

# The RPKI & Origin Validation

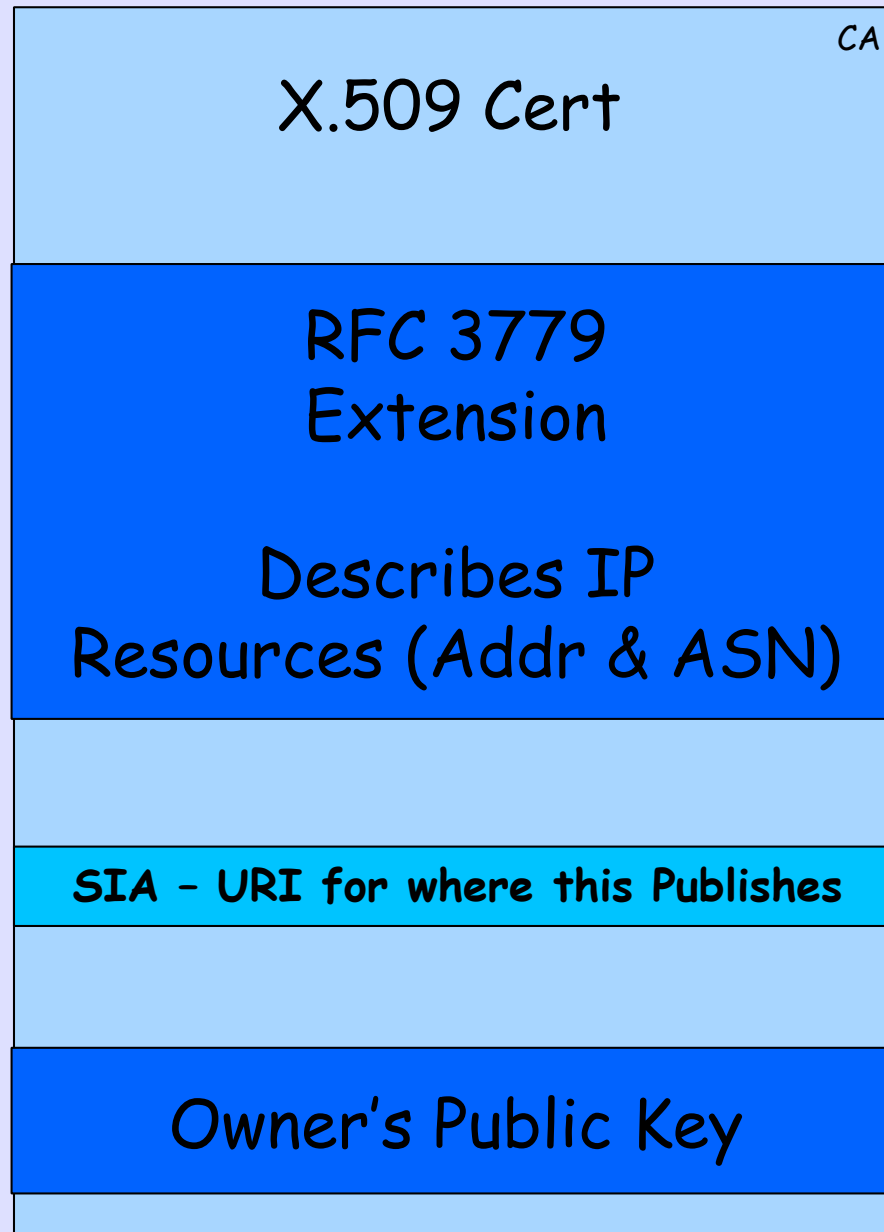
Joint Techs / Indianapolis  
2009.07.22

Randy Bush <randy@psg.com>

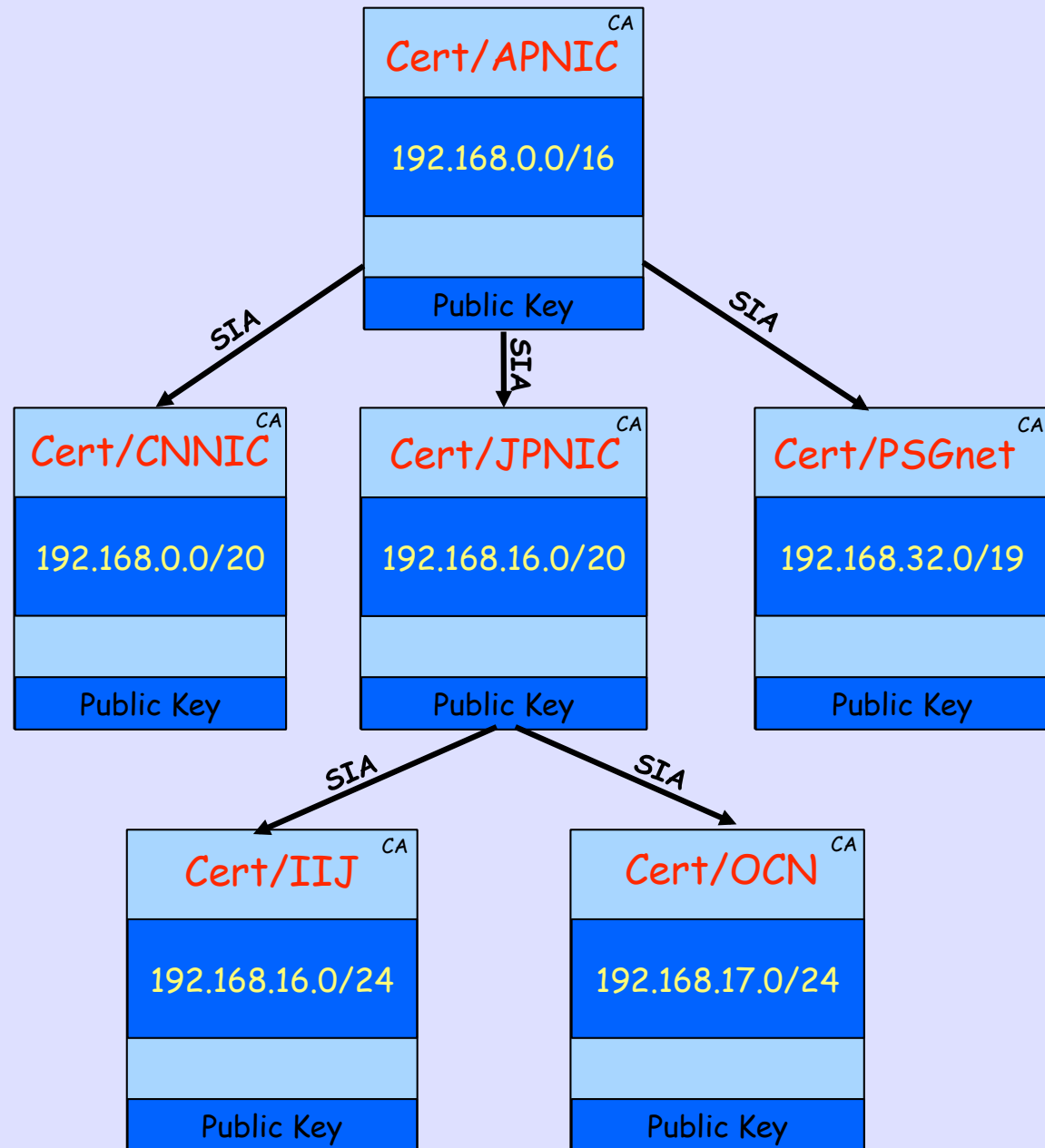
Rob Austein <sra@isc.org>

<<http://archive.psg.com/090722.jt-rpki.pdf>>

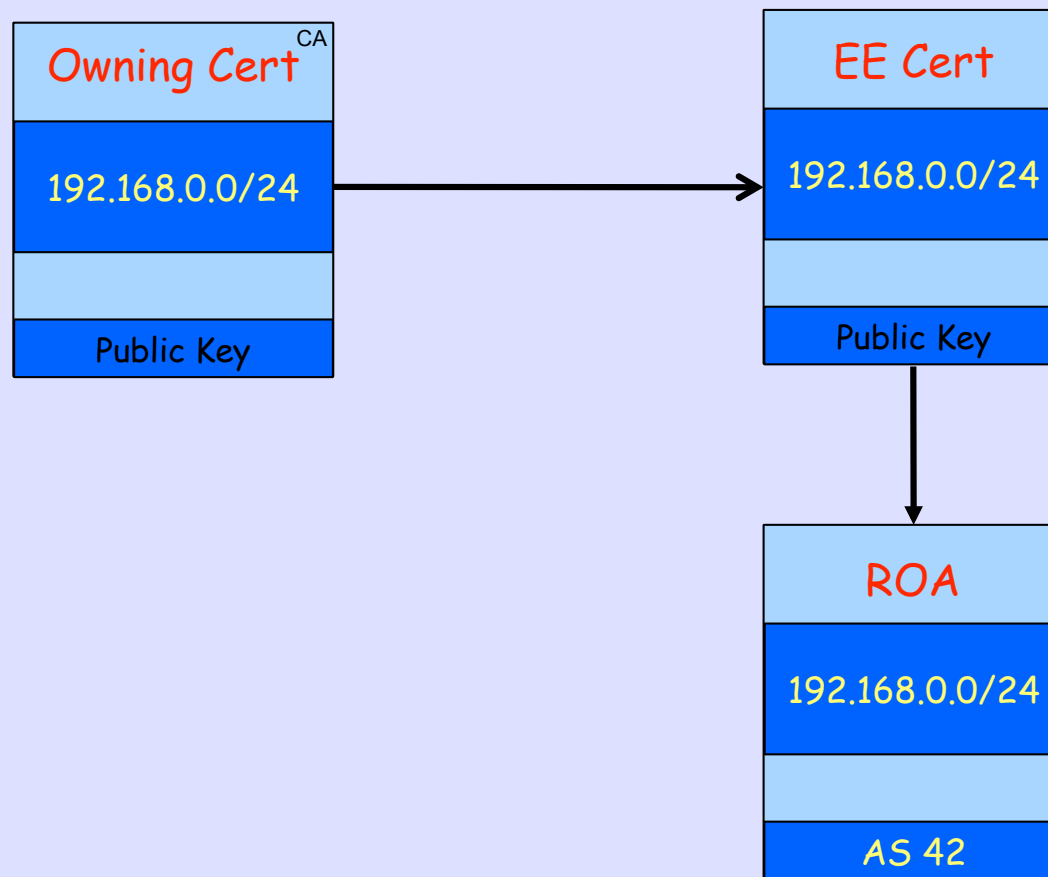
# X.509 Certificate w/ 3779 Ext



# Certificate Hierarchy follows Allocation Hierarchy



# Route Origin Authorization (ROA)

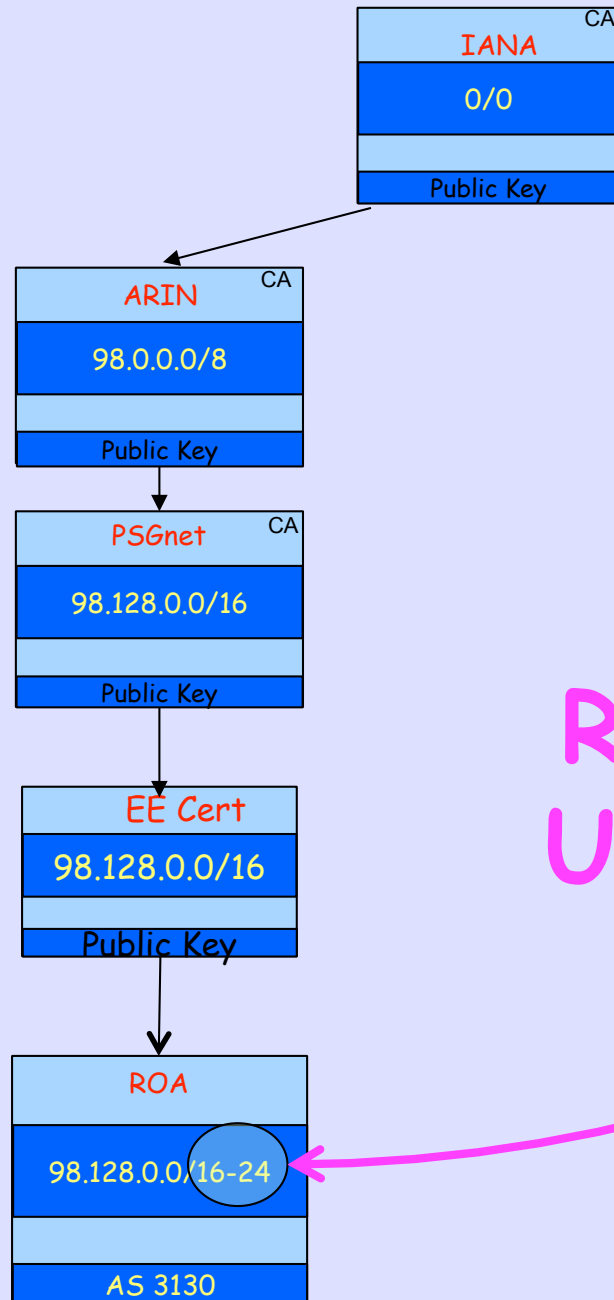


PSGnet /16  
Experimental  
Allocation  
from ARIN

Announces  
256 /24s



Too Many EE Certs and ROAs, Yucchhy!



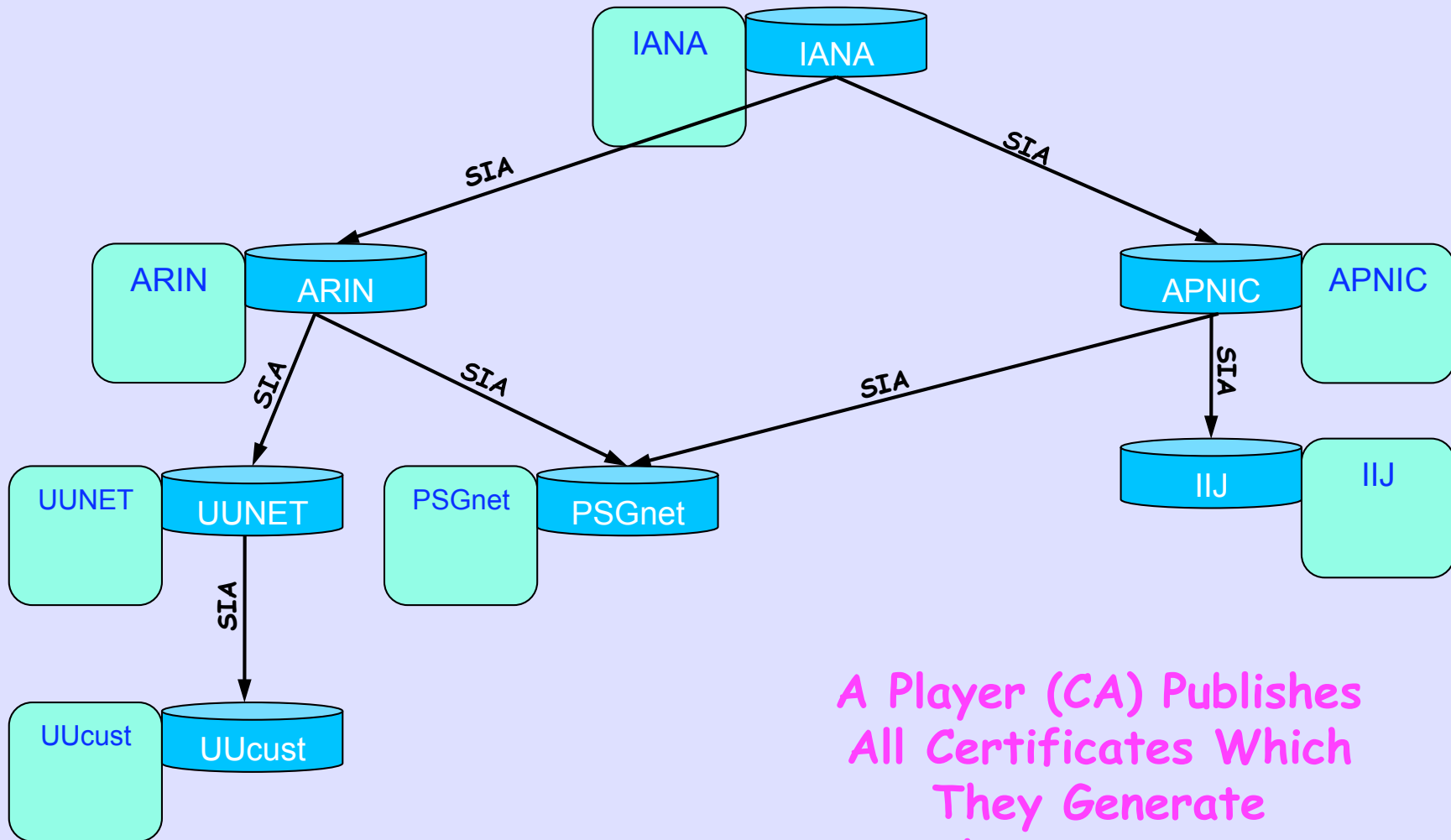
# ROA Aggregation Using Max Length

# Big, Centralized, & Scary We Don't Do This

**RPKI DataBase**

**IP Resource Certs  
ASN Resource Certs  
Route Origin Attestations**

# Distributed RPKI DataBase

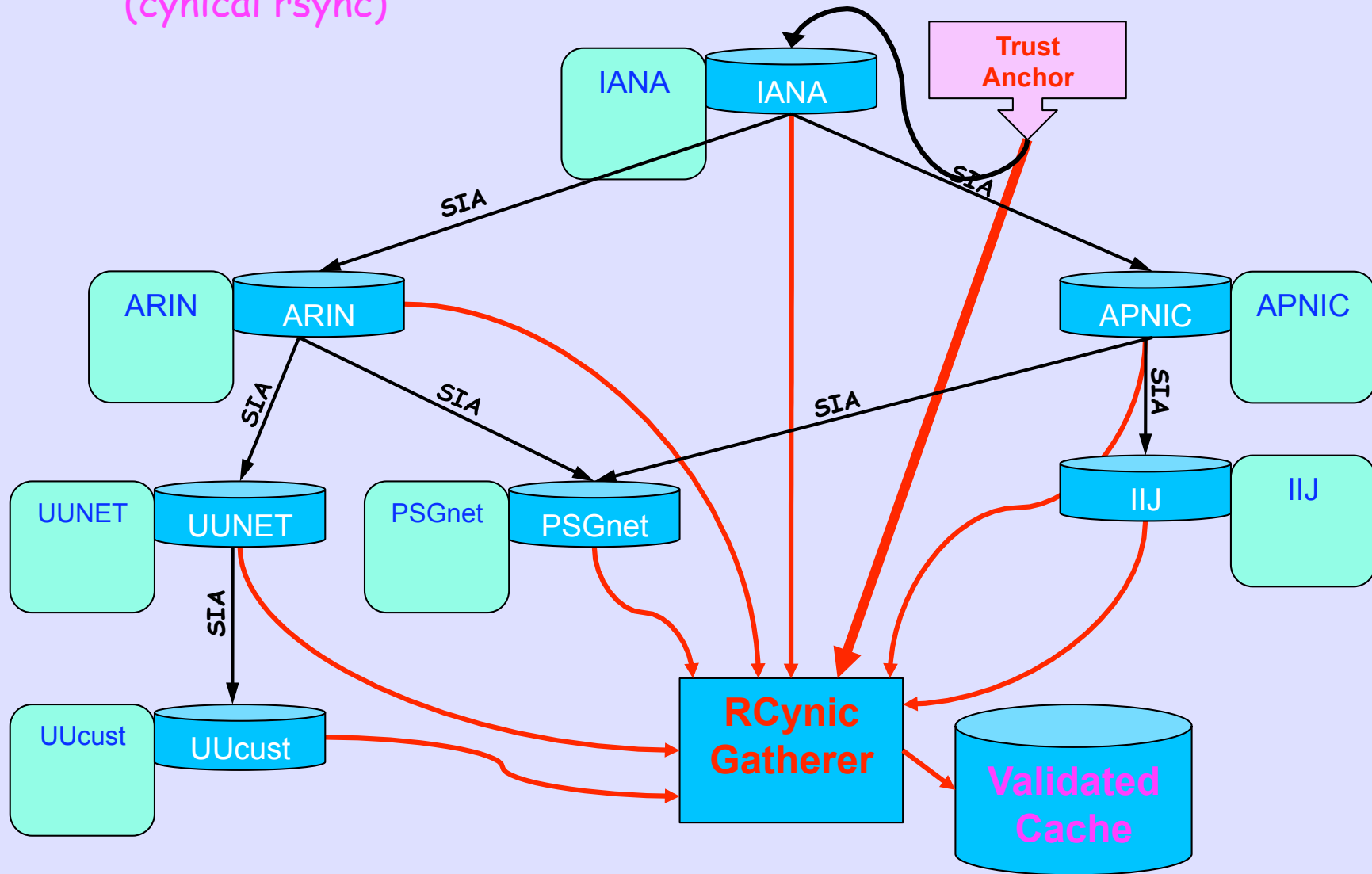


*A Player (CA) Publishes  
All Certificates Which  
They Generate  
in Their Own Unique  
Publication Point*

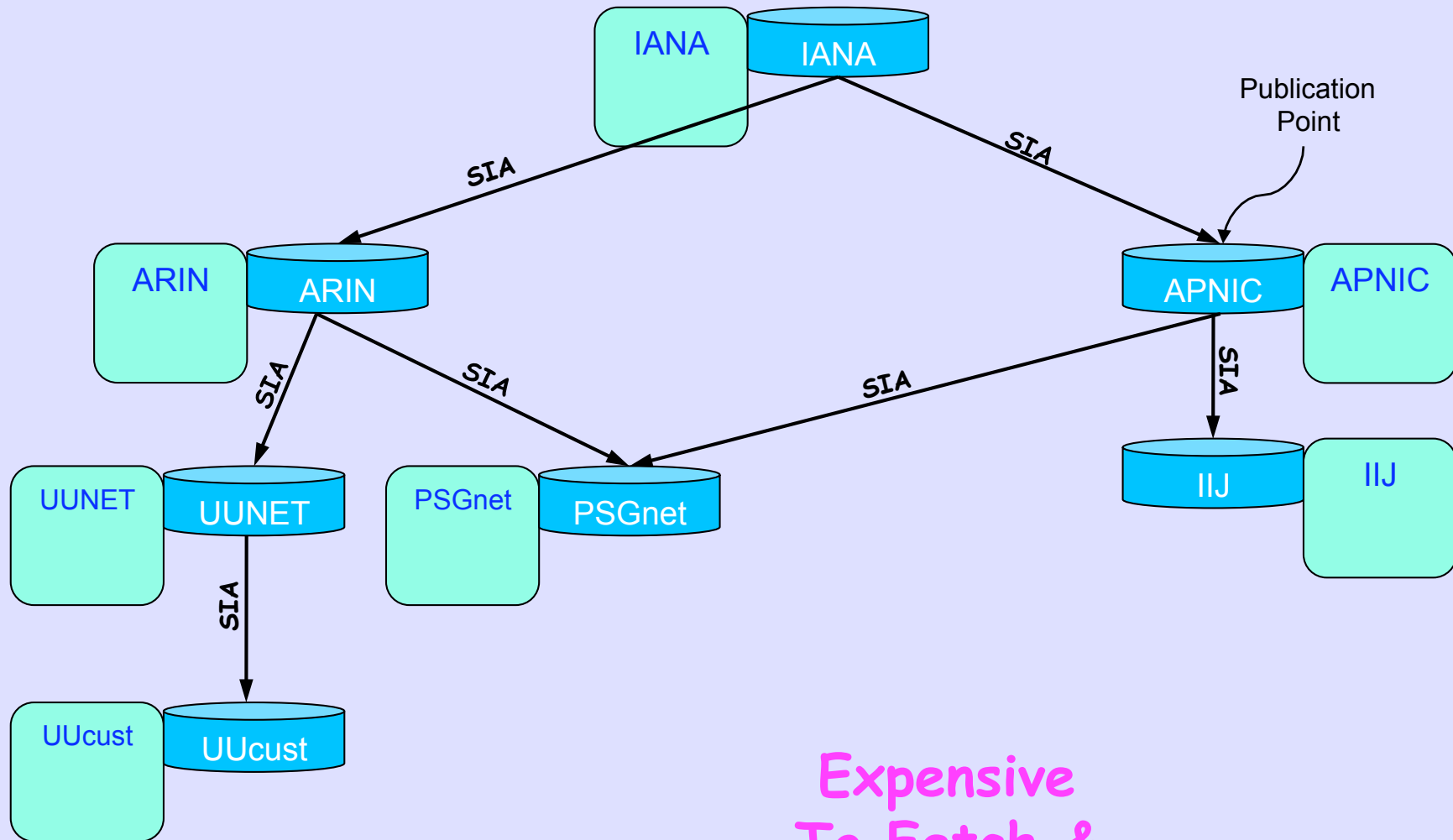


# RCynic Cache Gatherer

(cynical rsync)

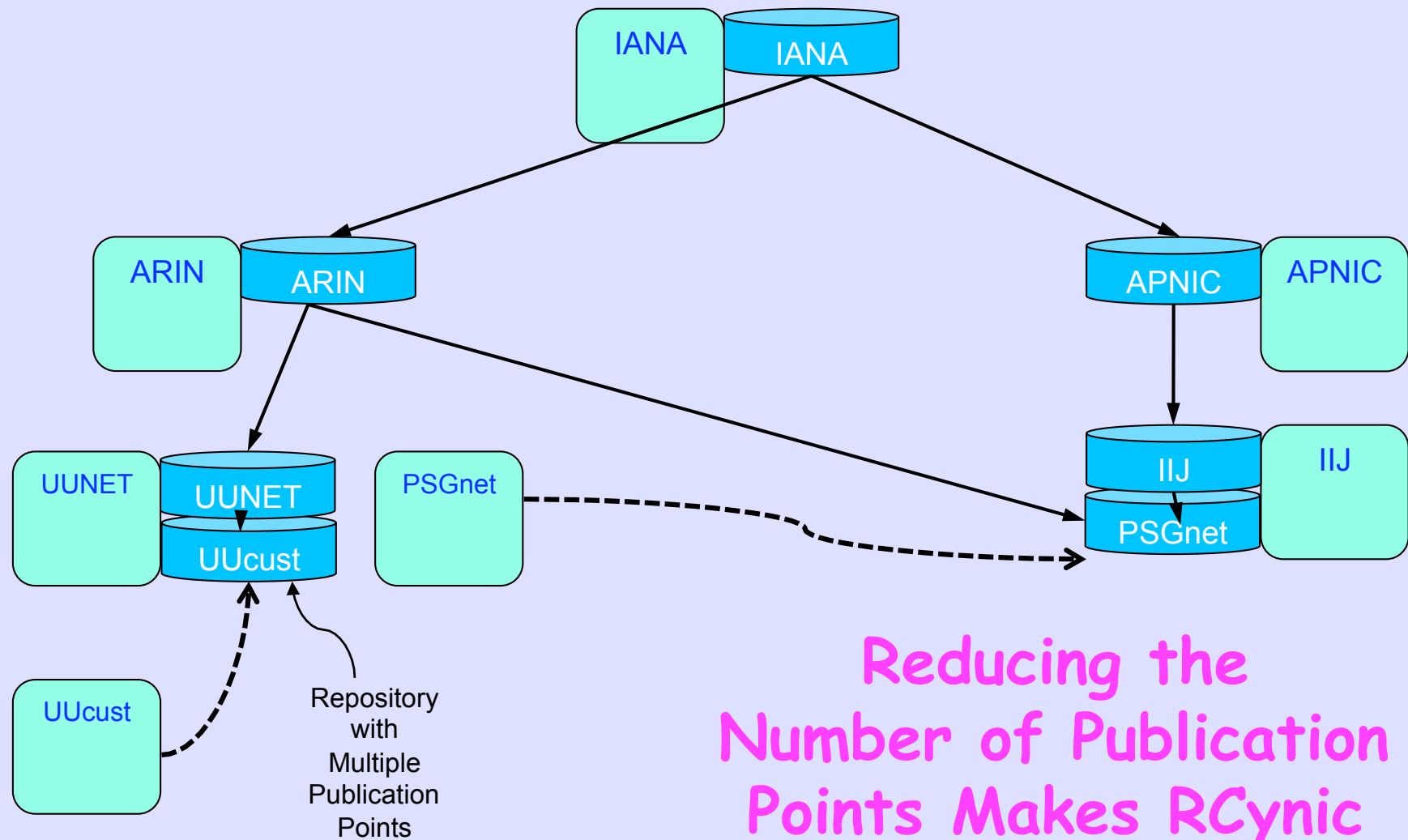


# Reliability Issue



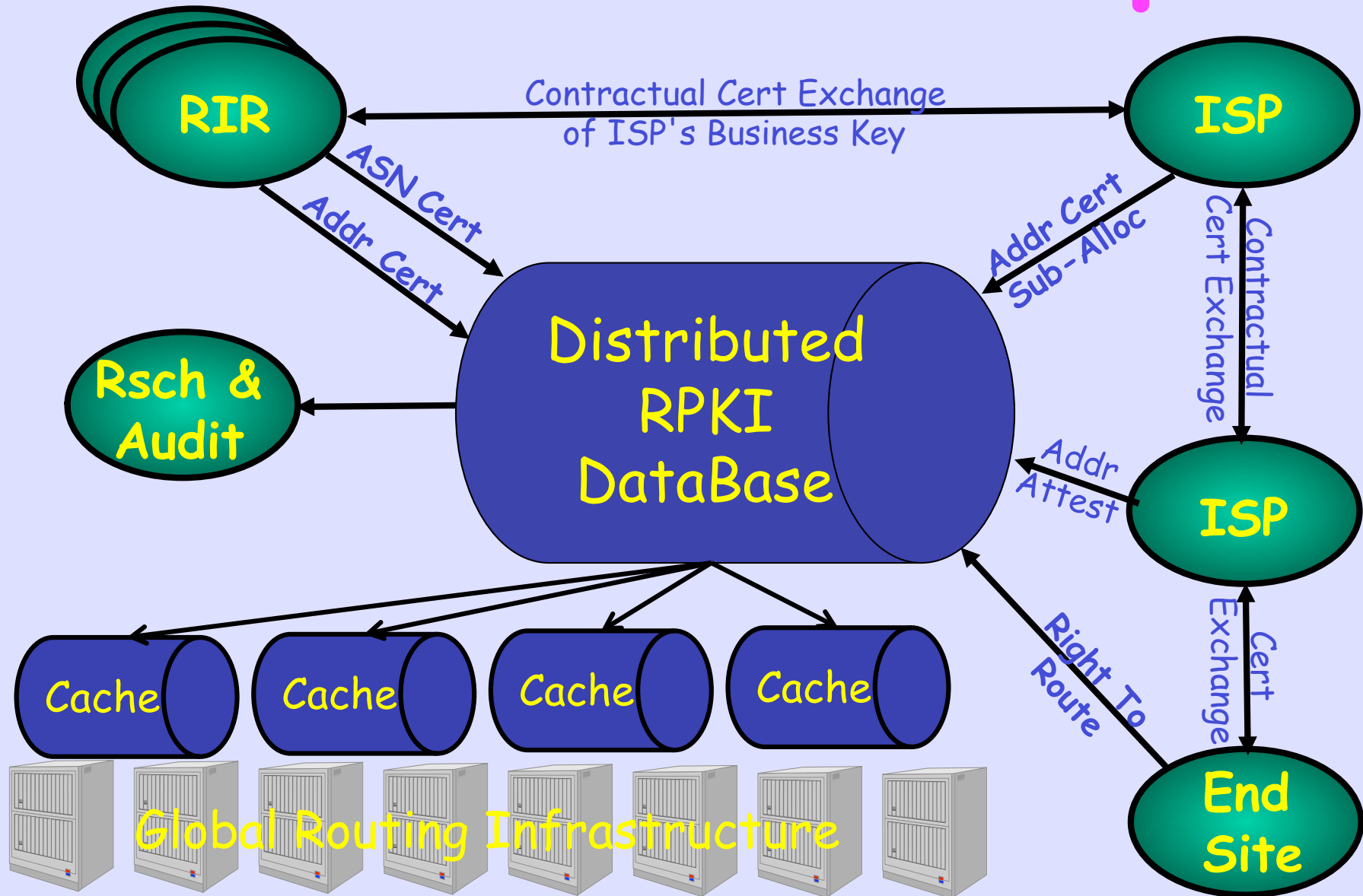
Expensive  
To Fetch &  
Unreliable

# Reliability Via Hosted Publication



Reducing the  
Number of Publication  
Points Makes RSync  
Much More Efficient

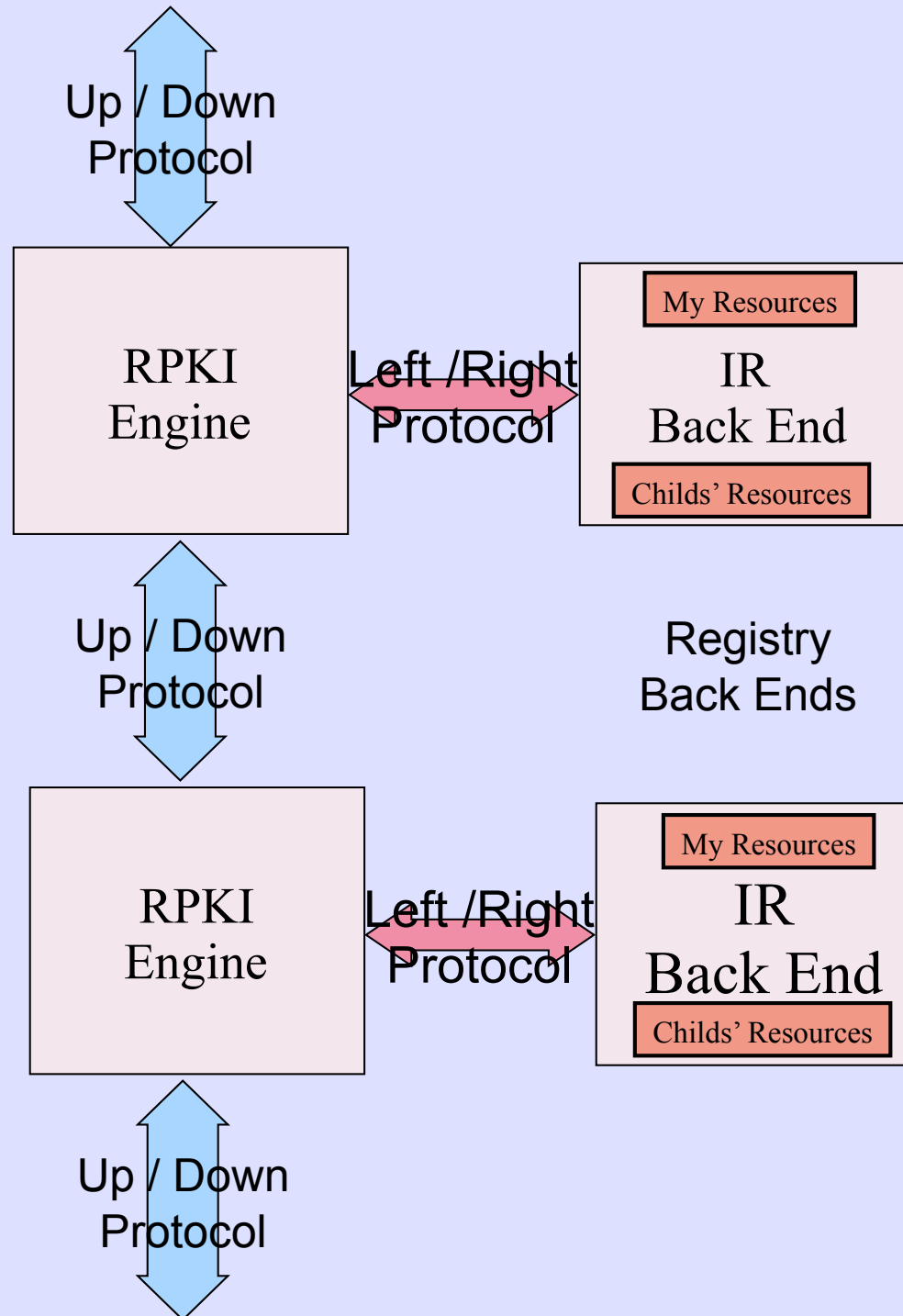
# RPKI Relationships



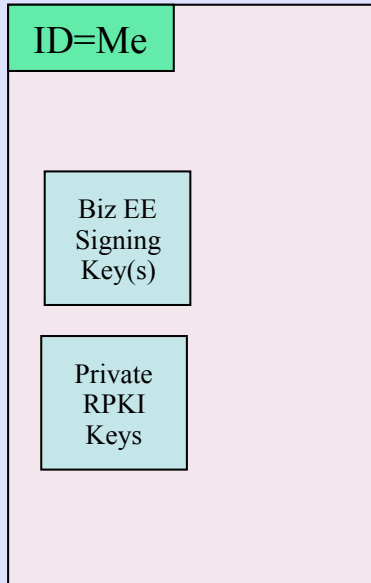
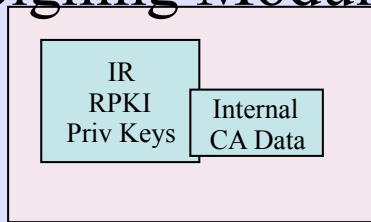
# Running Code

## And the Three RPKI Protocols

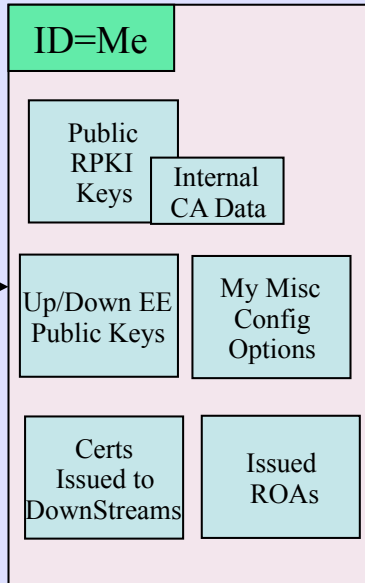
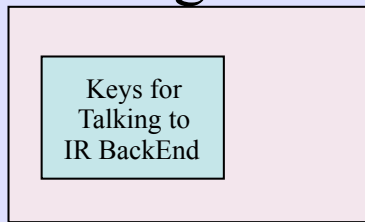
# Simple Parent and Simple Child



# [Hardware] Signing Module

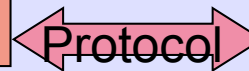
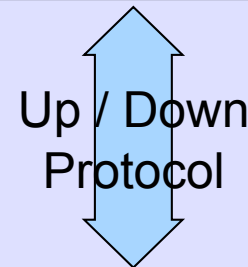
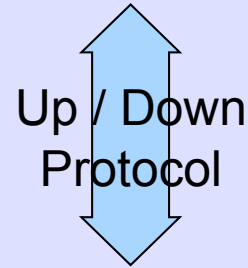
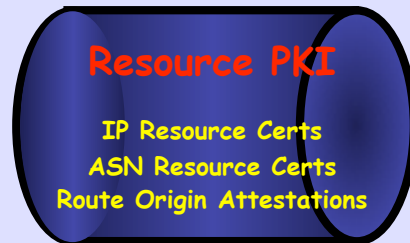


# RPKI Engine

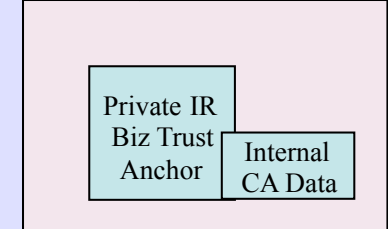
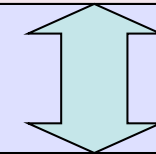
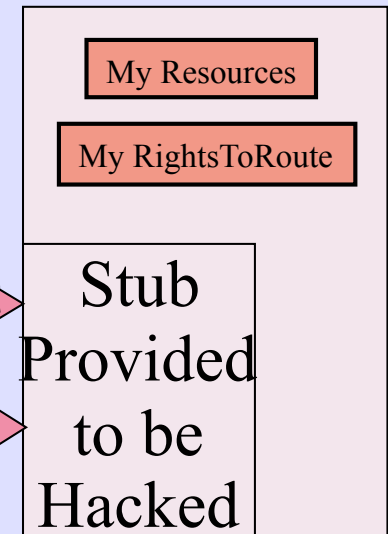


Publication Protocol

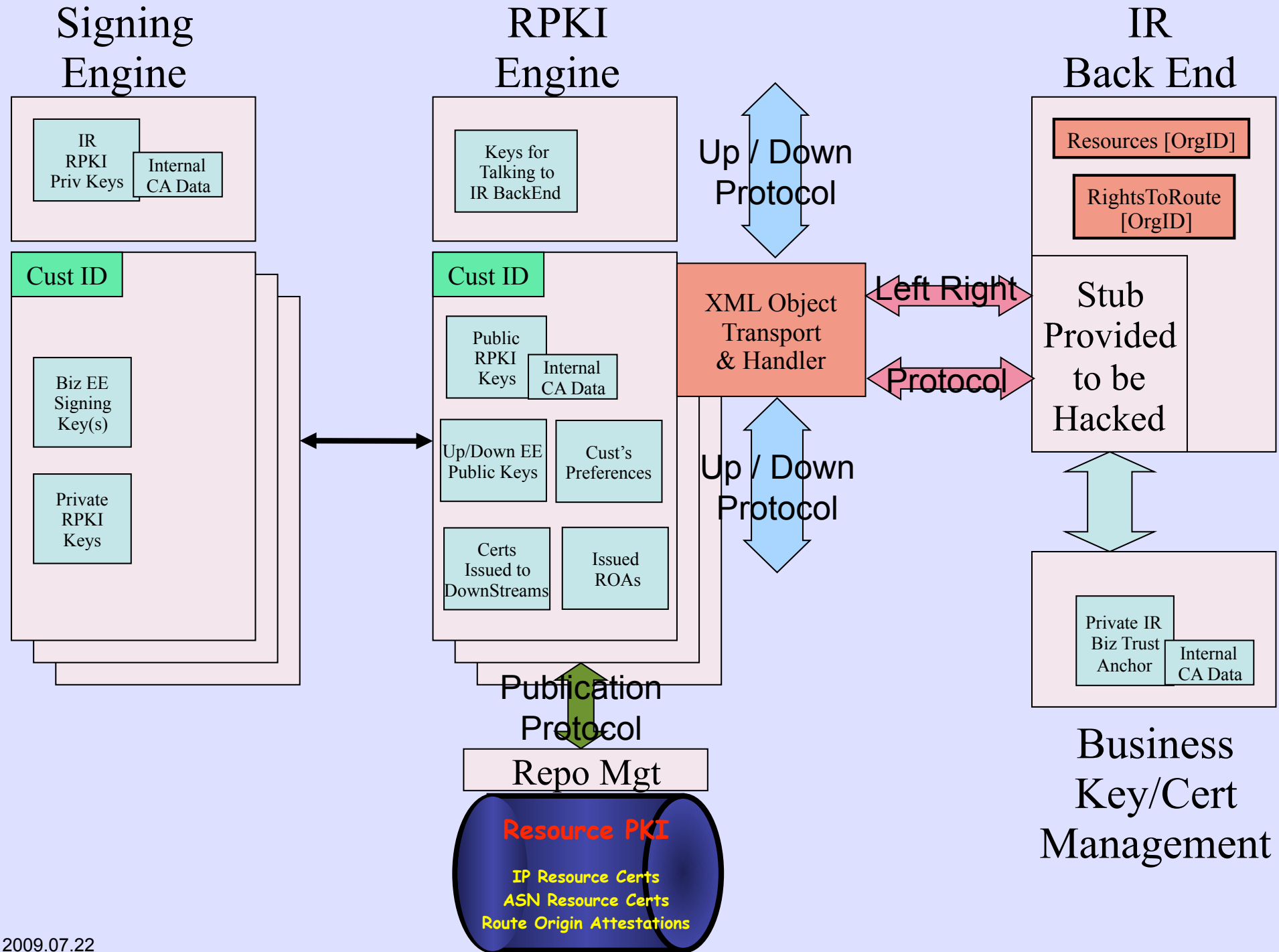
Repo Mgt



# IR Back End



Business Key/Cert Management



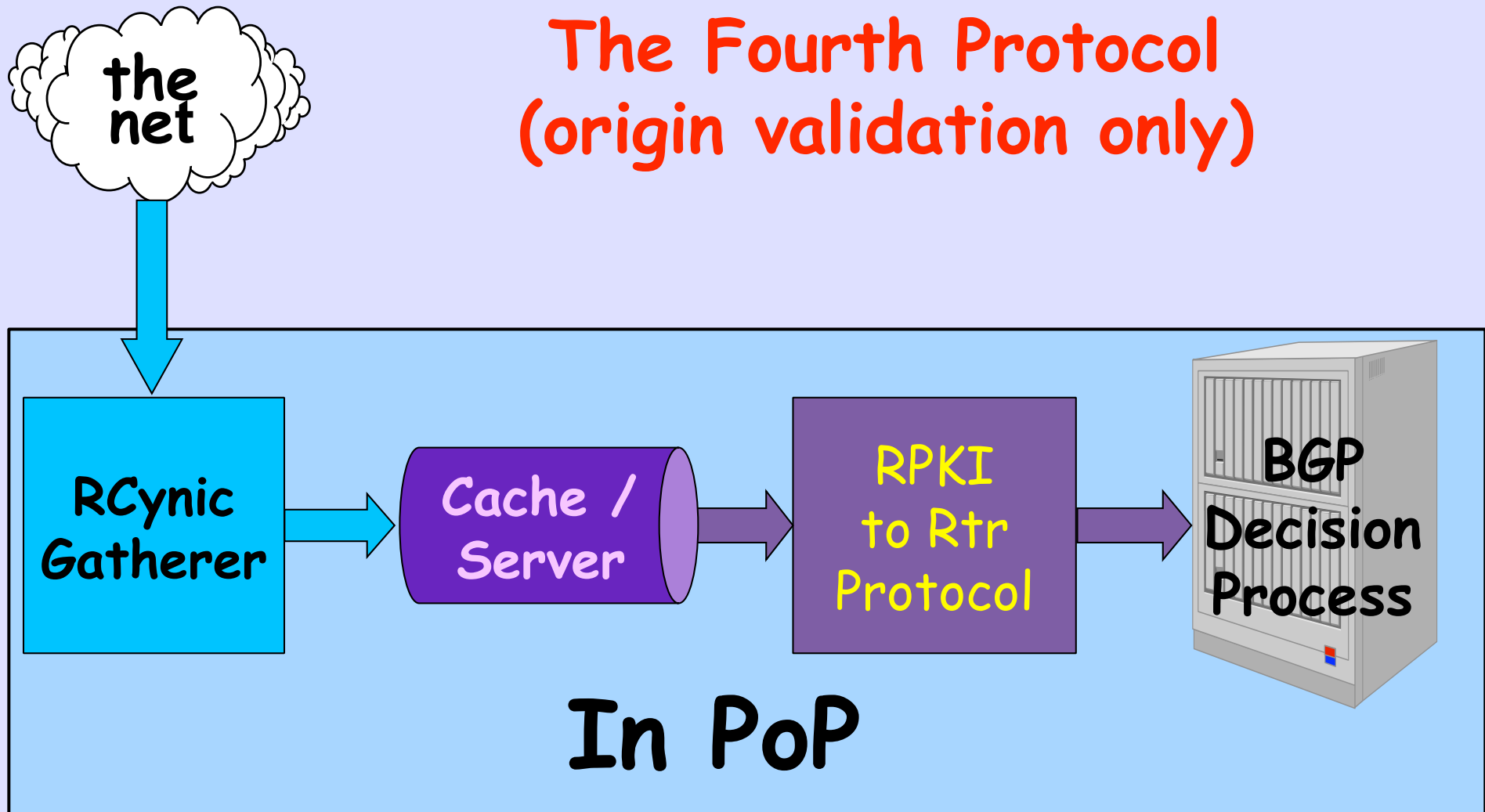


# Origin Validation

- 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

# RPKI -> Router

The Fourth Protocol  
(origin validation only)



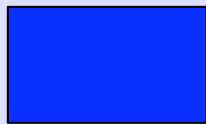
# Origin Only Validation

- Cisco has coded Origin Validation now
- We are exchanging clue with them
- We are doing research on estimation of compute and traffic loads
- Vendors will not do Path Validation if not first comfortable with Origin
- Need to get all vendors on board

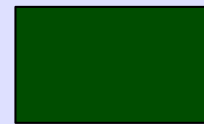
# The Contentious Bits

- Detestations / BOAs - assert that some space may not be announced by anyone
- This is not needed
- Root Trust Anchors - The RIRs demand independence from ICANN / DoC
- This is causing a technical kludge which is more open to error

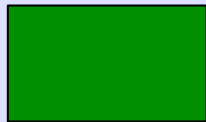
# Allocation in Reality



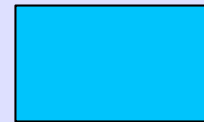
My Infrastructure



BGP Cust

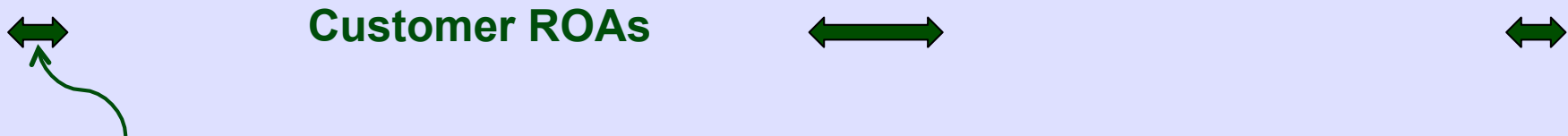


Static (non BGP) Cust



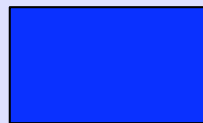
Unused

# ROA Use



Customer ROAs

I Generate for  
'Lazy' Customer



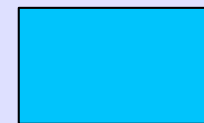
My Infrastructure



BGP Cust

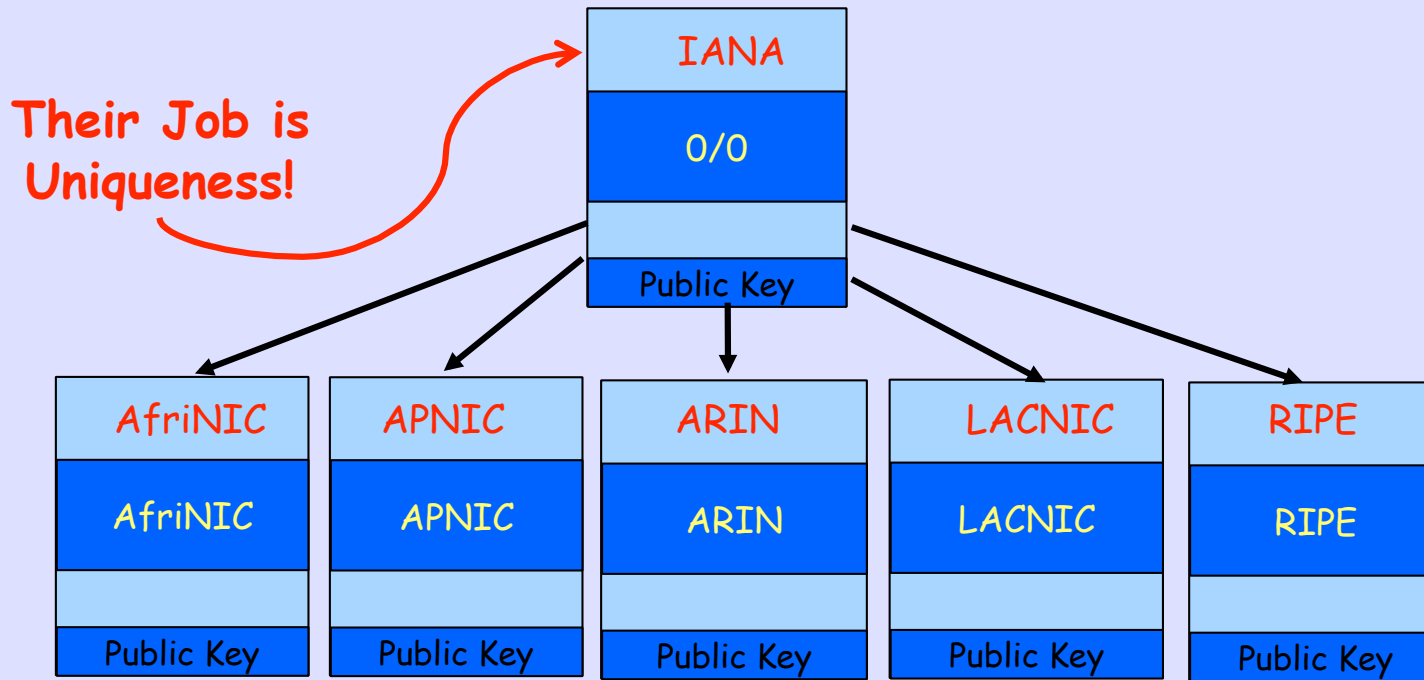


Static (non BGP) Cust

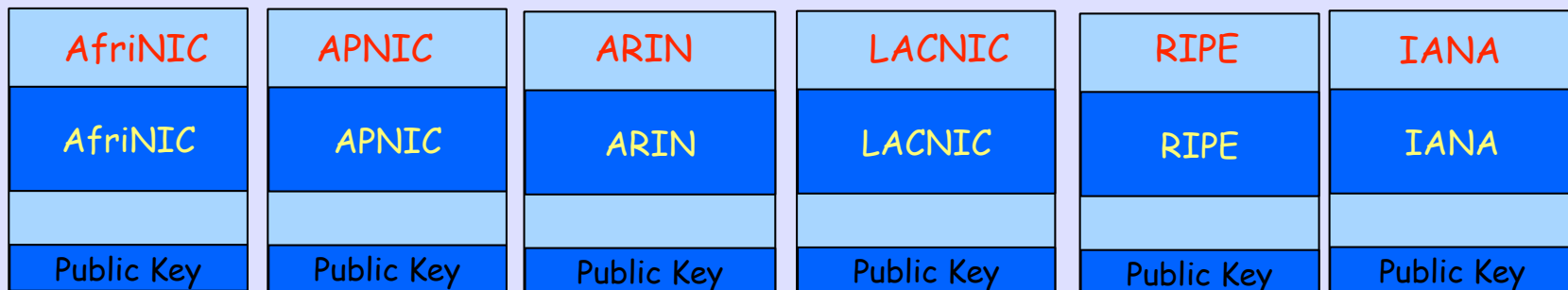


Unused

# Single Trust Anchor

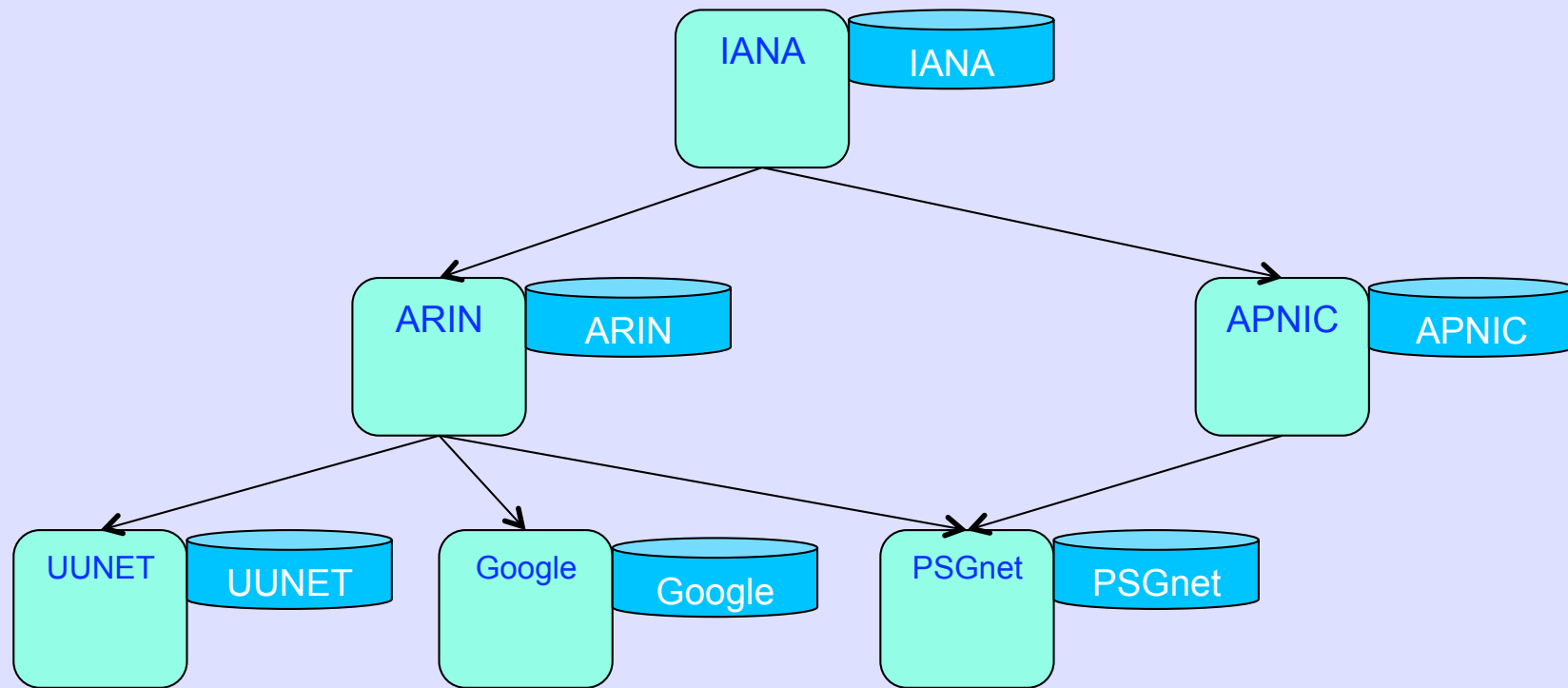


# Multiple Trust Anchors



Highly Vulnerable to Overlap and Gaps

# Test-Bed Start-Up





[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

Publication Protocol

Repo Mgt

**Resource PKI**

IP Resource Certs  
ASN Resource Certs  
Route Origin Attestations

Up / Down Protocol

XML Object Transport & Handler

Up / Down Protocol

Prototyping a Basic Back End

IR Back End

My Resources

My RightsToRoute

Stub Provided to be Hacked

Private IR Biz Trust Anchor Internal CA Data

Business Key/Cert Management

Left Right Protocol

# Work Supported By

- DHS / Sparta
- Internet Initiative Japan
- ARIN