The RPKI & Origin Validation

sidr - Stockholm

2009.07.30

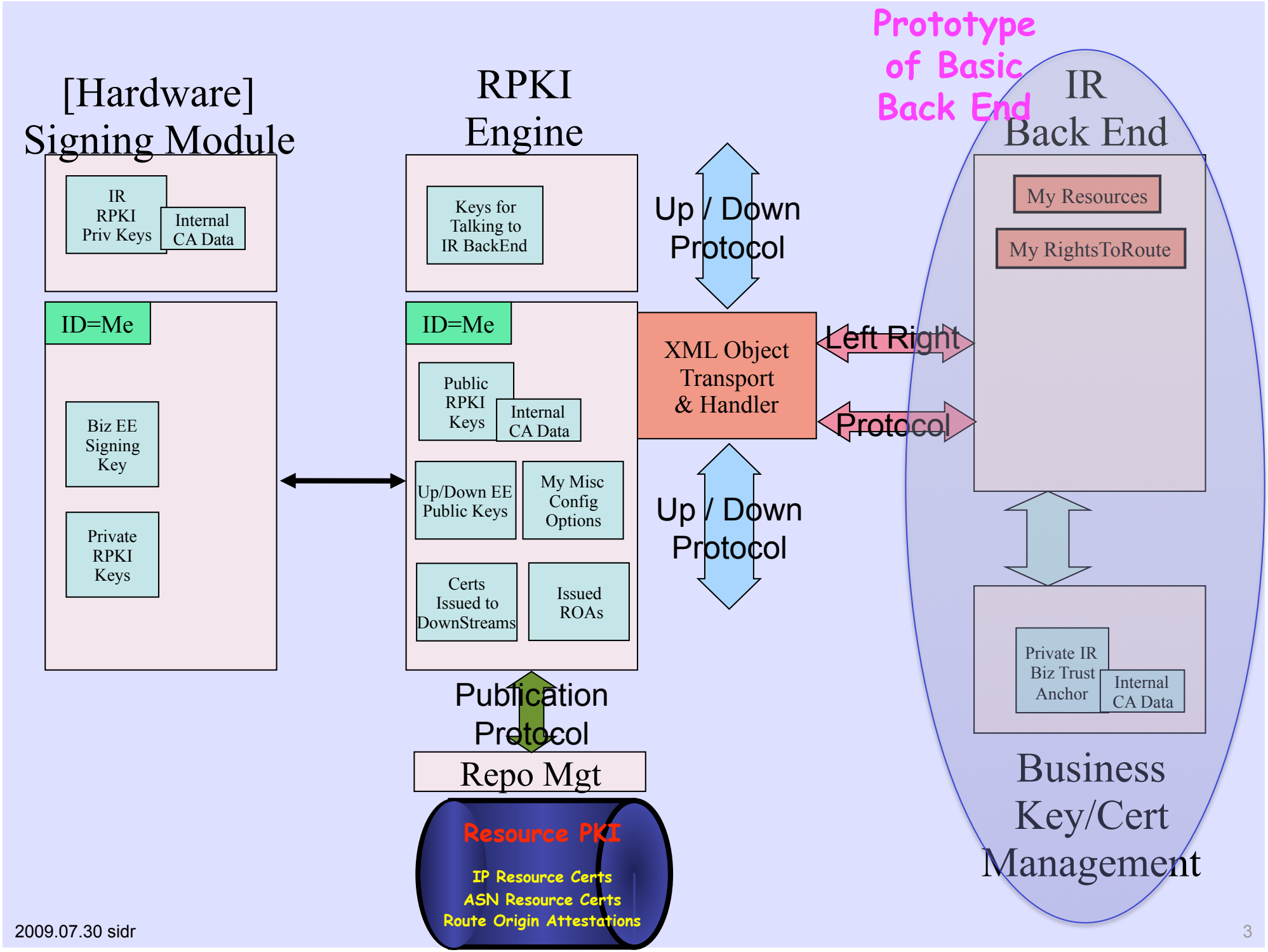
Randy Bush <randy@psg.com>

Rob Austein <sra@isc.org>

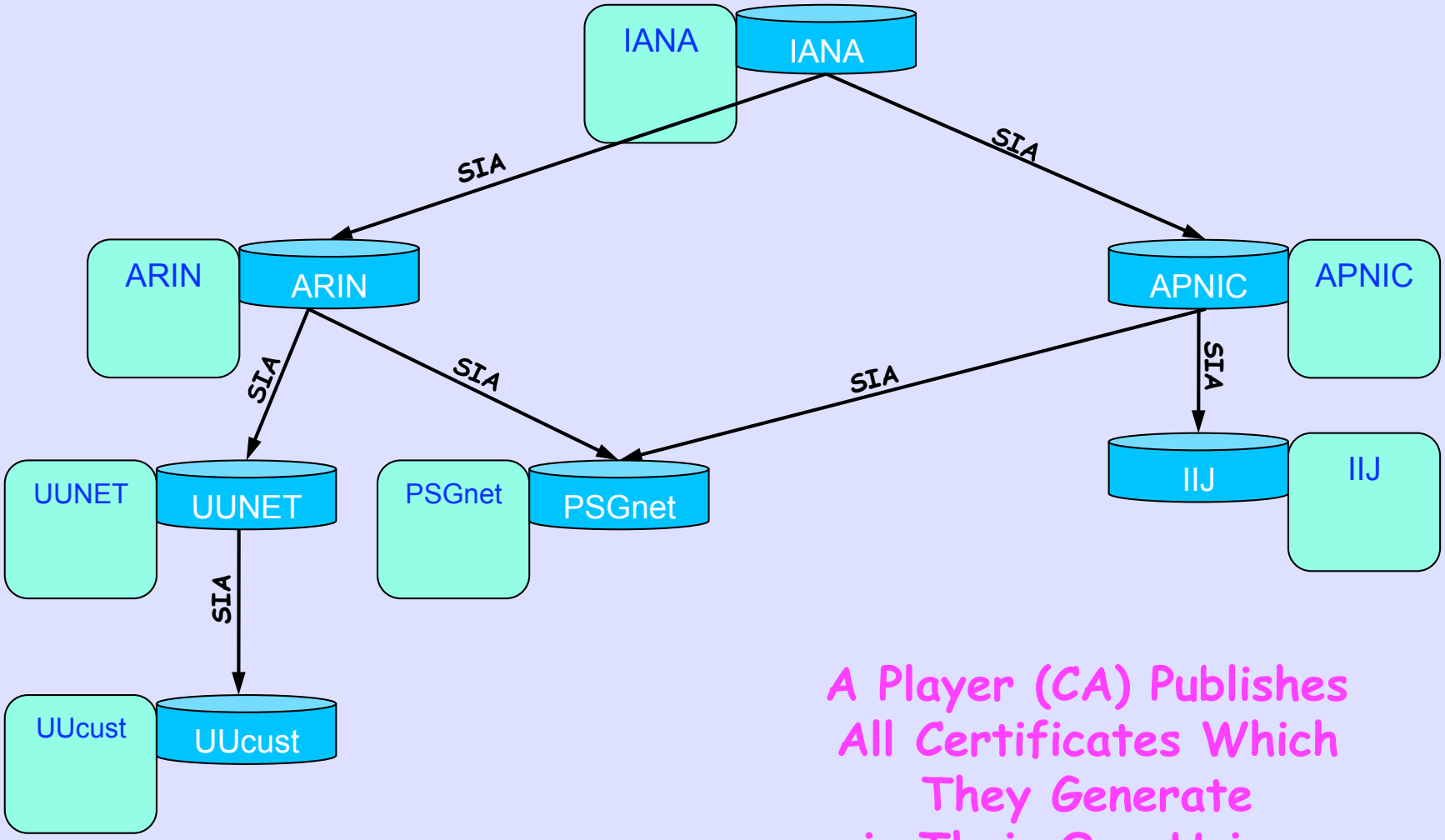
<http://archive.psg.com/090730.sidr-rpki.pdf>

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


Prototype of Basic Back End
[Hardware] Signing Module
IR RPKI Priv Keys
Internal CA Data
ID=Me
Biz EE Signing Key
Private RPKI Keys
RPKI Engine
Keys for Talking to IR BackEnd
ID=Me
Public RPKI Keys
Internal CA Data
Up/Down EE Public Keys
My Misc Config Options
Certs Issued to DownStreams
Issued ROAs
Up / Down Protocol
XML Object Transport & Handler
Up / Down Protocol
Left Right
Protocol
Publication Protocol
Repo Mgt
Resource PKI
IP Resource Certs
ASN Resource Certs
Route Origin Attestations
IR Back End
My Resources
My RightsToRoute
Private IR Biz Trust Anchor
Internal CA Data
Business Key/Cert Management

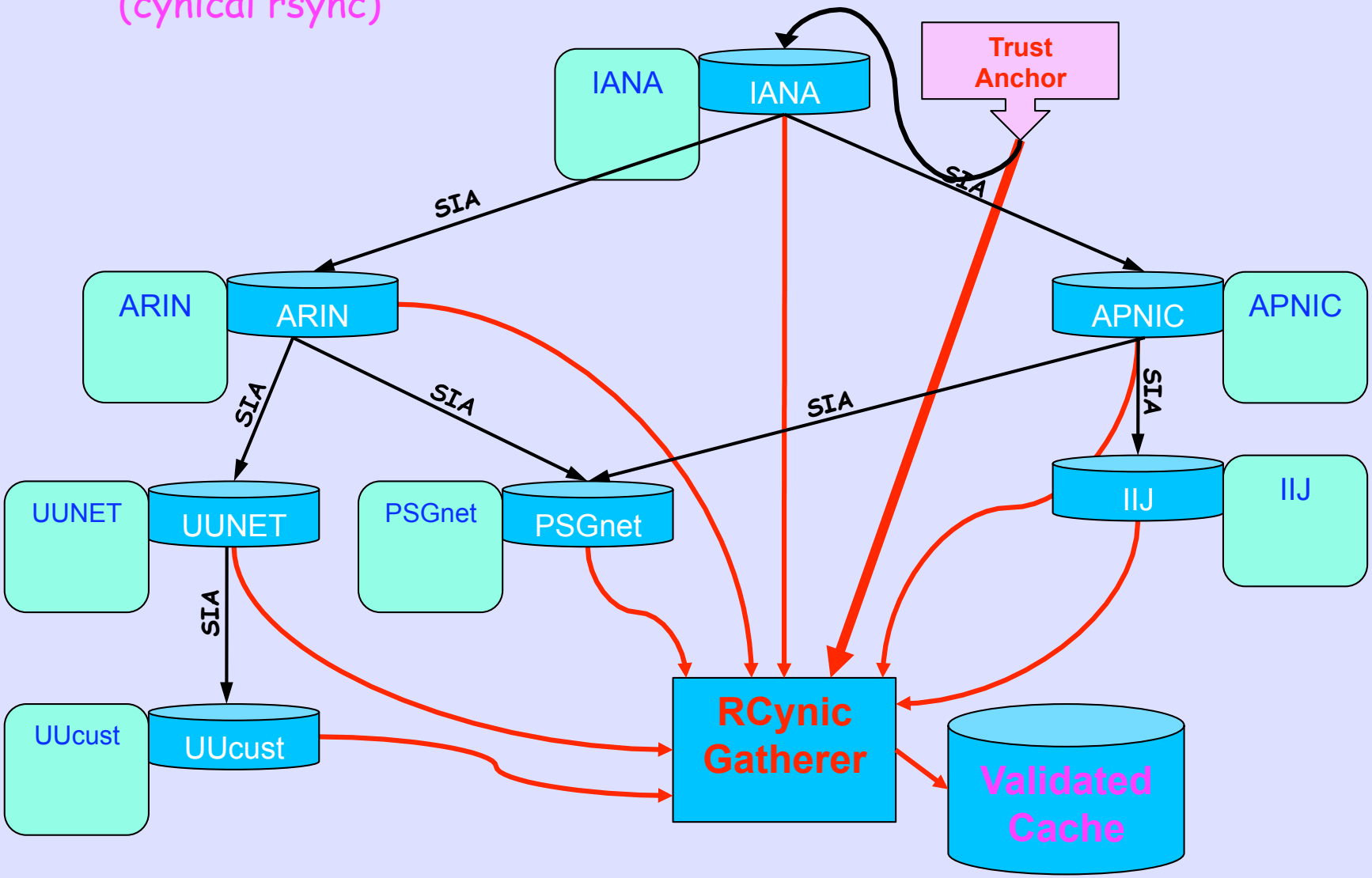
Distributed RPKI DataBase



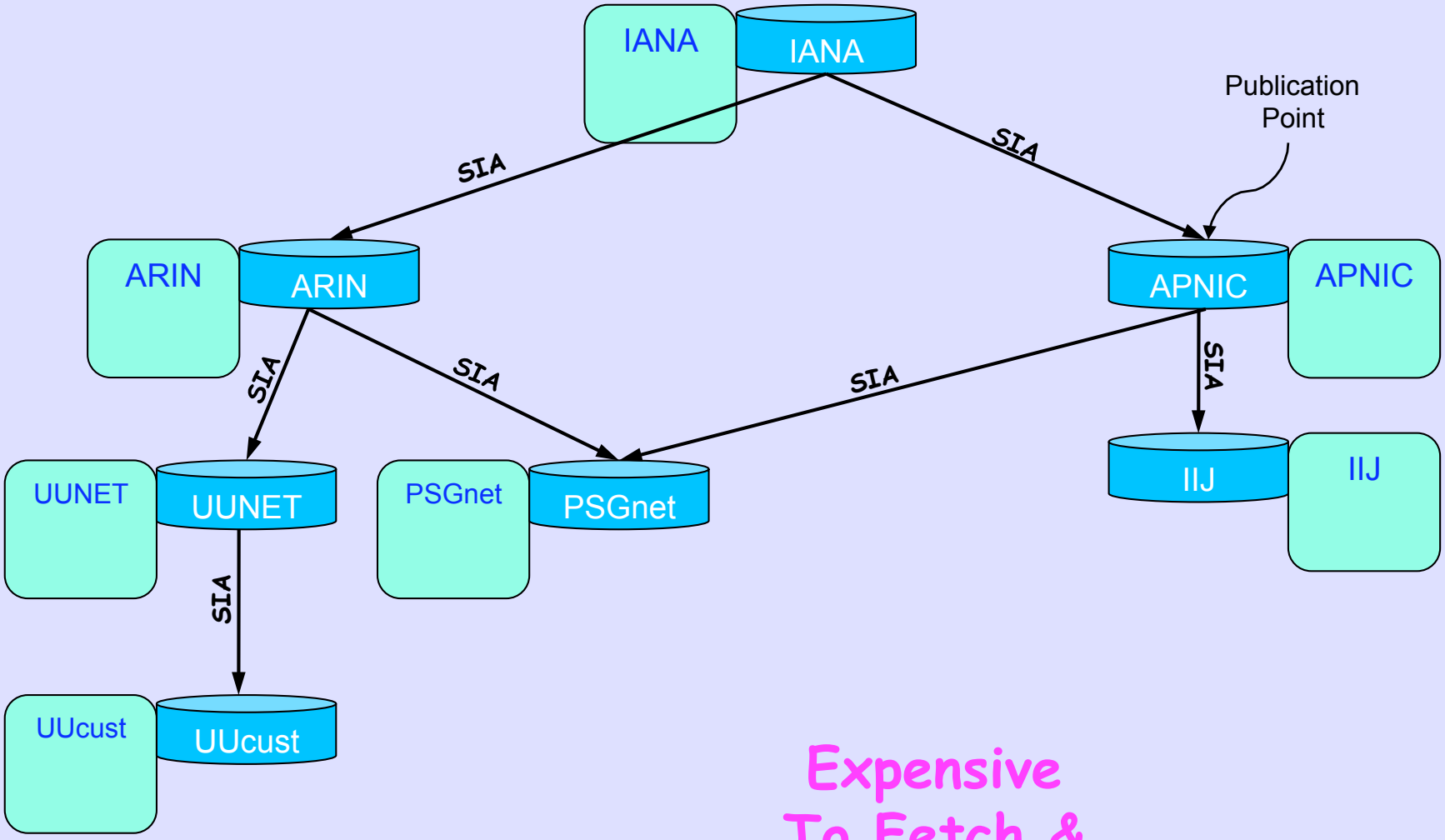
A Player (CA) Publishes
All Certificates Which
They Generate
in Their Own Unique
Publication Point

RCynic Cache Gatherer

(cynical rsync)

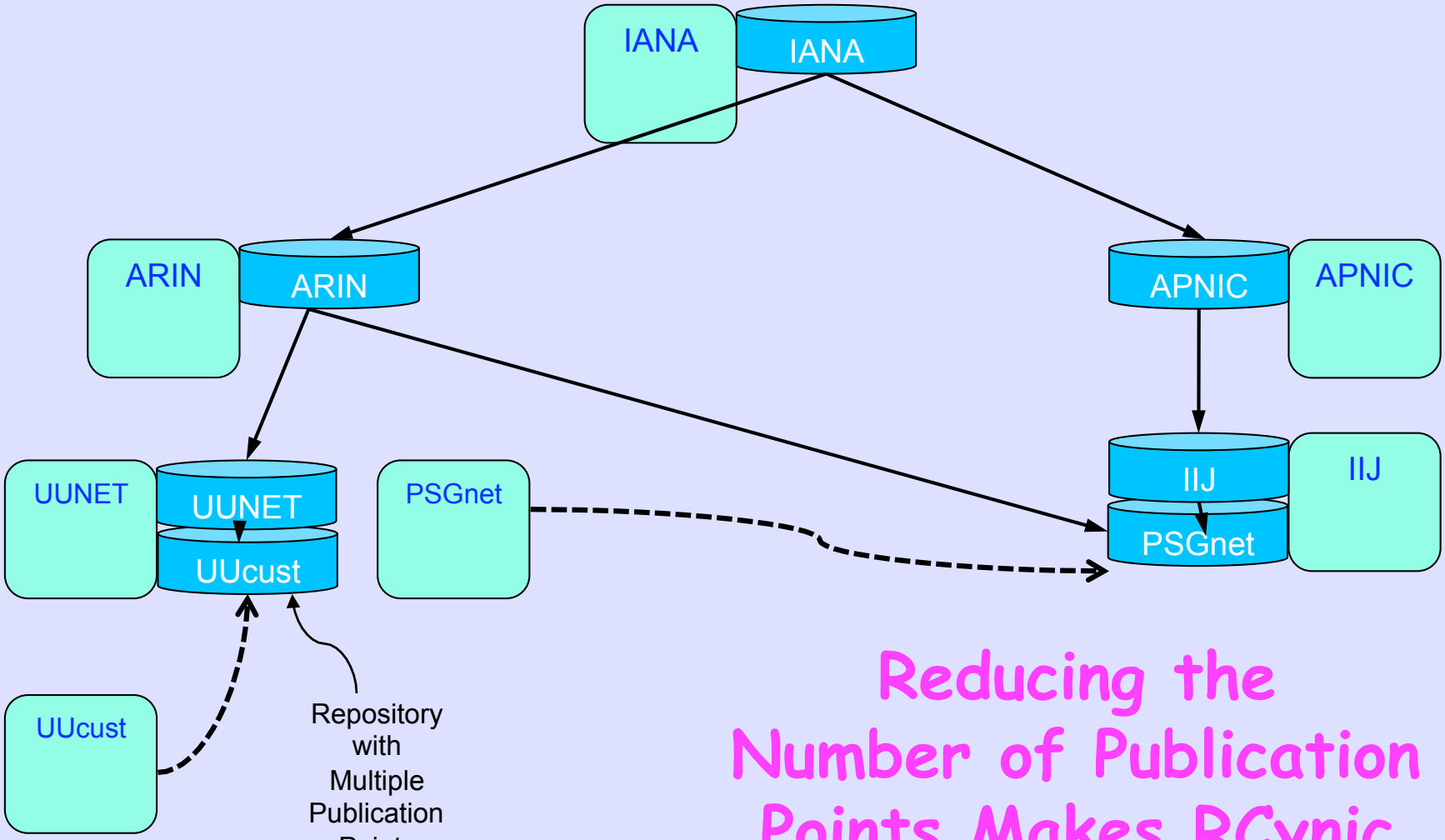


Reliability Issue



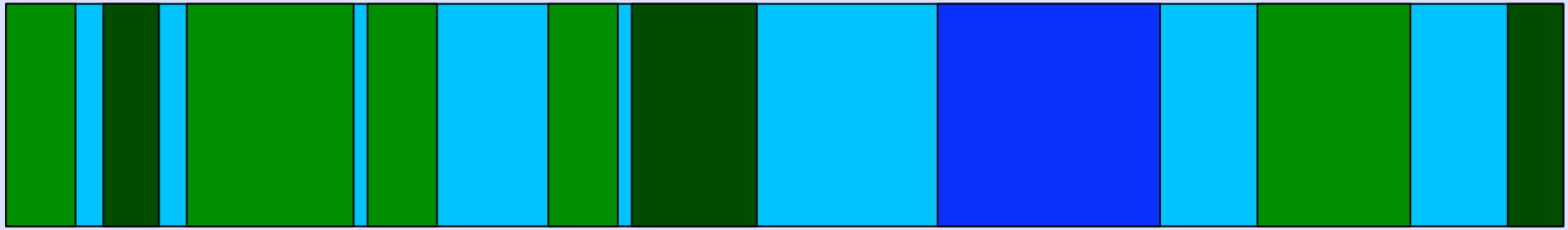
Expensive To Fetch & Unreliable

Reliability Via Hosted Publication



Reducing the Number of Publication Points Makes RCynic Much More Efficient

Allocation in Reality



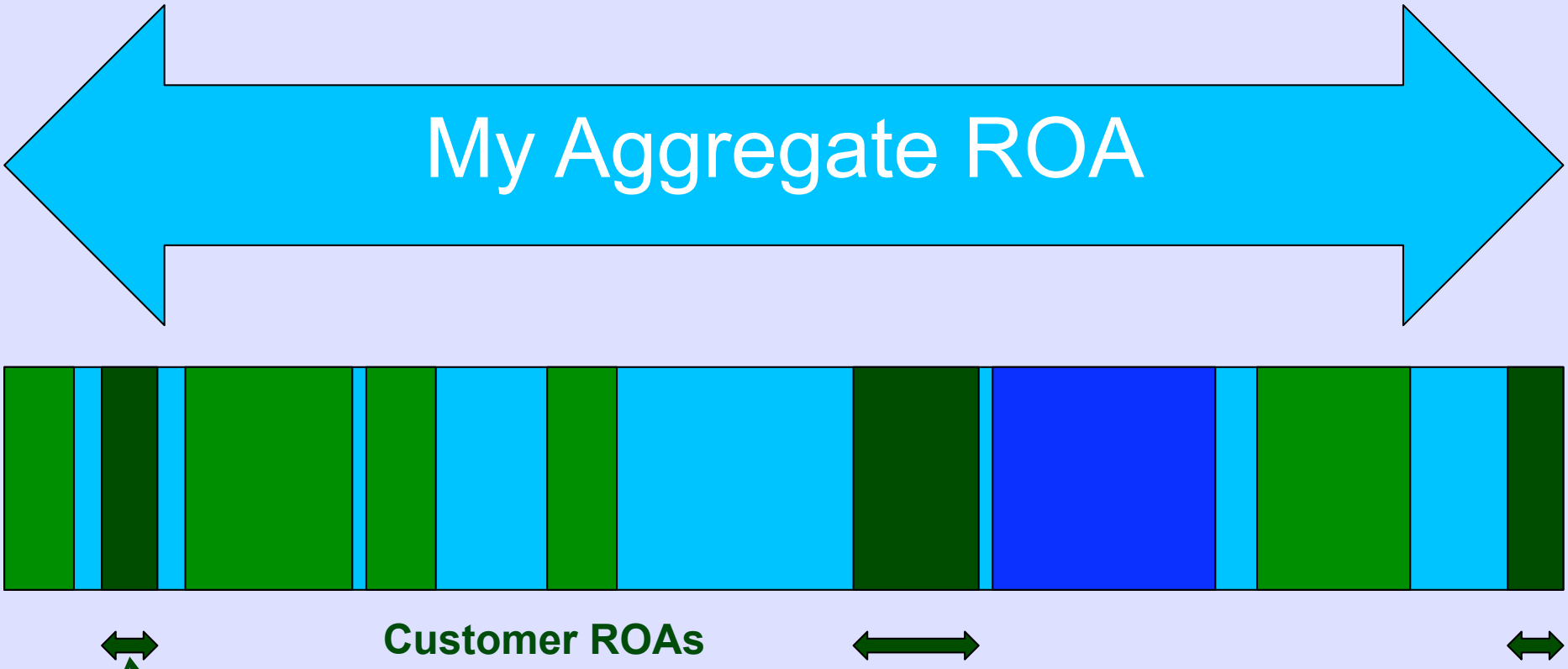
My Infrastructure

BGP Cust

Static (non BGP) Cust

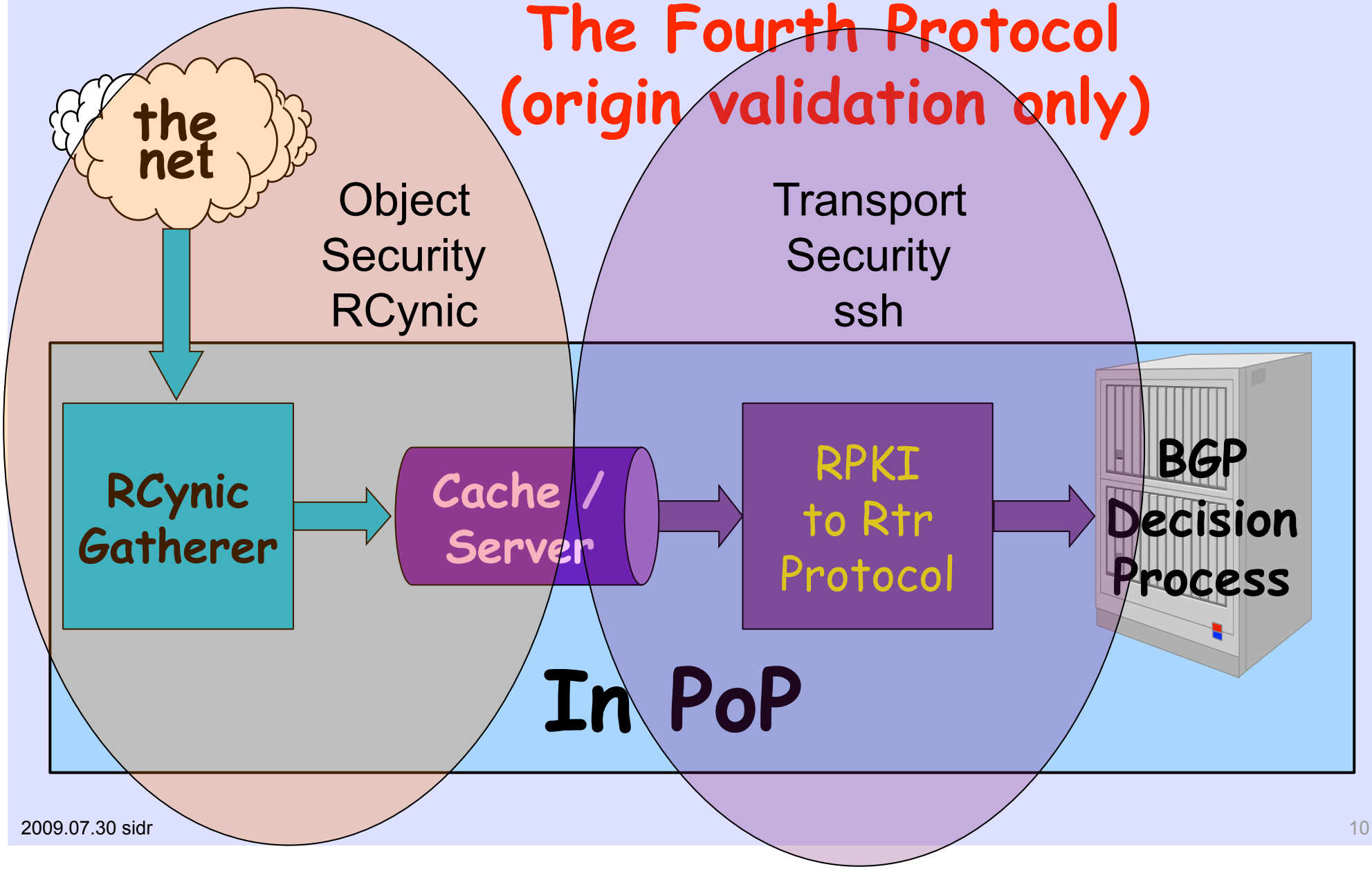
Unused

ROA Use

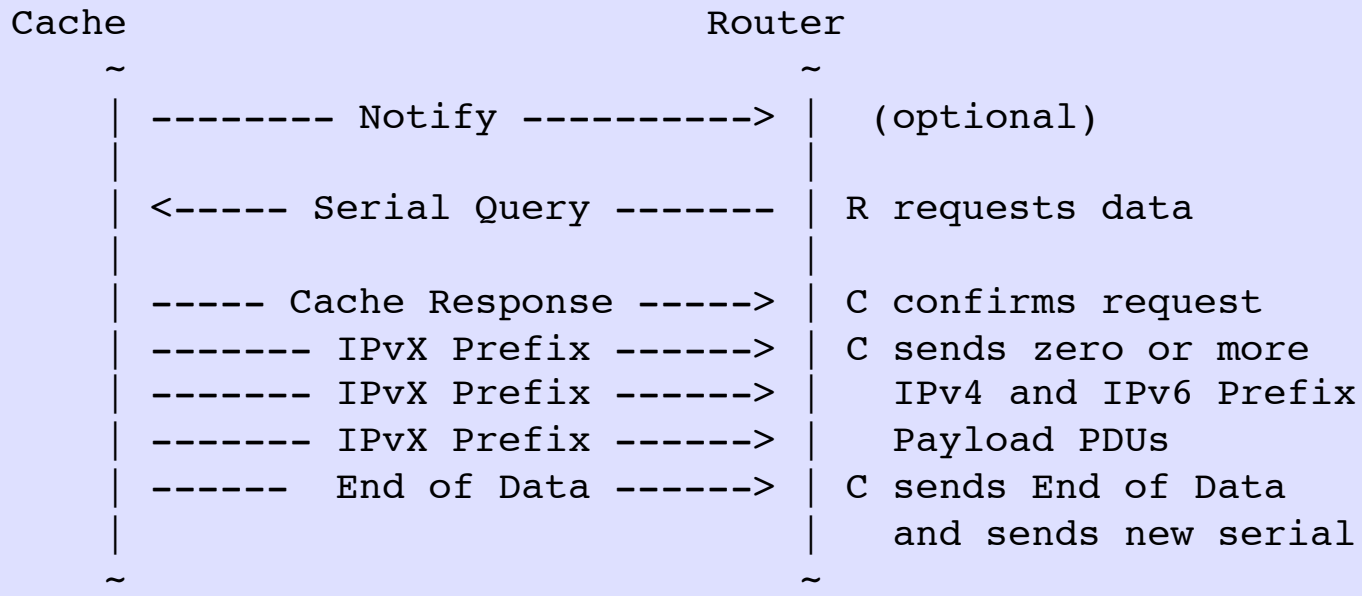

My Aggregate ROA
Customer ROAs
I Generate for
'Lazy' Customer
My Infrastructure
BGP Cust
Static (non BGP) Cust
Unused

RPKI -> Router

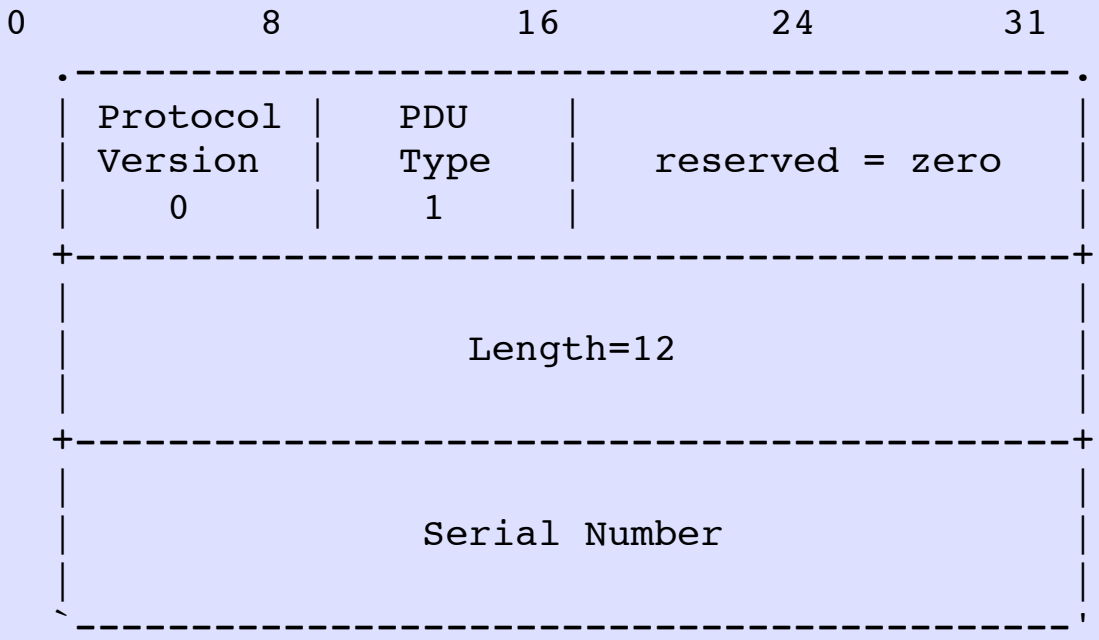
The Fourth Protocol (origin validation only)



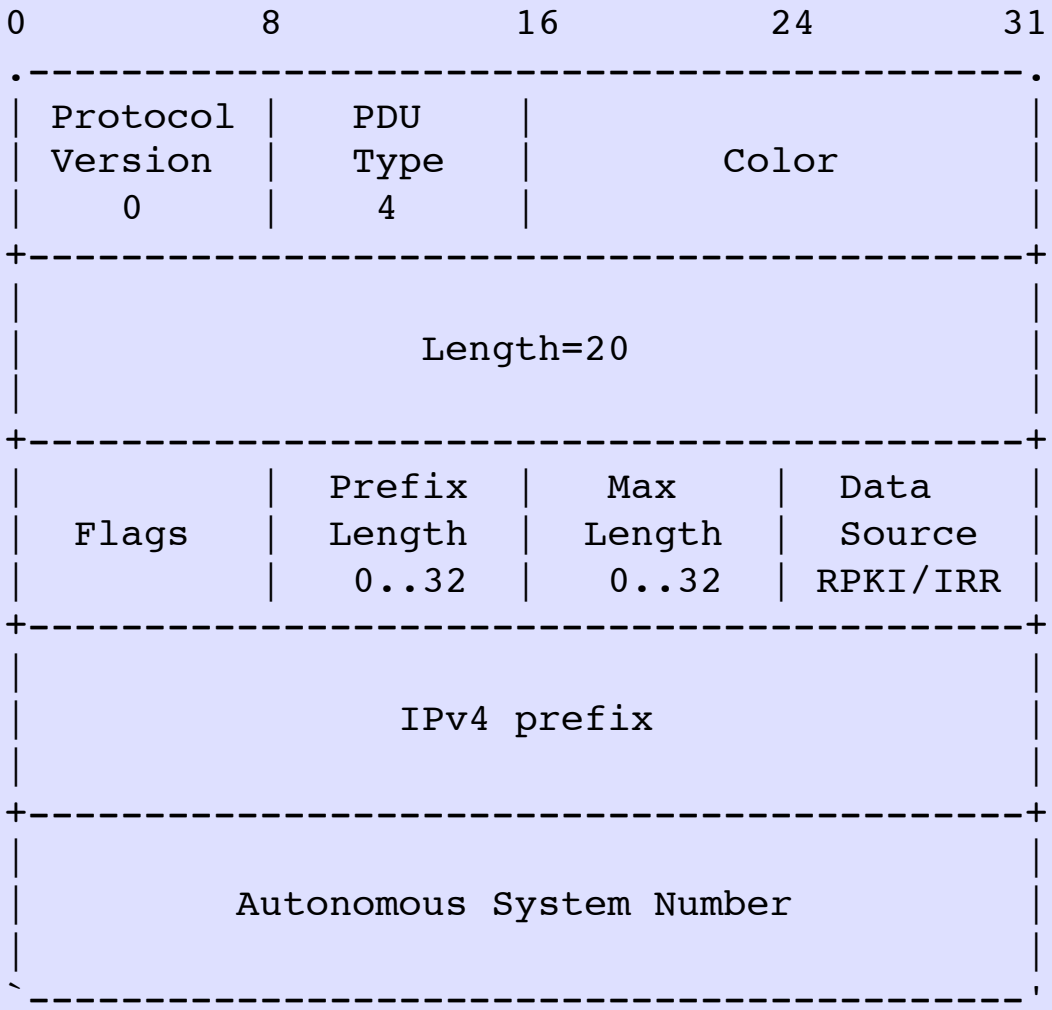
Typical Exchange



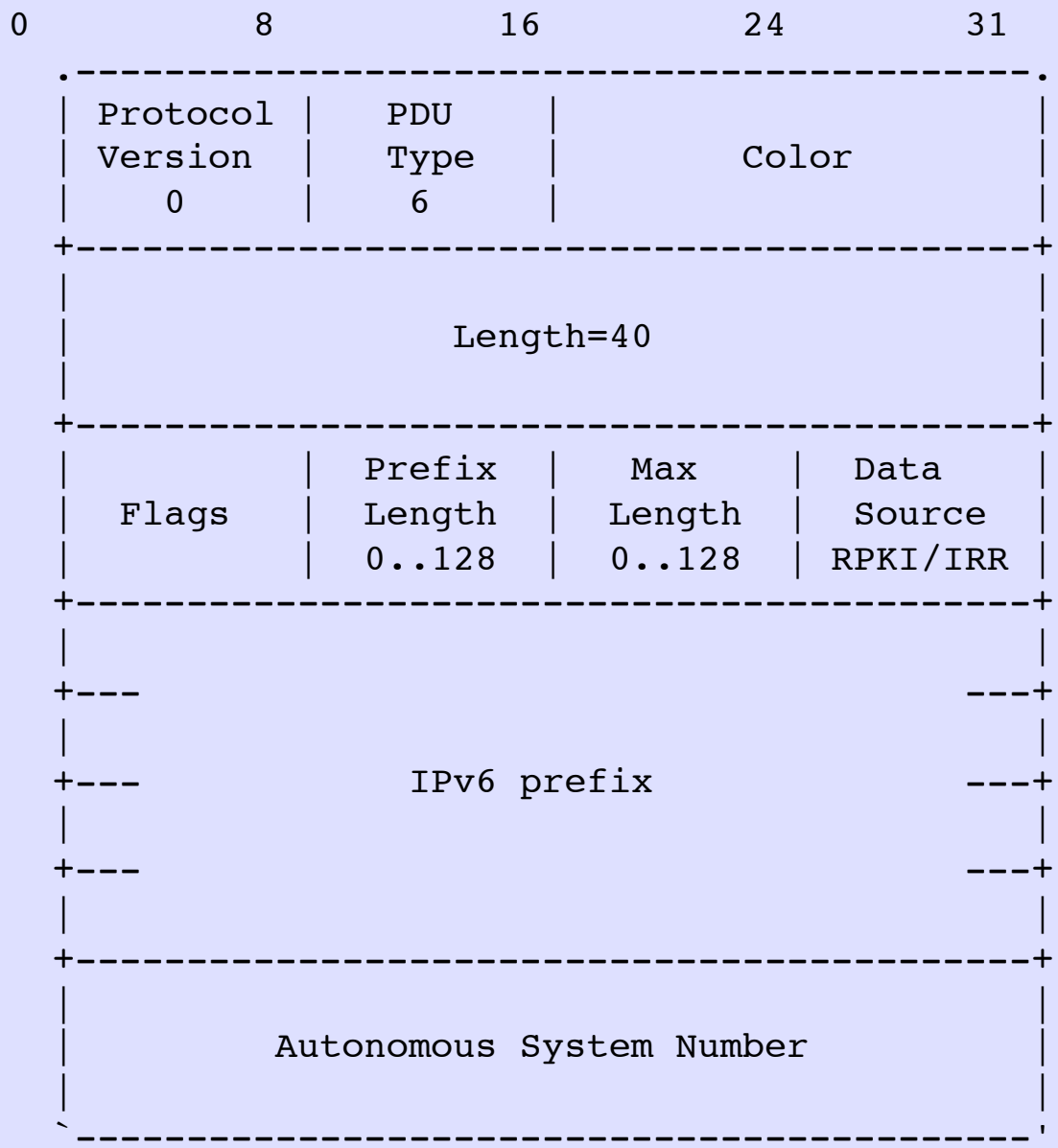
Serial Query



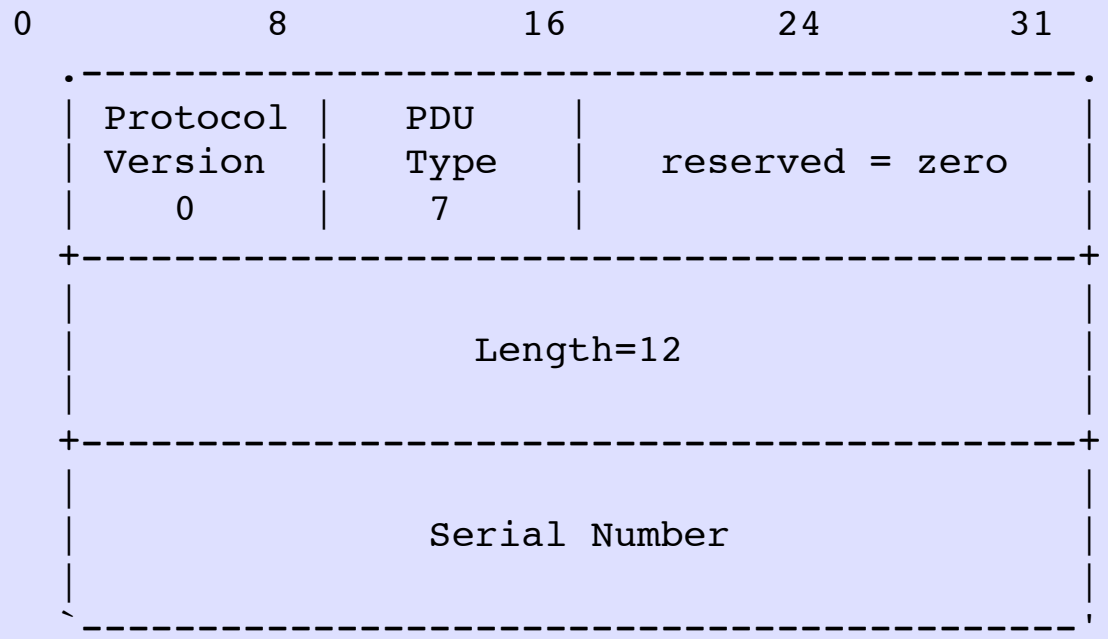
IPv4 Prefix


0
8
16
24
31
Protocol Version
0
PDU Type
4
Color
Length=20
Flags
Prefix Length
0..32
Max Length
0..32
Data Source
RPKI/IRR
IPv4 prefix
Autonomous System Number

IPv6 Prefix


0
8
16
24
31
Protocol Version 0
PDU Type 6
Color
Length=40
Flags
Prefix Length 0..128
Max Length 0..128
Data Source RPKI/IRR
IPv6 prefix
Autonomous System Number

End of Data


0
8
16
24
31
Protocol Version
0
PDU Type
7
reserved = zero
Length=12
Serial Number