

Practical Challenges with Cross-signed Certs

as a signature algorithm transition mechanism

Panos Kampanakis
kpanos@amazon.com

Viktor Dukhovni
ietf-dane@dukhovni.org

August 25, 2026

Cross-signed certificates have been used as a transition mechanism in PKI for years. For example, when there is a new Certificate Authority (CA) that needs time to proliferate through ecosystem Trust Stores, the CA is sometimes cross-signed by an existing trusted CA in order to prevent outages with certificates issued by it. After the new CA certificate is established in Trust Stores, then it can be used as-is and the cross-signed certificate becomes irrelevant. Cross-signing could lead to overlapping certificate chains which authenticate the same leaf certificate. This complexity has sometimes led to issues depending on which path the verifier picked when building the certificate chain. Ryan Sleevi previously talked about the challenges of building the right chain.

Cross-signed certificates can serve as a transition mechanism for the upcoming PQ migration as well. They can enable PQ relying parties (clients or servers) to consume and verify the post-quantum chain and traditional verifiers to depend on the traditional cert chain. It can also serve as a migration mechanism where a verifier has been upgraded to support the PQ algorithms, but its environment Trust Store does not include any PQ Roots yet. For these options to work smoothly, they require robust and well-defined certificate chain choice logic to provide the right certificate chain to the relying party. **In this work, we investigated TLS server implementations like OpenSSL 3.5.5, s2n-ls 1.7.7, and nginx 1.31.4 (with OpenSSL 3.5.5) and discovered challenges that would make the cross-signing options error prone that could cause authentication failures. We conclude that some TLS implementations would need well-defined certificate chain picking logic updates.**

The issues we observed include inadvertent failures due to PQ algorithm support in the relying party without the proper PQ Roots in the Trust Store, due to incorrectly sending certificate chains to a relying party with signatures it does not support, and picking certificate chains for the relying party based only on order of configuration. **This session will include these challenges and options to address them and cover each solution's tradeoffs.**

Appendix

Below we provide more details about our experimental investigations.

A. Cross-signed leaf certs

One transition option is leaf cross-signed certs where the traditional public key and identity is issued two certificates, one signed by a traditional (i.e. ECDSA) ICA and one with a PQ (i.e. MLDSA) ICA. Figure 1 demonstrates such a scenario. This approach was proposed as a transition mechanism which allows PQ-only verifiers to consume the PQ ICA (and Root) and traditional ones to consume the traditional chain. The advantage of the approach is that authenticating parties do not need updates as they require only one traditional leaf keypair to authenticate to a relying party and they do not need to “understand” the algorithms in the PQ chain.

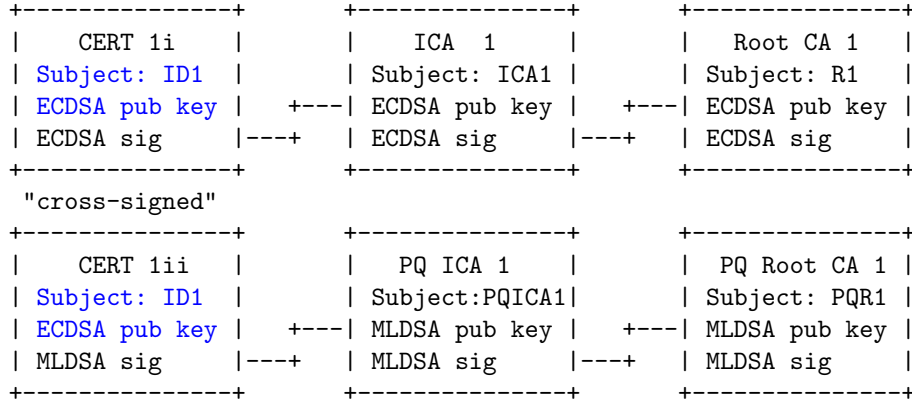


Figure 1: Cross-signed (by one ECDSA and one MLDSA ICA) leaf cert/identity.

Our investigation showed that this is not straightforward. We observed that OpenSSL, s2n-tls, and nginx (using OpenSSL) servers were picking the leaf certificate to send to the relaying party based on the leaf public key, but they were not honoring the client advertised `sigAlgs` in any of the signatures in the cert chain. So, even if the relaying party in Figure 1 was advertising support only for ECDSA, it could still get the PQ ICA1 based on the certificate configuration order on the server. This would lead to an authentication failure for legacy clients.

Note that this issue had probably not manifested itself in the past because cross-signing mostly applied to new CAs that were getting cross-signed. Leaf certificates sometimes were issued for different public keys (RSA or ECDSA) which tied to an issuing (RSA or ECDSA) Intermediate CA (ICA), but it has not been common for an entity to get issued and use two identity certificates with the same public key tying to different issuing CAs and certificate chains.

B. Cross-signed ICA certs

Another use case is cross-signing a PQ ICA identity with a traditional (i.e. ECDSA) and a PQ (i.e. MLDSA) Root CA in order to enable upgraded relying parties that support MLDSA but have not received the MLDSA Root in their Trust Store. This approach is common for such scenarios and was proposed as a PQ migration transition mechanism in draft-reddy-pquip-pqc-signature-migration. Figure 2 shows such a scenario.

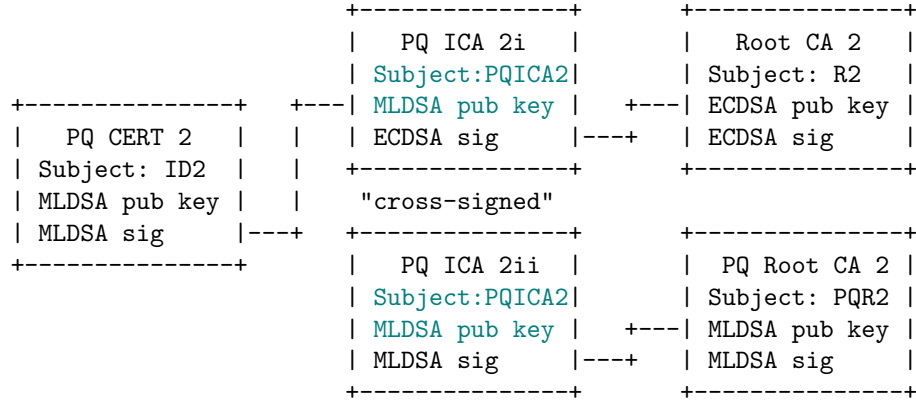


Figure 2: Cross-signed (by one ECDSA and one MLDSA Root CA) MLDSA ICA which issues MLDSA leaf certificates.

Our investigation showed that this approach won't be straightforward either. OpenSSL, s2n-tls, and nginx (using OpenSSL) servers were picking the leaf certificate and certificate chain to send to the relying part based only on the leaf public key without honoring the client advertised `sigAlgs` in the ICA cert signatures. So, even if the relying party in Figure 2 was advertising support for ECDSA only, it could get the PQ ICA 2ii based on the configured order on the server which would lead to an authentication failure in a legacy client.

Note that this issue had probably not manifested itself previously because relying parties were likely to support all traditional algorithms in cross-signed ICAs and had the necessary Roots.