RPKI Resilience

How Trustworthy is our Trust Anchor?
Problem Statement

- RPKI is becoming a fundamental component in the Internet infrastructure
- An prolonged outage in RPKI can have a severe impact on the operations of the Internet
- Having a resilient RPKI infrastructure is very important
Risk Areas We Identified

- Technical infrastructure (e.g. uptime, redundancy)
- Operations (e.g. staffing, processes)
- Trust (e.g. verified by independent third-party)
Technical Infrastructure

- Our current uptime numbers are very good
  - RPKI repository: 100%
  - Core: 99.94%
- Downtime only due to scheduled maintenance
- Updated core systems in 2019
Operational

• Improve knowledge on the RPKI core by the team
  • Prioritise work that involves RPKI core changes (e.g. TA key-roll)

• Division of knowledge between technical teams
  • Implement DevOps in the RPKI team (merging IT and Software Development into one team)

• Enhance procedures and processes
Trust

- We sign our own Trust Anchor
  - Have a third-party assessing our code (focus on the crypto)
- No third-party assessing if we are doing what we say we are doing
  - We also want to do a security assessment (check for security vulnerabilities)
Questions

nathalie@ripe.net