A Reference Implementation of Ascertaining RPKI Signed Objects to be Validated in Incremental Updates (draft-madi-sidrops-partial-validation-00)

Di Ma & Yu Zhang
SIDROPS @ IETF 119
Brisbane, Australia
Motivation

• Due to the hierarchical allocation of INRs and the trust model in the RPKI, an update to an RPKI signed object might lead to change of validation status of others in the RPKI.

• It is desirable to ascertain all the affected parts of the RPKI trees and perform the corresponding validation tasks as quickly as possible in order to inform the routing system of those changes in time.
Overview

• Comprehending the characteristics of different RSOs and the correlations among them, this document is to describe a reference implementation of ascertaining RSOs that need to be validated
  – After a transaction of RPKI incremental update from the perspective of the RP
  – Before performing the RPKI validation specified by RFC6487 and RFC8360

• We are defining some terminologies to describe how the RP manages the correlations of RSOs in the memory.

  RSO: RPKI Signed Object in the very context generally includes resource certificate, CRL, manifest, ROA and any other signed data derived from the RPKI.
Horizontal Correlation

- A horizontal correlation: RSOs with the same AKI value
- The union set of those horizontal correlations: the Horizontal Correlation Set
- If the validation status of an RSO X needs to be verified due to the update of an RSO Y that is in the same horizontal correlation with X, X is considered to be horizontally involved with Y.

Figure 1: Example of an element of Horizontal Correlation Set
Vertical Correlation

• A vertical correlation: An RSO (Primary Object) and its all adjacent child RSOs
• The union set of those vertical correlations: the Vertical Correlation Set
  — The process establishes the vertical correlation for every resource certificate in the RPKI.
• If the validation status of an RSO X needs to be verified due to the update of the primary object Z in the vertical correlation, X is considered to be vertically involved with Z.
Involvement Correlation

✓ An involvement correlation: An RSO (primary object) and all the other RSOs (target objects) that are either horizontally or vertically involved with it.

✓ The union set of those involvement correlations: the Involvement Correlation Set.

Figure 3: Example of an element of Involvement Correlation Set.
Procedure of Target Object Discovery

For a given updated RSO X, the task of establishing the involvement correlation of X is called **Target Object Discovery** of X.
Clarifications

1) This document is not syntactically bringing any change to validation of RPKI signed objects in any sense.

2) This document is intended to offer a referenced method to manage those “hard states” (the so-called Horizontal Correlations and Vertical Correlations) and “soft states” (the so-called Involvement Correlations) in the memory by the RP to verify the validation statuses of RPKI signed objects.
QUESTIONS?