. Compatibility
   The need for backward compatibility can sometimes lead to very messy solutions

X.509v4 Wish List (Base Fields)

1. Multi signature and key support (mandatory)
   One signature and one key must belong to a PQC procedure
2. Assurance Level (AL)
   Trustworthiness should no longer be based on the interpretation of documents (CP/CPS); → AL 1-4
3. Key Attestation (Proof of Origin)
   Key generation in hardware should be verifiable (HSM, TPM, smart cards, etc.)
4. Issuer Hash
   Large PQC trust anchors could be indexed extremely quickly (local key-value database)
5. Usage Constraints
   The intended use should clearly defined (ephemeral flag, context binding {API}, etc.)
6. ASN.1/DER → CBOR o.a.f.
   CBOR is extremely compact, secure and easy to parse (IoT and satellite communication)

Why X.509v4? – More Than Just an Update

- Settle technological debts
  - **Legacy Cleanup**
    Eliminate outdated ASN.1 structures in favour of secure, modern encodings (e.g. CBOR)
  - **Parser Security**
    Reduction of the attack surface through simplified, deterministic logic.
- Native quantum security (PQC)
  - **Remove Hybrid Hacks**
    Direct support for hybrid key pairs without insecure bindings or stripping risks
  - **Efficiency**
    Optimised data formats for the significantly larger PQC signatures

Why X.509v4? – More Than Just an Update

- Take advantage of unavoidable adjustments
  - **Touching Every Stack**
    Since libraries and parsers for PQC need to be updated anyway, the effort involved would be minimal at this point.
  - **Securing the future**
    one-off modernisation instead of decades of patchwork extensions.
- Operational Agility
  - **Base Fields**
    Standardised fields for rapid algorithm exchange (crypto agility)
  - **Short-term certificates**
    Better support for short-term certificates without the burden of old CRLs and OCSP-Responses

Why X.509v4 won’t Become a Reality

- Technology - Legacy dependency
  Millions of IoT devices and old servers might not even be able to “read” v4 certificates in order to reject them
- Security - Parser risk
  New standards bring new bugs; the stability of global TLS traffic would be compromised
- Logistics - Global Synchronisation
  There is no central authority that could set the “switchover date” for the internet.
- Philosophy - Simplicity of v3
  Extensions allow for an “untidy but functional” solution (PQC hybrid), which reduces the burden

TEMET
end-to-end IT security

Can We Afford to Wait for Standards?

Why Waiting Is Not a Strategy

- In view of developments, **waiting is not a strategically** sensible option
- Panic-stricken actionism with an overnight changeover is not appropriate
  - **Start of a well-considered, step-by-step PQC transition**
- Sensitive areas requires urgent action

- **Reasons for acting now**
  - **Trust Now - Forge Later** (TNFL)
  - **Transition & Migration Cycles**
  - **Standards & Integrations are available or in progress**
  - **Growing Pressure of PQC Roadmaps** (2035)
    → Compliance & Liability
  - **Incomplete Crypto Landscape**
    → Asset Inventar
    → Vendor Dependency

¿ Questions ?