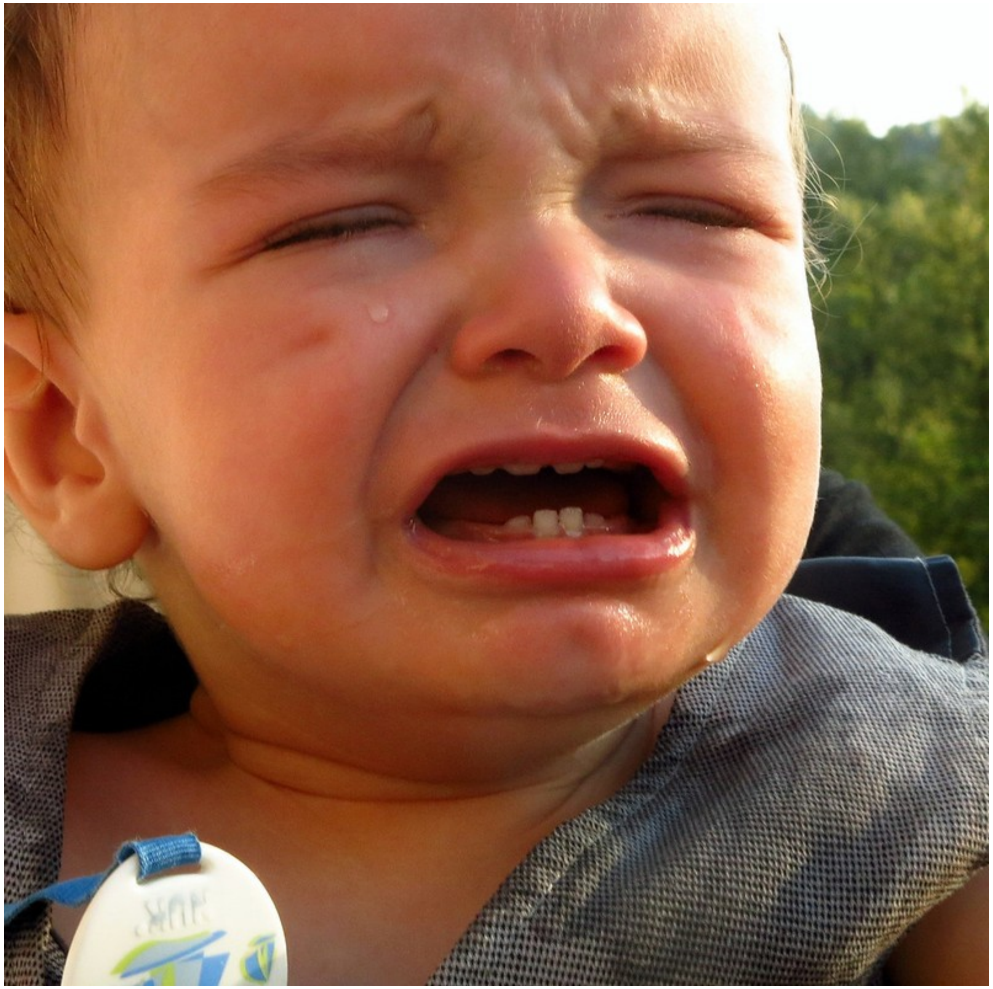
RPKI & Certificate Transparency & Discoverability (2022-2026)

Job Snijders

job@fastly.com

RPKI & Maturity: teething pains :-)



https://www.flickr.com/photos/amre/17575782121 2014 by Amre

Looking at our bigger sister: WebPKI

https://pixabay.com/photos/face-motorcycle-leather-jacket-1001876/

Some differences between RPKI & WebPKI

WebPKI roots need to jump through many hoops before being admitted into (for example) the Mozilla Trust Store:

- Show annual *audit reports* that conform to CA/B Forum specs
- Before inclusion, WebPKI CAs might operate *years* without subscribers: stringent track record required
- → Certificate Transparency is *tech* to help justify trust in a PKI ←

Certificate Transparency @ RIPE Routing WG

Martin Hutchinson (Google) gave a high level introduction

about Certificate Transparency at RIPE 83 Routing WG

https://ripe83.ripe.net/wp-content/uploads/presentations/12-Certificate-Transparency-and-Discoverability.pdf

https://ripe83.ripe.net/archives/video/648

Mapping WebPKI CT to RPKI CT terminology

CT term	WebPKI	RPKI
Believer	Web Browser	RPKI Validator (rpki-client, fort, etc)
Verifier	Domain Owner	INR holder (AS or IP owner / LIR)
Verifier	Security Researchers	Security Researchers
Claimant	CAs (GeoTrust, Let's Encrypt, GoDaddy)	RIR Trust Anchor Operator operated CAs

https://github.com/google/trillian/tree/master/docs/claimantmodel

Why not tap RRDP or RSYNC?

Both RRDP and RSYNC provide “incomplete” views on all CA certificates (by design): both protocols focus on providing efficient discoverability of the “most current set of objects”.

Example: although manifestNumbers monotonically increment, two adjacent RRDP delta’s might show gaps between Manifests.

Certificate Transparency happens in an earlier stage: right before you are about to issue a RFC3779 constrained CA Certificate, tell someone else! (the Log)

Benefit to the community: auditable logs of RIRs

RPKI Certificate Transparency:

INR holders can audit exactly which CAs had what INR entitlements at what moment in time. (Did the RIR temporarily give some other party the ability to “sign with MY resources”?! Or, exactly between when I got revoked and a new cert was issued?)

Implementing CT raises the bar in this ecosystem, aspiring to implement CT will have positive impact (everyone needs to take another careful look at how exactly their processes / procedures work)

Todo list – keep in mind this is a multi year project

Initial scope: keep track of CA certs (not EE certs like MFT/ROAs/BGPsec/etc)

In scope people: RIRs, Log operators, Verifiers

Out of scope: Delegated RPKI, RP implementations

Looking for other interested people:

- Author internet-draft mapping out a plan
- Find people who want to host Logs
- Find people who want to send pre-certificates to Logs
- Find people who have hands-on experience with CT