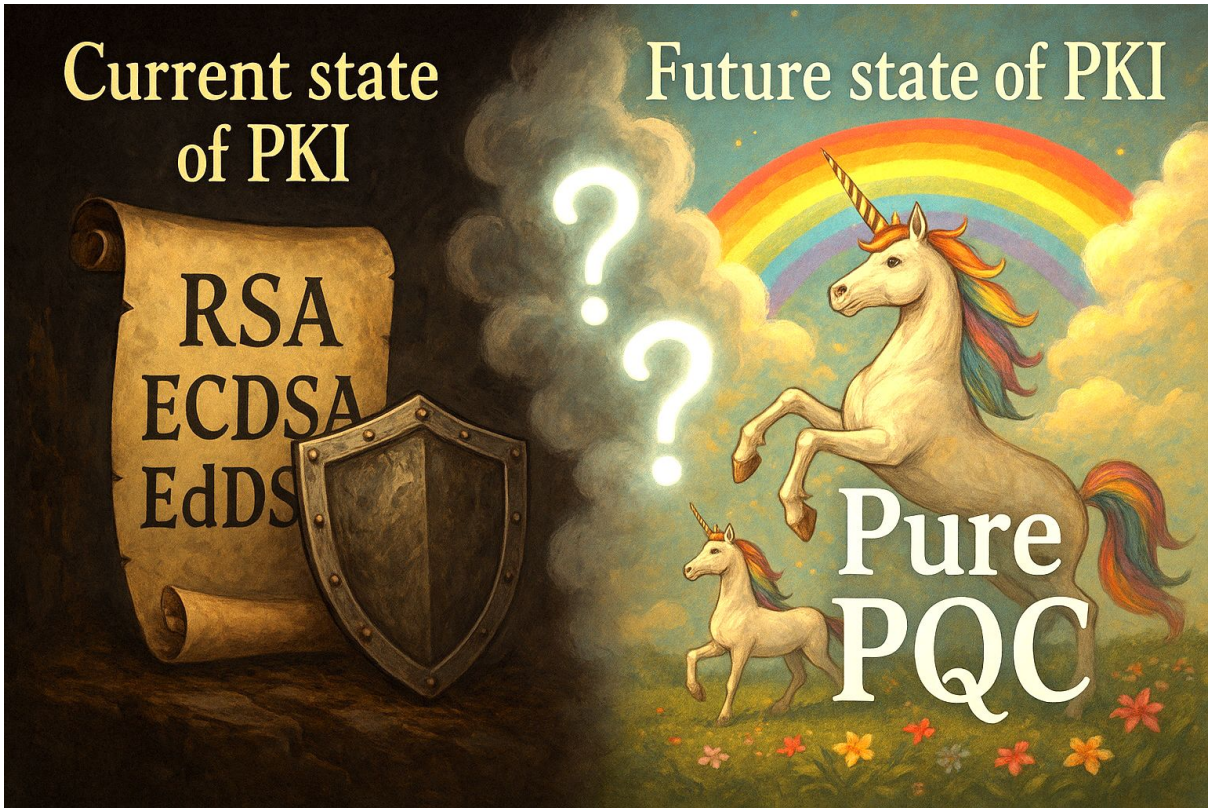
Dual Certificates in TLS 1.3

draft-yusef-tls-pqt-dual-certs-00

Rifaat Shekh-Yusef
Hannes Tschofenig
Mike Ounsworth
Yaron Sheffer
Tirumaleswar Reddy
Yaroslav Rosomakho

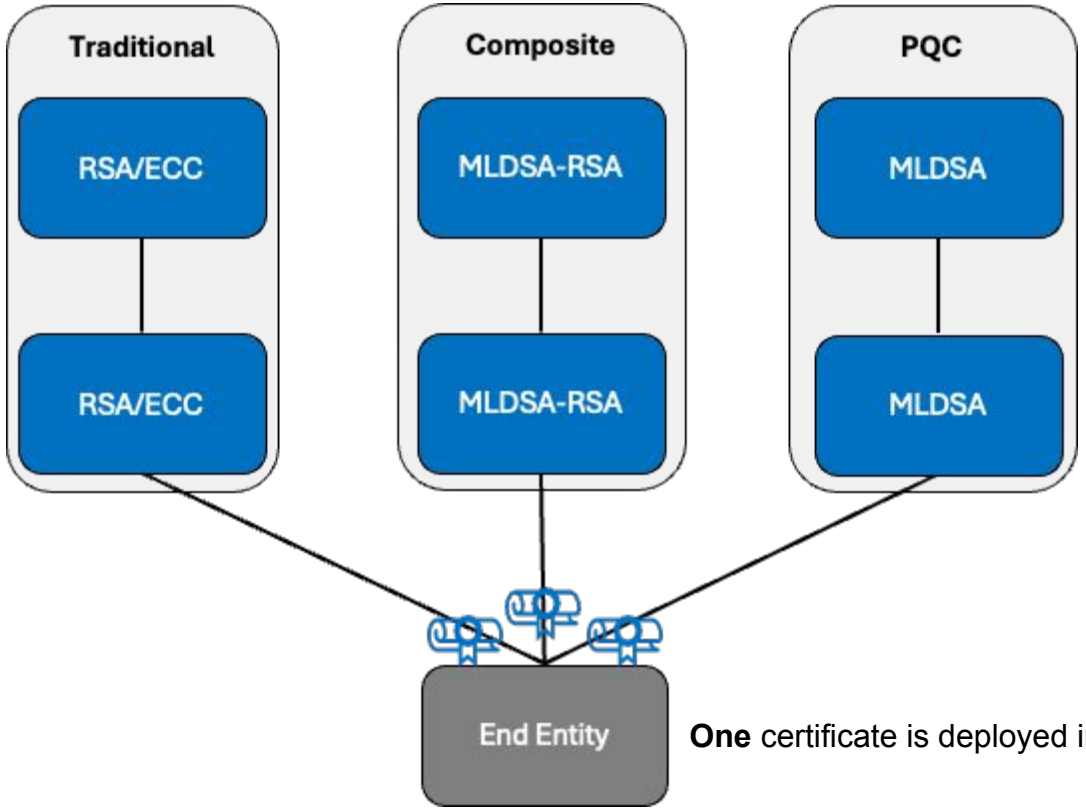
PQC PKI migration



Can we migrate directly from RSA/ECDSA/EdDSA to SLH-DSA/ML-DSA?

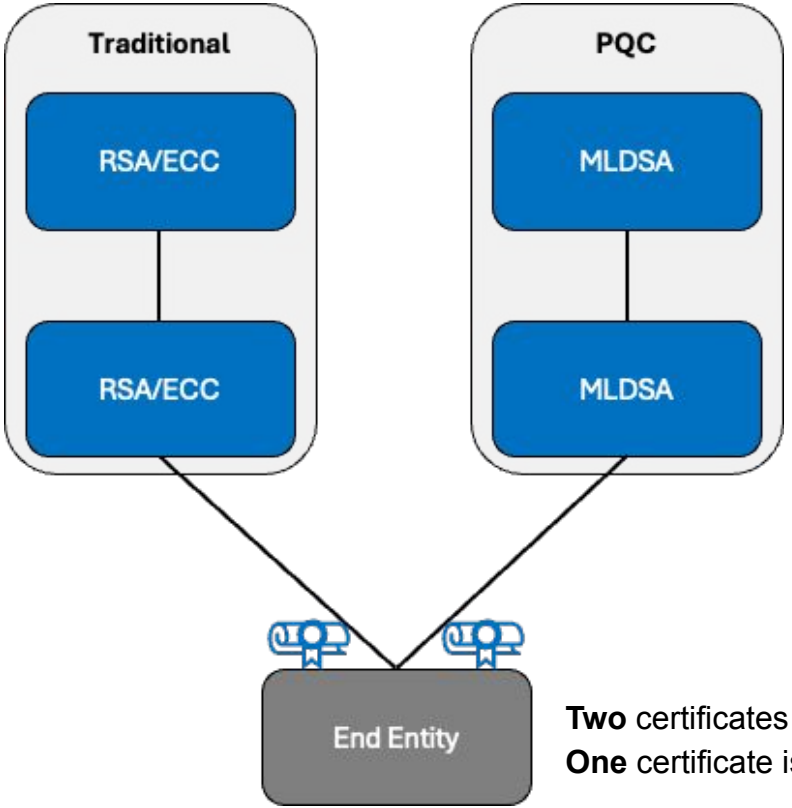
- There are concerns about security of ML-DSA
- German BSI TR-02102-1 section 5.3.4: *This Technical Guideline recommends the use of a quantum-safe signature scheme only in combination with a classic signature scheme*

Hybrid/Composite PKI



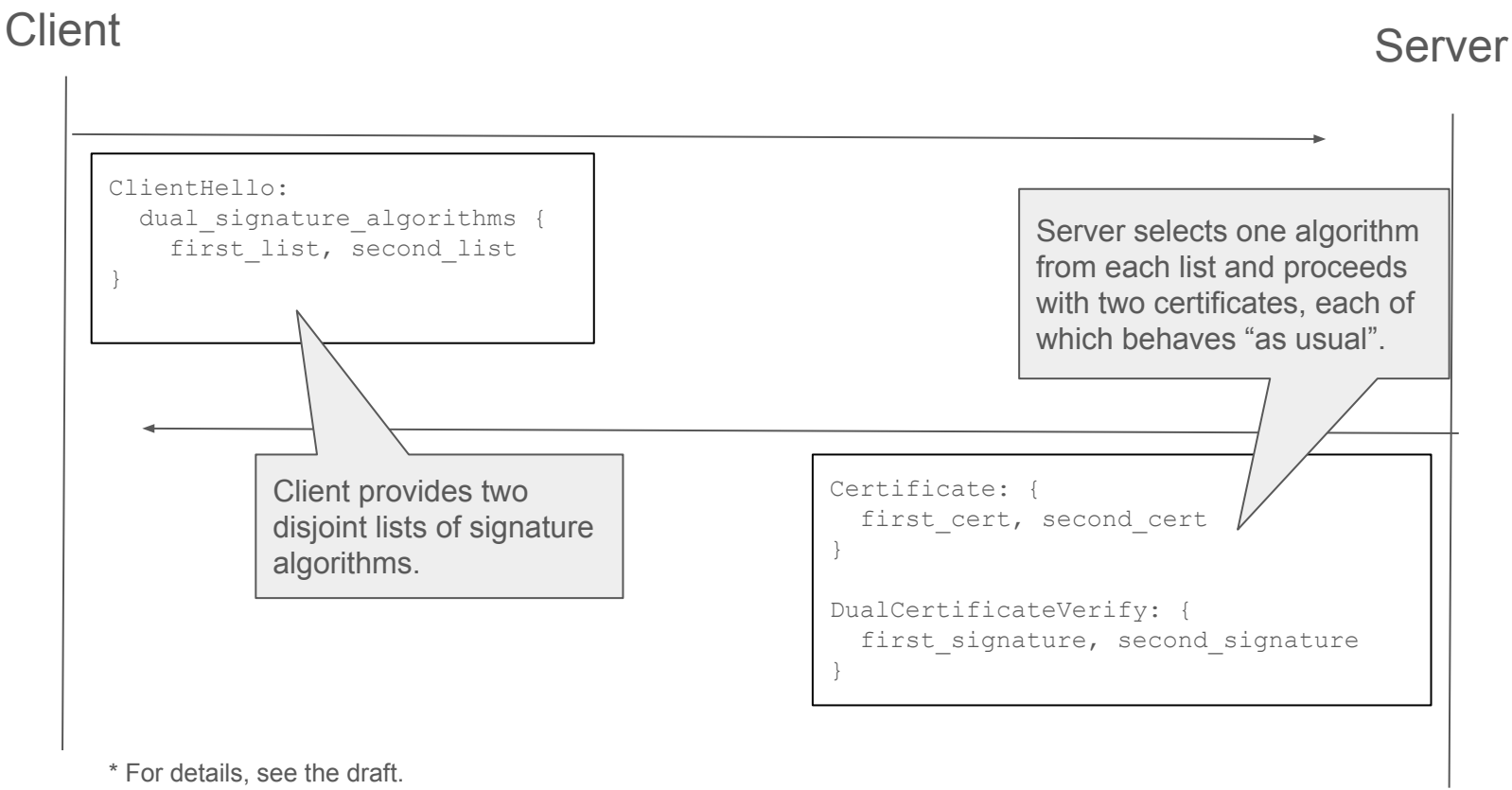
One certificate is deployed in each mode.

Parallel independent PKI



Two certificates are deployed in **Hybrid** mode.
One certificate is deployed in other modes.

Protocol Change Proposal



* For details, see the draft.

Pros of Dual Certificates compared to composites

- Traditional only, PQC only, Dual are negotiable.
  - Smoother transition to pure PQC mode.
- Simpler PKI (2 instead of 3 PKIs).
  - In multi-tenancy cases, there might be a need for more than 3 PKIs as there is no consensus on the preferred classic or PQ algorithms.
  - Easier to satisfy broader range of requirements in different jurisdictions.
- Simpler transition to new algorithms (no need to define a new composite).
- Standard single-algorithm X.509 certificates and chains, maximizing compatibility with existing PKI infrastructures.
- Maintains clear separation between traditional and post-quantum keys.

Cons of Dual Certificates compared to composites

- Requires changes to TLS 1.3 negotiation.
- Increases protocol message size due to the transmission of multiple certificate chains and signatures.
- Still requires management of two certificates/PKIs, but not as many as for composite certificates
  - Managing dual certificates from two different CAs introduces additional complexity, including handling separate renewal processes, trust anchors, and potential inconsistencies in certificate policies
- Transmission of dual certificates and corresponding certificate chains, can lead to message fragmentation and additional round trips, especially in constrained networks.
- The number of possible combinations when using separate PQC and traditional certificates can be large, whereas composite signatures typically allow only a defined and limited set of algorithm combinations at the protocol level.

Backup Slide
Technical Details

Technical Detail 1/3: dual_signature_algorithms Extension

```
struct {
    SignatureScheme first_signature_algorithms<2..2^16-2>;
    SignatureScheme second_signature_algorithms<2..2^16-2>;
} DualSignatureSchemeList;
```

Technical Detail 2/3: dual Certificate

The Certificate message is unchanged from TLS 1.3, it is:

```
struct {
    opaque certificate_request_context<0..2^8-1>;
    CertificateEntry certificate_list<0..2^24-1>;
} Certificate;
```

However, a delimiter of “0x00 0x00 0x00” (which is an empty CertificateEntry) is used to denote the end of one cert chain and the beginning of the next.

Technical Detail 3/3: DualCertificateVerify

```
struct {
    SignatureScheme first_algorithm;
    opaque first_signature<0..2^16-1>;
    SignatureScheme second_algorithm;
    opaque second_signature<0..2^16-1>;
} DualCertificateVerify;
```

The delimiter trick does not work here since any byte sequence could occur naturally within a signature, so a new message is required.

Additional use cases and Interactions

- The basic use case of 1 PQ chain + 1 Traditional chain is covered by the the new extensions and messages by themselves.
- This also interacts gracefully with Composite signature algorithms.
- More complex use cases such as allowing SLH-DSA for CAs but not for End Entities, or allowing both the PQ and Traditional End Entities to come from a PQ CA are handled via interaction with the existing `signature_algorithms_certs` extension. This part needs more design effort.