

Post-Quantum Signature Algorithm Profile and Migration Considerations for the RPKI

Tomoki Yoshikawa

Graduate School of Informatics, Kyoto University

yoshikawa.tomoki.67i@st.kyoto-u.ac.jp

IETF 126 · SIDROPS

Draft status

- `draft-yoshikawa-sidrops-pqc-rpki-00` was published on 19 June 2026
- The current revision is `-01`, published on 4 July 2026
- Today: report the `-01` results and discuss how to divide the future work

Agenda

- Proposed document split
- PQC considerations: scope and candidates
- Measurements and migration design
- Implementation status and questions

Proposed document split

1. PQC considerations for the RPKI

- Informational: requirements, candidates, measurements, and operations
- Does not select a mandatory Next Suite

2. Mixed Certification Chains

- Algorithm-agnostic migration mechanism and update to RFC 6916

3. Concrete RPKI signature suite

- Standards Track work after the underlying specifications and deployment requirements mature

PQC considerations for the RPKI

- Intended status: Informational
- PQ signature requirements for RPKI certificates, CRLs, and signed objects
- Candidate algorithms and selection criteria
 - Pure PQ, Composite, and possible alternatives such as the Null Scheme
- Implementation experience, measurements, and test results
- Repository, RP, signer, HSM, and operational considerations
- No mandatory Next Suite is selected

Motivation and scope

- NIST standardized ML-DSA and SLH-DSA in 2024
- ML-DSA use in X.509 and CMS is standardized in RFC 9881 and RFC 9882
- RPKI still relies on RSA-2048/SHA-256 and needs a coordinated migration path

In scope

- Resource certificates, CRLs, and certification requests
- RFC 6488 signed objects
- BGPsec Router Certificates
- CA, repository, and RP processing

Out of scope

- BGPsec UPDATE signatures
- RTR, TAL, RRDP, and rsync
- RPKI object payloads and router behavior
- BPKI and the production transition timetable

Candidate signature profile

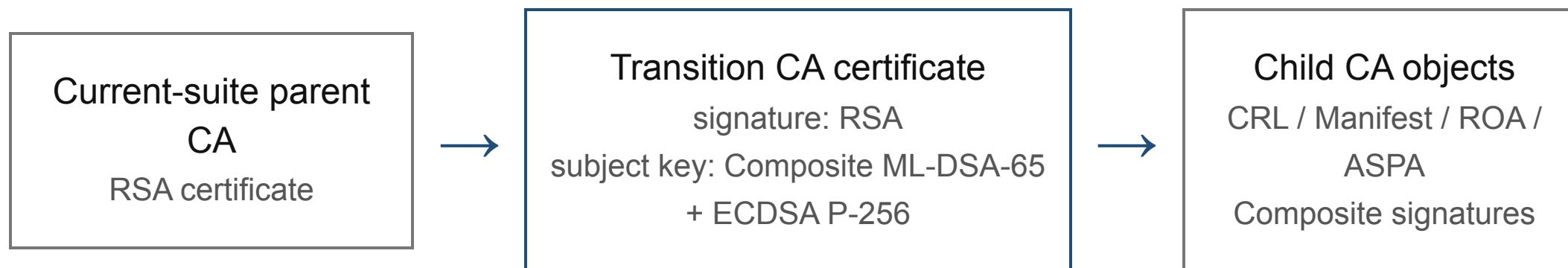
- Primary experimental candidate:
 - Composite ML-DSA-65 with ECDSA P-256
 - Both component signatures must validate
- Uses the LAMPS Composite signature and CMS specifications
- Pure ML-DSA PKIX/CMS profiles are standardized; the Composite encodings used here remain Internet-Drafts
- Provides security while either component remains secure
- Avoids separately signed classical and PQ versions of the same object
- Does not provide compatibility with existing RPs
- This is an experimental reference point, not a mandatory Next Suite

Additional measurements

Algorithm	Repository ratio	Sign 100k	Verify 100k
RSA-2048	1.00×	34.3 s	1.0 s
ML-DSA-44	3.08×	25.1 s	5.0 s
ML-DSA-65	4.01×	40.5 s	7.7 s
ML-DSA-87	5.28×	47.9 s	11.7 s
ML-DSA-44 + P-256	3.16×	26.0 s	8.2 s
ML-DSA-65 + P-256	4.09×	41.4 s	10.8 s
ML-DSA-87 + P-384	5.40×	58.1 s	32.8 s

- Composite rows use the Draft-19 message representative and raw concatenation encoding
- Repository ratios use measured Composite key/signature sizes; they are model outputs, not full-repository measurements
- Key generation, I/O, and X.509/CMS construction are excluded

Migration design



- Mixed Certification Chains switch algorithms at a CA boundary
- RPs must support the new algorithm before a subtree switches
- This algorithm-agnostic design should be specified in the new Mixed Certification Chains draft

The RSA parent certifies the child CA's Composite public key

Implementation status and next steps

Completed

- Published the reproducible implementation and measurements
- Completed Composite primitive generation, verification, and benchmarking based on Draft-19

Next

- Split the current work into clearly scoped drafts
- Broaden the evaluation of candidate approaches
- Integrate Composite signatures into X.509, CRLs, and CMS signed objects
- Add interoperability, HSM, and operational evidence

Questions for SIDROPS

1. Is the proposed three-document split the right direction?
2. Are the proposed requirements and selection criteria complete?
3. Which signature candidates need further evaluation?
4. What implementation and operational evidence should be included?

Thank you

- Thank you to everyone who reviewed `-01` and joined the mailing-list discussion!
- Special thanks to Job Snijders, Dirk Doesburg, and Tim Bruijnzeels
- Comments and implementation feedback are welcome!
- Co-authors are welcome!