NRO Declaration on RPKI
27 July 2009

Over several years, a set of mechanisms has been under development for digital certification of Internet number resources, through a so-called Resource Public Key Infrastructure, or "RPKI". Like other PKIs, the RPKI requires one or more root authorities, to act as so-called "trust anchors" for one or more certification hierarchies.

The RPKI architecture has been designed to allow a number of trust anchor configurations involving: either a single trust anchor located at the root of a single certification hierarchy; a set of independent trust anchors to be located at the roots of several independent hierarchies; or a hybrid of these. The alternative models may have advantages and disadvantages in various dimensions including: operational efficiency; alignment with resource allocation hierarchies; centralisation vs distribution of functions; recognised global or regional authority; and, operational capacity of the respective host organisations.

The Regional Internet Registries (RIRs) believe that the optimal eventual RPKI configuration involves a single authoritative trust anchor.

That configuration may not be achievable in the short-term and the details and timelines for its implementation will depend among other things on discussions within the RIRs' communities and dialogues with others including the Internet Architecture Board (IAB) and the Internet Engineering Task Force (IETF).

In the meantime, the RIRs have agreed to undertake pragmatic implementations of RPKI services based on interim trust anchor models, such as, self-signed trust anchors. All such implementations will comply with the overall RPKI architecture. The implementations will also have the ability to evolve into a single trust anchor model and to provide robust and fully operational (and inter-operational) services for those who wish to use them. The objective is for all RIRs to be ready to start issuing certificates by no later than 01 January 2011.

The RIRs will continue working with and receiving feedback from their respective communities and industry partners to ensure effective ongoing evolution of the RPKI system.