Origin Validation

• Prevent YouTube incident
• Prevent 7007 accident
• Prevents most accidental announcements
• Does not prevent malicious path attacks such as the Kapela/Pilosov attack
• That requires “Path Validation” and locking the data plane to the control plane, the next steps
IR Back End

[Hardware]

Signing Module

IR

RPKI

Priv Keys

Private RPKI

Keys

Issued ROAs

My Misc Config Options

Public RPKI

Keys

ID=Me

RPKI Engine

XML Object

Transport & Handler

Private RPKI

Biz EE Signing Key

IR

RPKI

Priv Keys

Internal CA Data

ID=Me

Keys for Talking to IR Backend

My Resources

My RightsToRoute

Pub Key/Cert Management

Up/Down EE

Public Keys

Up/Down Protocols

Publication Protocol

Resource PKI

IP Resource Certs

ASN Resource Certs

Route Origin Attestations

Left Right Protocol

Business Key/Cert Management

Private IR Biz Trust Anchor CA Data

Internal CA Data

Repo Mgt

Up/Down Protocols

Prototype of Basic Back End
A Player (CA) Publishes All Certificates Which They Generate in Their Own Unique Publication Point
RCynic Cache Gatherer
(cynical rsync)
Reliability Issue

Expensive To Fetch & Unreliable
Reliability Via Hosted Publication

Reducing the Number of Publication Points Makes RCyinic Much More Efficient
Allocation in Reality

My Infrastructure

Static (non BGP) Cust

BGP Cust

Unused
ROA Use

My Aggregate ROA

Customer ROAs

I Generate for 'Lazy' Customer

My Infrastructure

BGP Cust

Static (non BGP) Cust

Unused
RPKI -> Router

The Fourth Protocol
(origin validation only)

the net

Object Security
RCynic Gatherer

Cache / Server

Transport Security
ssh

RCynic to Rtr Protocol

BGP Decision Process

In PoP

2009.07.30 sidr
Typical Exchange

```
Cache                    Router
~                         ~
| -------------- Notify ---------> | (optional)
|<-------------- Serial Query -------| R requests data
|----- Cache Response ---------> | C confirms request
|---------- IPvX Prefix --------> | C sends zero or more IPv4 and IPv6 Prefix
|---------- IPvX Prefix --------> | Payload PDUs
|---------- IPvX Prefix --------> | C sends End of Data
|----- End of Data ---------> | and sends new serial
~                         ~
```
Serial Query

0          8          16         24        31

| Protocol |   PDU    |                     |
| Version  |   Type   |   reserved = zero   |
|    0     |    1     |                     |
|          |   0      |   1                 |

Length=12

Serial Number
## IPv4 Prefix

### Format:

<table>
<thead>
<tr>
<th>Field</th>
<th>Length</th>
</tr>
</thead>
<tbody>
<tr>
<td>Protocol</td>
<td>8</td>
</tr>
<tr>
<td>Version</td>
<td>8</td>
</tr>
<tr>
<td>PDU Type</td>
<td>8</td>
</tr>
<tr>
<td>Color</td>
<td>8</td>
</tr>
<tr>
<td>Length</td>
<td>8</td>
</tr>
<tr>
<td>Prefix</td>
<td>32</td>
</tr>
<tr>
<td>Max Length</td>
<td>32</td>
</tr>
<tr>
<td>Data Source</td>
<td>32</td>
</tr>
</tbody>
</table>

### Example:

<table>
<thead>
<tr>
<th>0</th>
<th>8</th>
<th>16</th>
<th>24</th>
<th>31</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>0</td>
<td>4</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Flags</th>
<th>Prefix</th>
<th>Max</th>
<th>Data</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>0..32</td>
<td>0..32</td>
<td>RPKI/IRR</td>
</tr>
</tbody>
</table>

### Interpretation:

- **IPv4 prefix**: 2009.07.30 sidr
- **Autonomous System Number**: 13
IPv6 Prefix

<table>
<thead>
<tr>
<th>Protocol Version</th>
<th>PDU Type</th>
<th>Color</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>6</td>
<td></td>
</tr>
</tbody>
</table>

Length=40

<table>
<thead>
<tr>
<th>Flags</th>
<th>Prefix Length</th>
<th>Max Length</th>
<th>Data Source</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>0..128</td>
<td>0..128</td>
<td>RPKI/IRR</td>
</tr>
</tbody>
</table>

---

IPv6 prefix

---

Autonomous System Number
End of Data

<table>
<thead>
<tr>
<th>Protocol Version</th>
<th>PDU Type</th>
<th>reserved = zero</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>7</td>
<td></td>
</tr>
</tbody>
</table>

Length=12

Serial Number