Revocation of Persistently Non-functional Delegated RPKI CAs

Author(s): Job Snijders, Nick Hilliard
Document ID: ripe-847
Approved by: Routing Working Group
Date: October 2025

Abstract:

The RIPE NCC offers users of its RPKI certification service two deployment models: "Hosted CA setup" and "Delegated CA setup".

In the Hosted setup the RIPE NCC is responsible for timely issuance and publication of new RPKI Manifests and CRLs, but in the Delegated setup resource holders themselves manage their CA on their own infrastructure.

It is possible for Delegated CA infrastructure to be offline for extended periods of time, or for the contents of publication repositories to become stale or otherwise invalid. This policy provides a mandate to the RIPE NCC to revoke resource certificates associated with longtime non-functional CAs to reduce Relying Party workload.

This policy targets only pathologically non-functional CAs. An example of a situation considered out-of-scope for this policy would be a publication repository service advertised to also be available via IPv6 and RRDP but in practice only reachable via IPv4 and Rsync: the associated CA would still be considered functional (provided a valid and current Manifest could somehow be retrieved and validated sometime in the previous three months). In other words: this policy isn't about CAs that didn't achieve 100% uptime, but about CAs that are down all the time.

Policy Text:

If the RIPE NCC is unable to discover and validate a Delegated RPKI Certification Authority's (CA's) current Manifest and Certification Revocation List (CRL) for more than three months, that Delegated CA's resource certificate shall be revoked by the RIPE NCC.

The RIPE NCC shall make reasonable efforts to discover new Manifests, to notify the Delegated CA operator if a current Manifest and CRL cannot be validated, and to notify the operator if the delegation is revoked.