Aspects of Resource Public Key Infrastructure (RPKI) Deployment

John Curran
President & CEO, ARIN
Resource PKI Functionality

- Creates digital certificates which correspond to Internet number resource blocks (The user assigned an IP address block “JKL” has the matching certificate for address block “JKL”)

- Allows use of those certificates to “sign” a routing authorization (The user digitally signs an authorization record that Internet service provider “ABC” may route their address block “JKL”)

- Allows publication in a secure manner of the certificates and the authorization records in a secure & verifiable repository

- Networks which receive routing update may consult with the repository to determine if the actual source network of a routing update is matches an authorization record for that address block.

- Prevents inadvertent and intentional hijacking of a specific users network traffic by unauthorized networks
The IETF SIDR working group chartered with RPKI development has produced dozens of Internet Drafts, and all of these have been publicly available for review and comment.

Providing RPKI certificates is an *optional* service which the RIR community has been working on because service providers and users desire the resulting functionality.

RPKI provides the same type of data as today’s WHOIS and the routing registries, only with a higher degree of credibility.

RPKI deployment occurs when users start certifying the service providers that can route their addresses, and service providers begin using it to verify routes received by other service providers.

Service providers already prioritize, weight, and filter the routing information they receive to assemble the most reliable routing possible; RPKI simply provides another tool for this purpose.