Routing Security

Let's Get Serious

PLNOG / Kraków

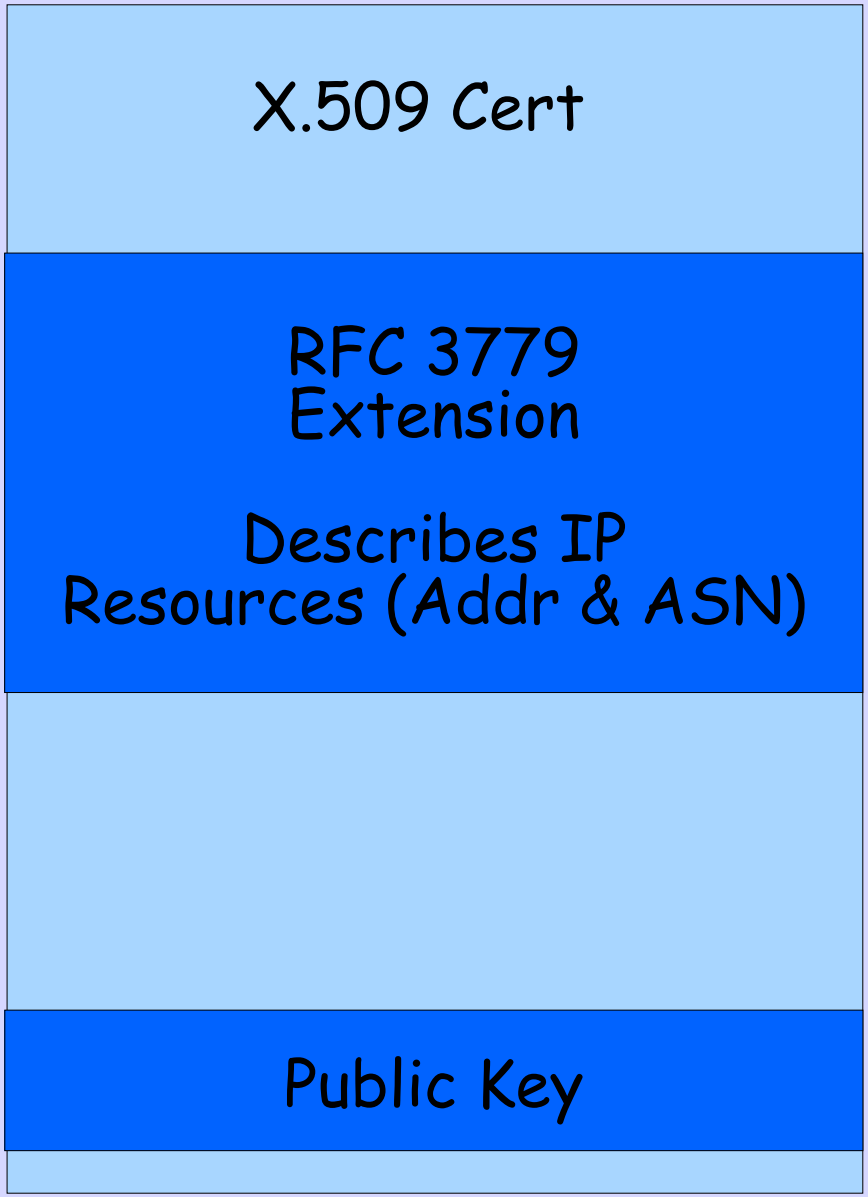
2008.09.18

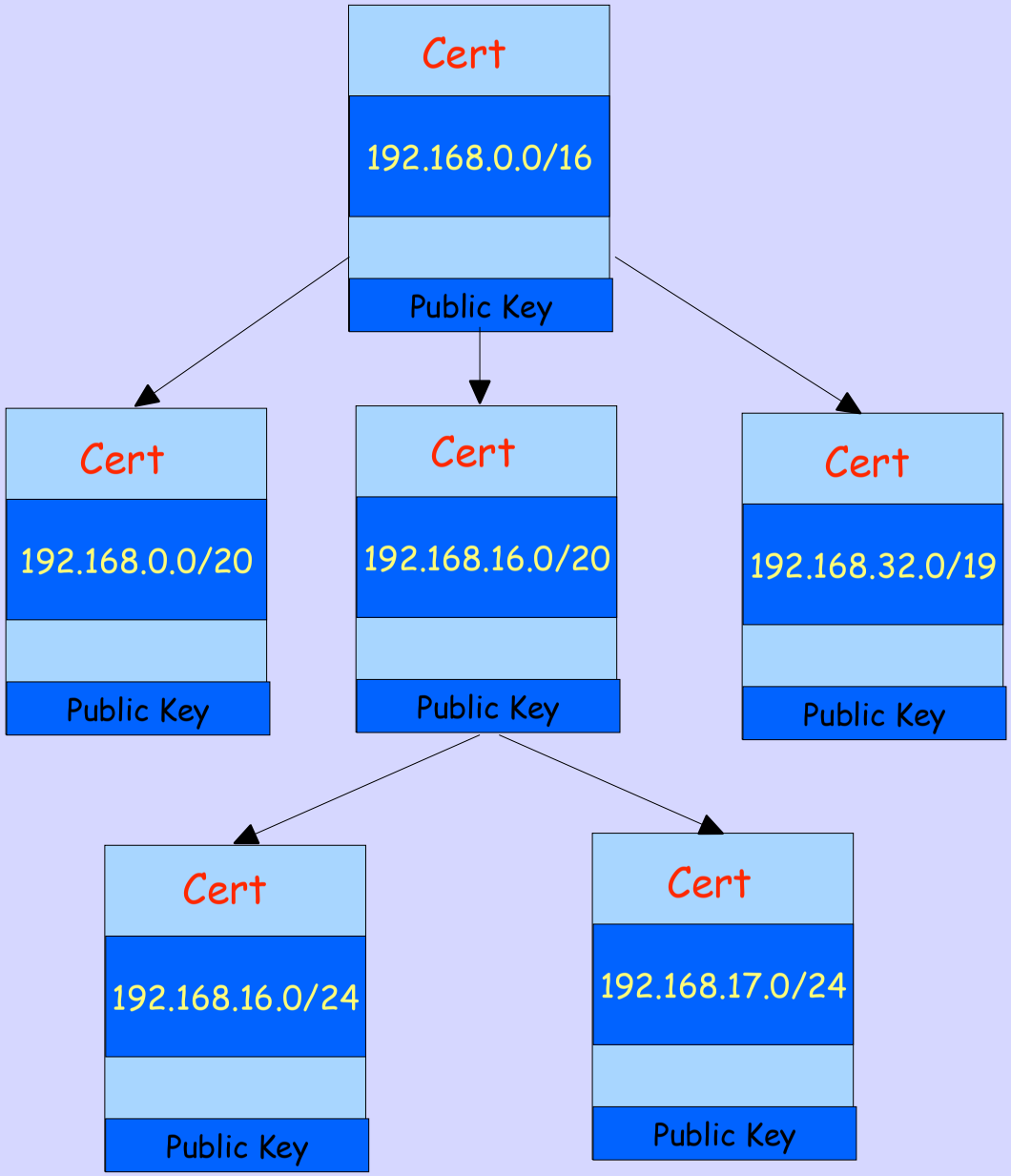
Randy Bush <randy@psg.com>

<http://archive.psg.com/080918.plnog-route-sec.pdf>

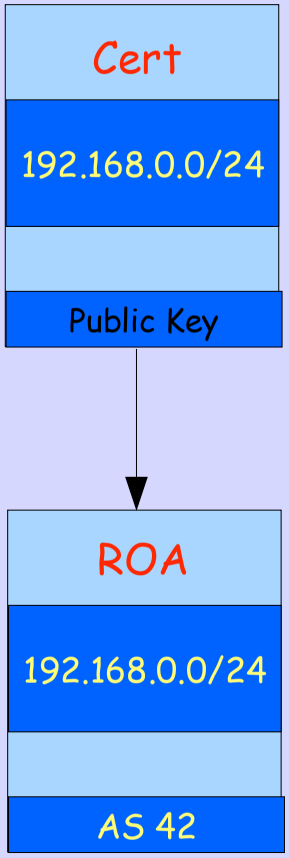
I have been working on this RPKI X.509 Certification of Resource Stuff

X.509 Cert w/ 3779

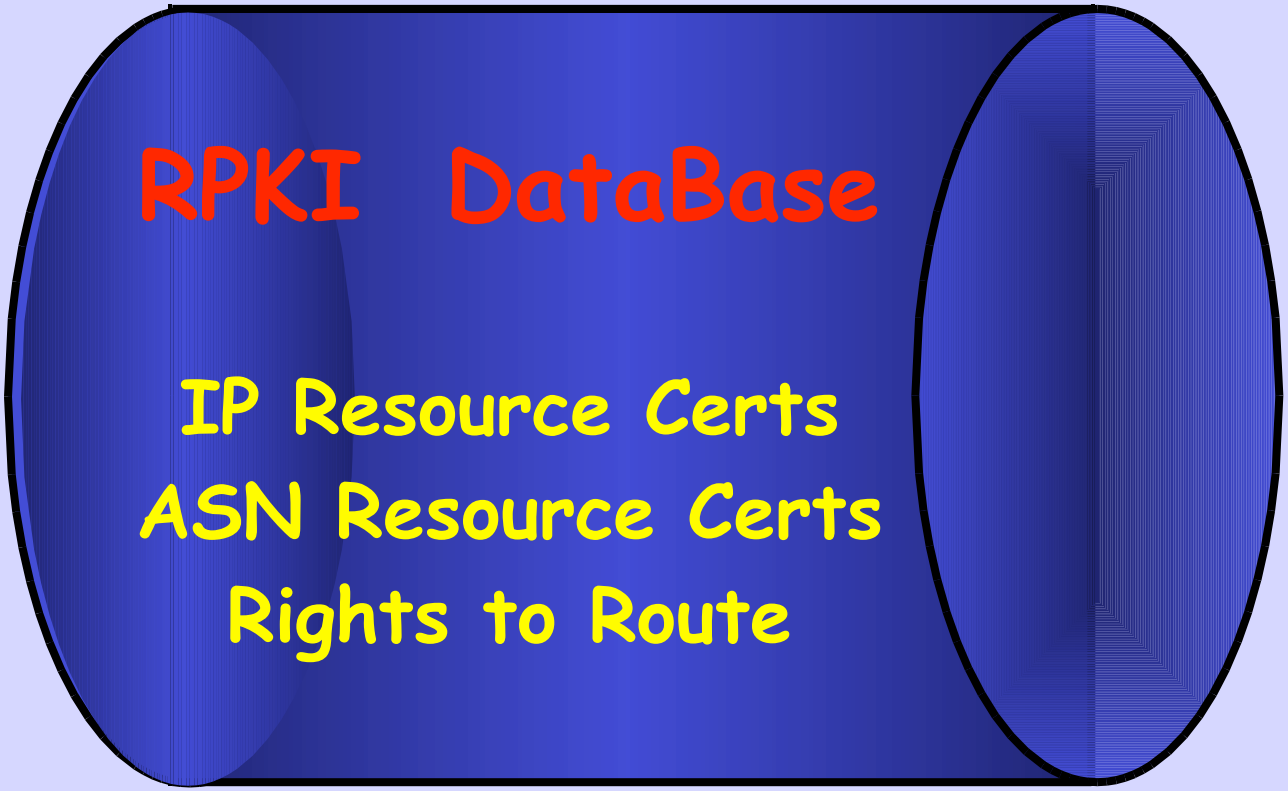


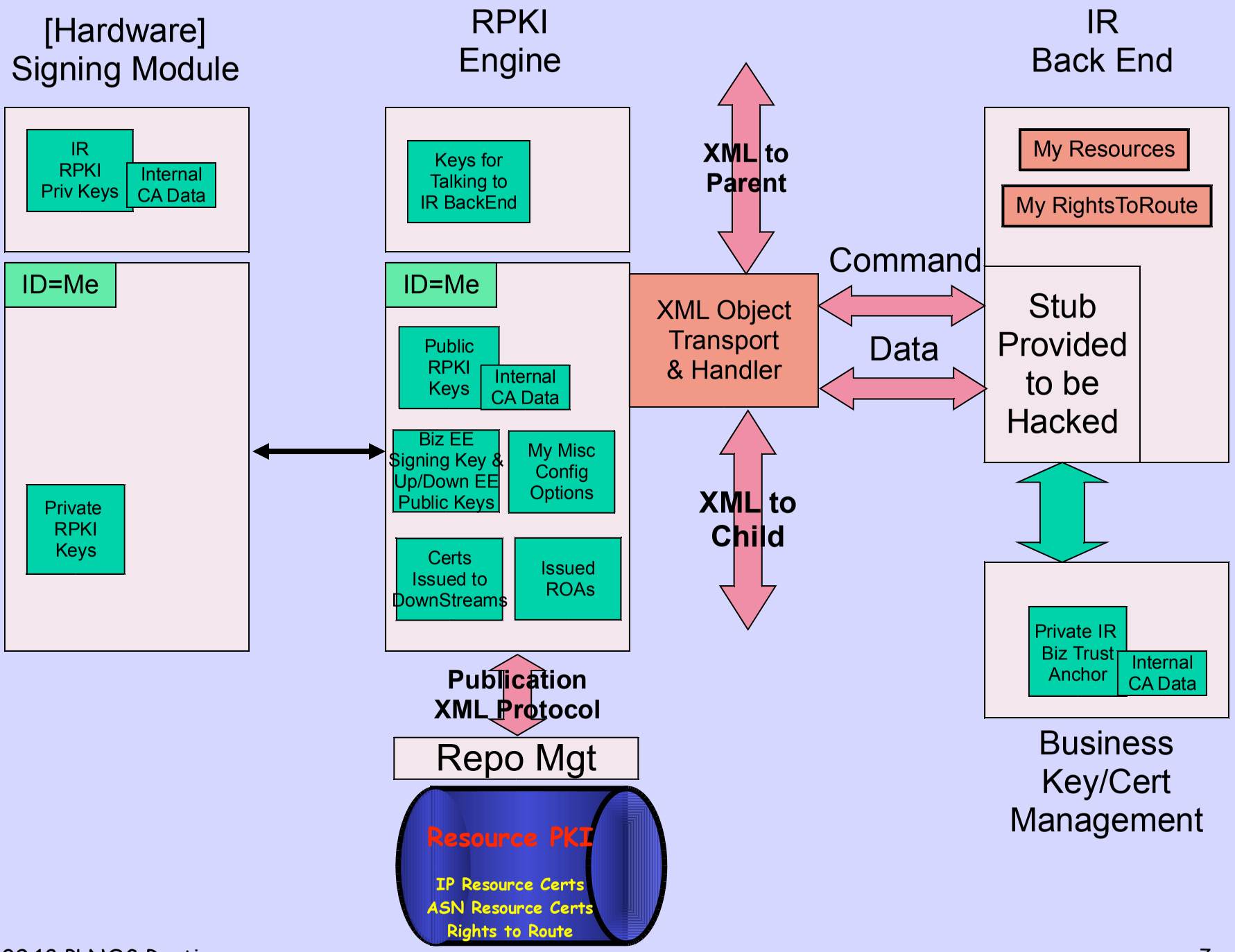

Cert
192.168.0.0/16
Public Key
Cert
192.168.0.0/20
Public Key
Cert
192.168.16.0/20
Public Key
Cert
192.168.32.0/19
Public Key
Cert
192.168.16.0/24
Public Key
Cert
192.168.17.0/24
Public Key

Route Origin Attestation (ROA)

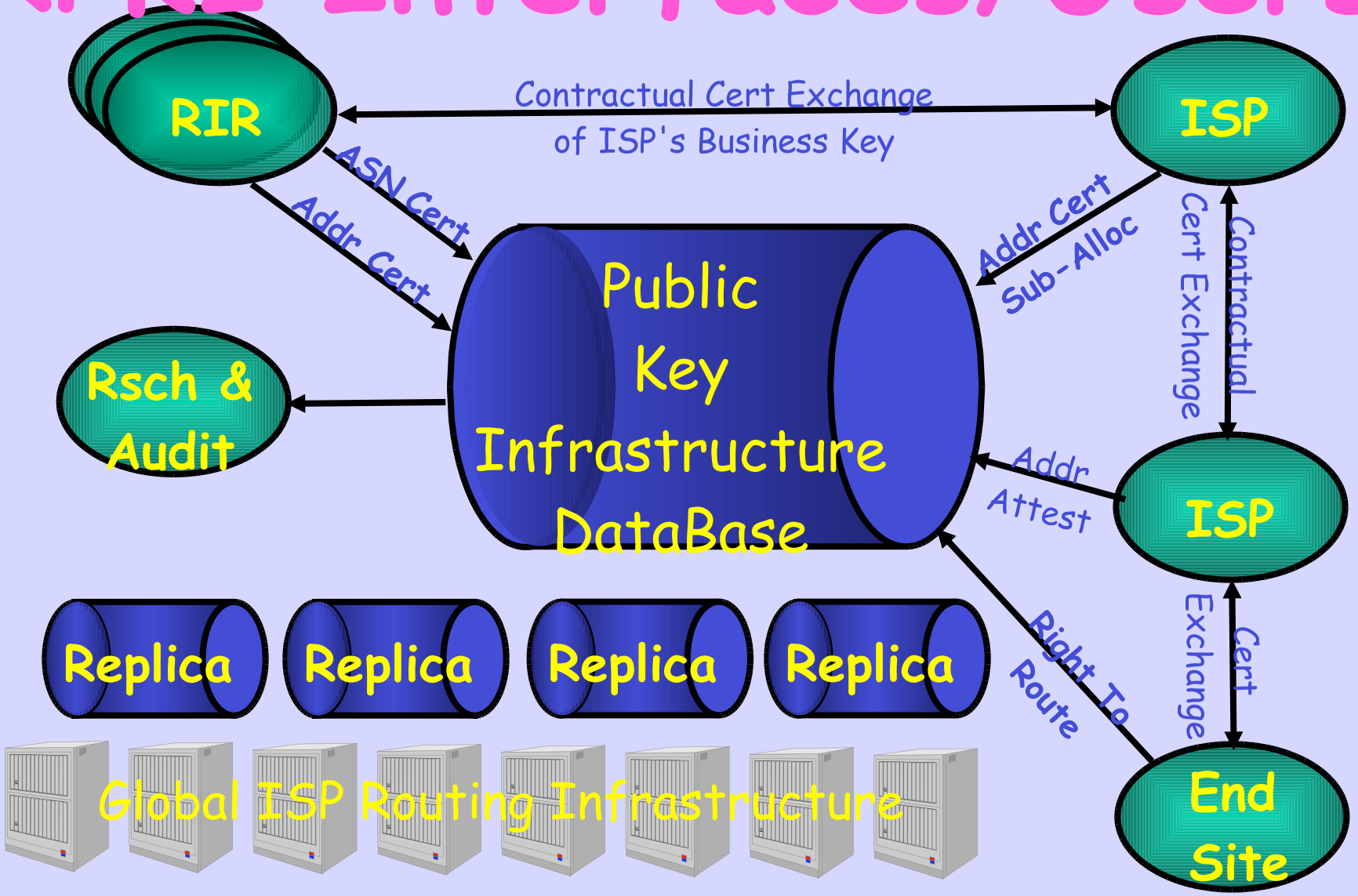


Resource Public Key Infrastructure




[Hardware]
Signing Module
RPKI
Engine
IR
Back End
IR
RPKI
Priv Keys
Internal
CA Data
Keys for
Talking to
IR BackEnd
My Resources
My RightsToRoute
XML to
Parent
Command
ID=Me
ID=Me
XML Object
Transport
& Handler
Data
Stub
Provided
to be
Hacked
Public
RPKI
Keys
Internal
CA Data
Biz EE
Signing Key &
Up/Down EE
Public Keys
My Misc
Config
Options
Private
RPKI
Keys
XML to
Child
Certs
Issued to
DownStreams
Issued
ROAs
Private IR
Biz Trust
Anchor
Internal
CA Data
Publication
XML Protocol
Repo Mgt
Business
Key/Cert
Management
Resource PKI
IP Resource Certs
ASN Resource Certs
Rights to Route

RPKI Interfaces/Users



Implementations

- APNIC Up/Down only, and no intent to deal with hosting hierarchy below them
- RIPE, ARIN, and others deciding
- Lack of Left-Right not a big issue as it only inhibits software independence
- Lack of Publication Protocol forces RIR repository on the members

Why Do I Care?

- Formal validation of who can ask me to route what prefixes
- Automation of route filters
- Real routing security in the long term
- Fairness in address trading

Cheap Filter Automation

- This is Ruediger's epiphany, not mine
- Use ROAs to generate a fake IRR of Route: objects
- Put this ersatz-IRR in front of the other IRRs when running peval()
- A lot of benefit at zero RPSL or software change!

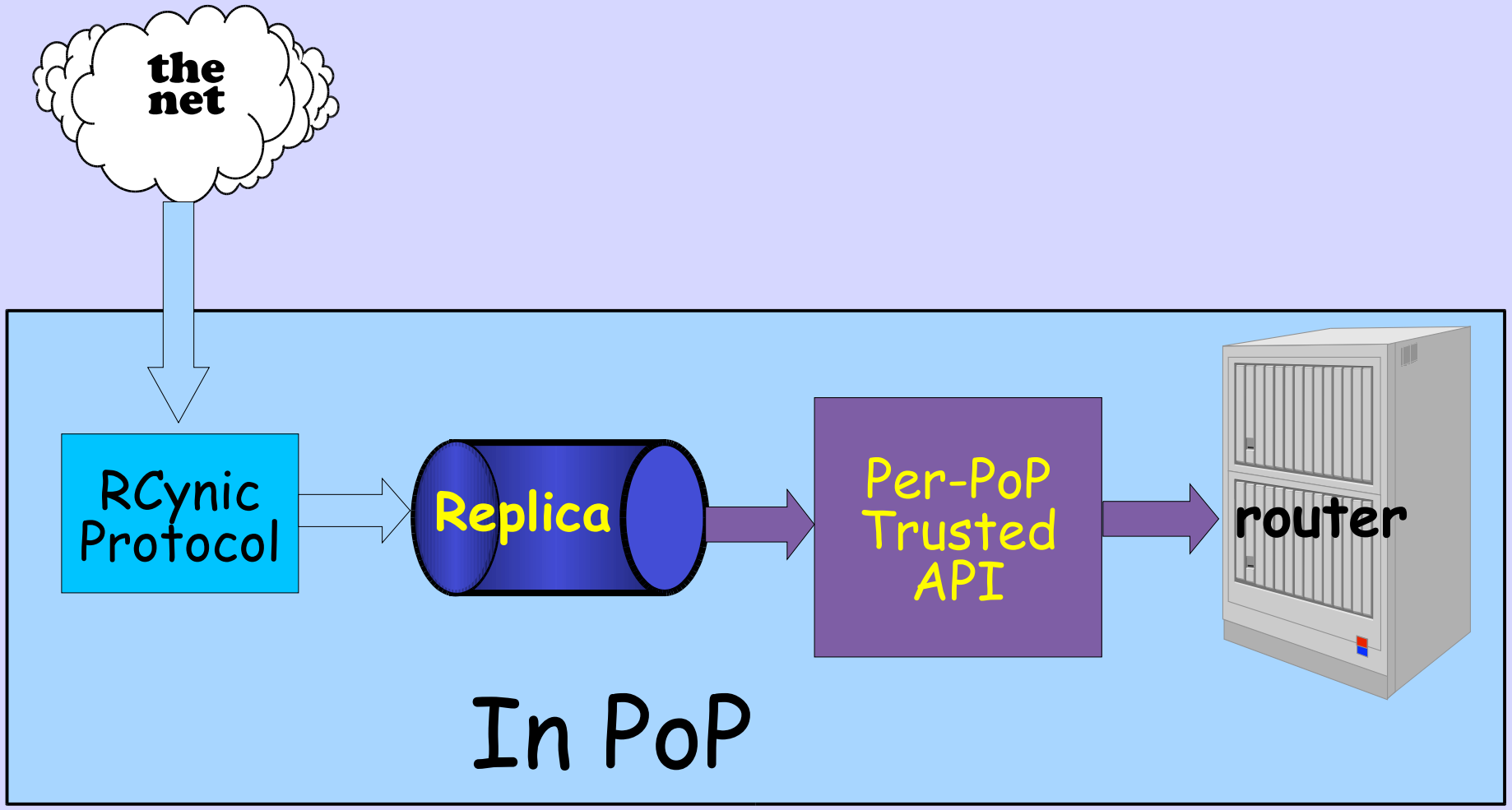
Where I am really going in the long term is

BGP Routing Security

Origin-only Validation

- A vendor is willing to do, & is starting
  - We are passing clue to them
  - We are doing research on estimation of compute and traffic loads
- Will not do Path Validation if not first comfortable with Origin
- Need to get all vendors on board

RPKI / Router API



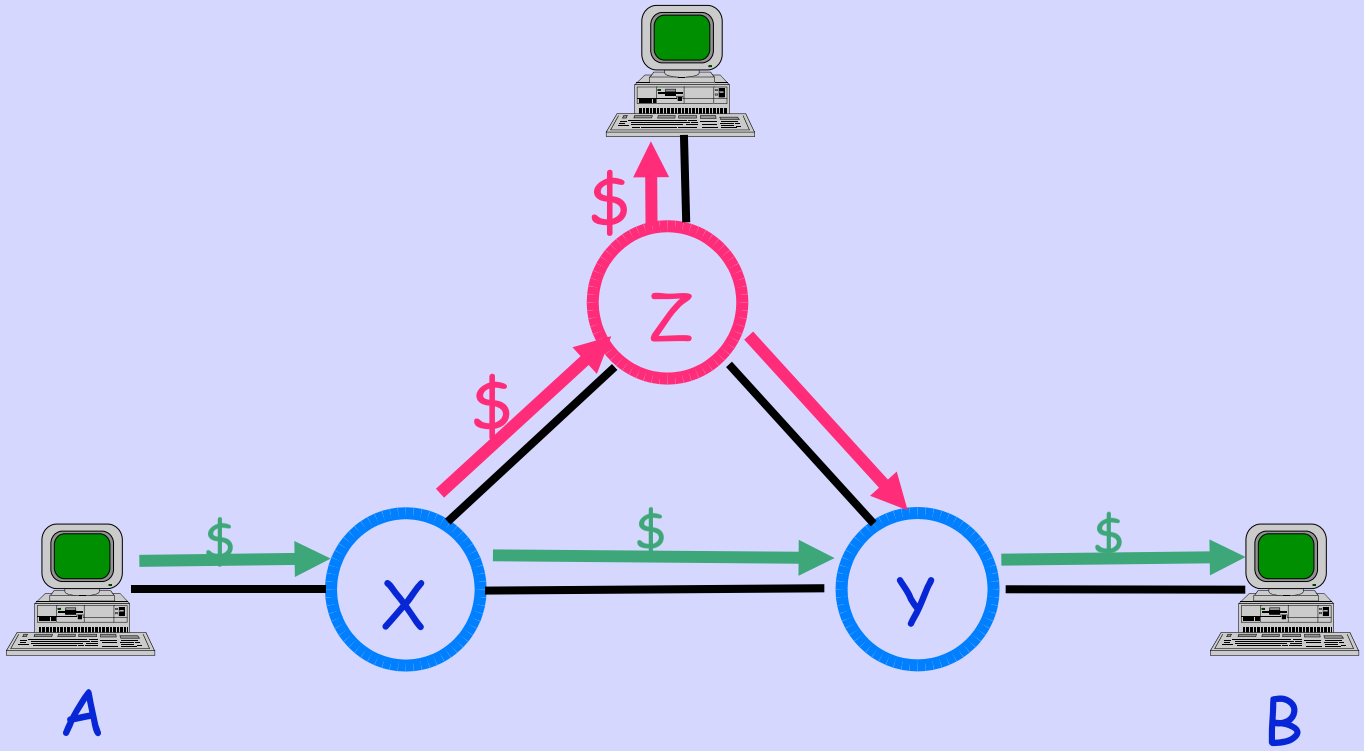
RPKI/Router API

- Must work with ROA for origin-only
- And with all certs for S-BGP
- And must not be vendor biased
- And it must work when it is all stuffed inside a bigish router
- Get Juniper on board too

But This is Not Enough

- It will help with configuration errors, e.g. the YouTube Incident
- It will not prevent even all manual misconfiguration issues
- It will not protect against BGP routing attacks
- See Tony's and Alex's DefCon Attack

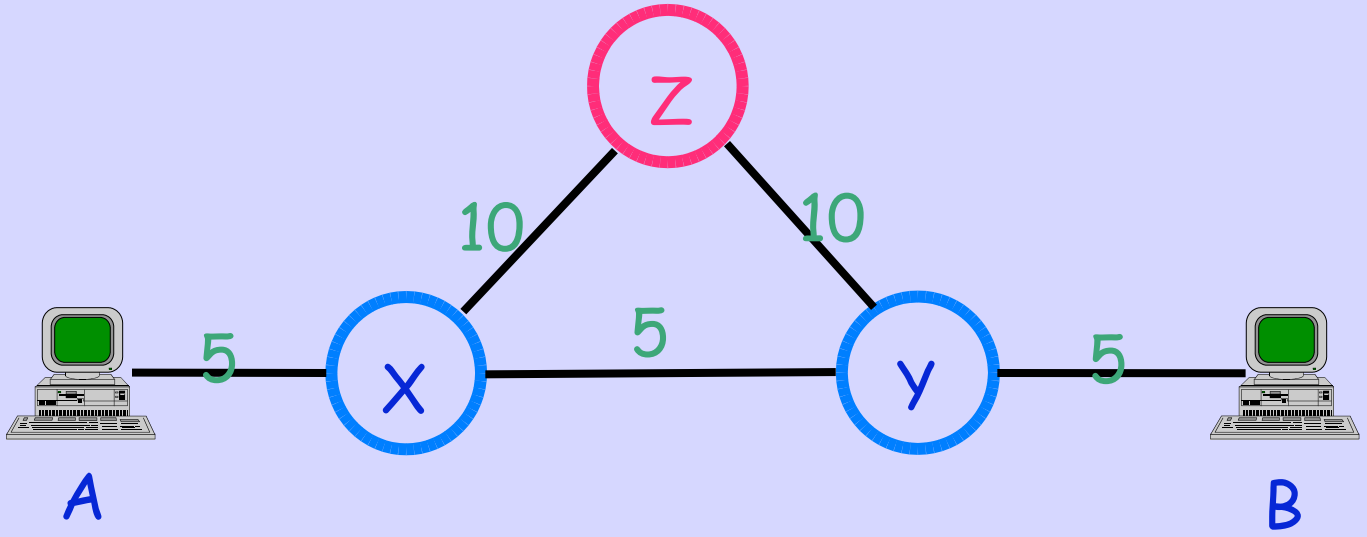
Diversion Attack



Expected Path - A->X->Y->B

Diverted Path - A->X->Z->Y->B

How Does Z Do It?



Y tells X and Z that costs are B:5

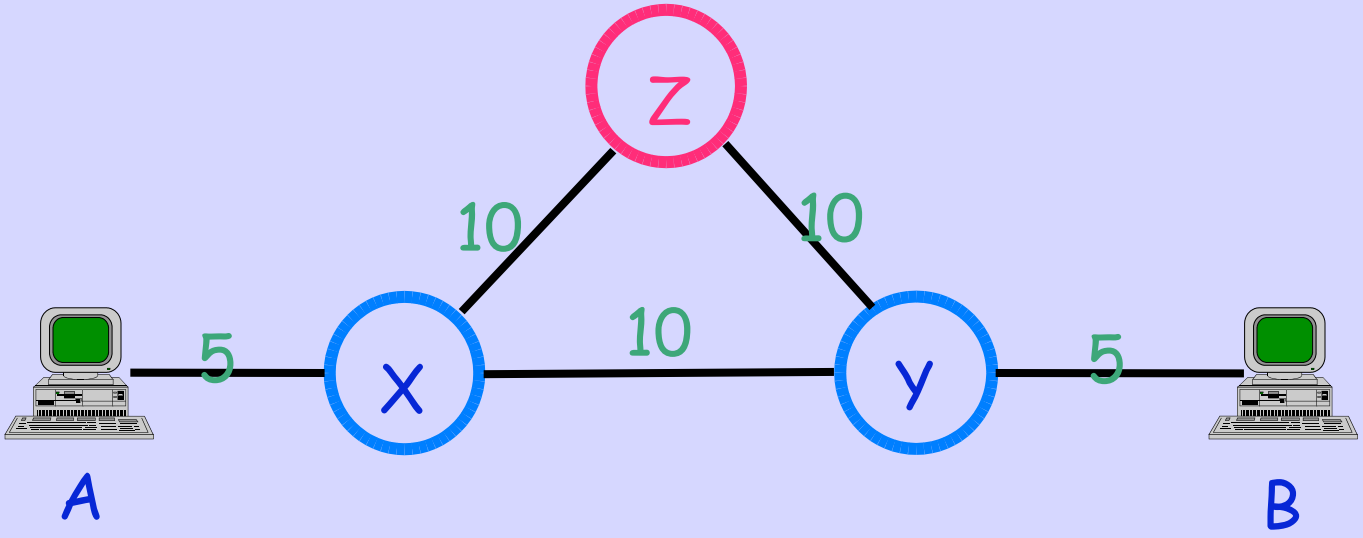
X tells A and Z that costs are Y:5 B:10

Z tells X that costs are Y:10 B:15

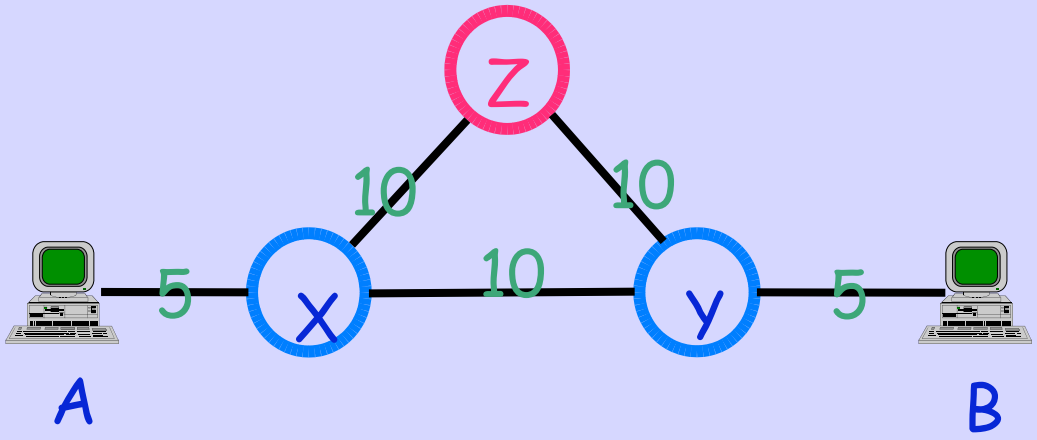
Z tells X that costs are Y:10 **B:4**

X now sends B's traffic to Z!!!

Why is this a Hard Problem?

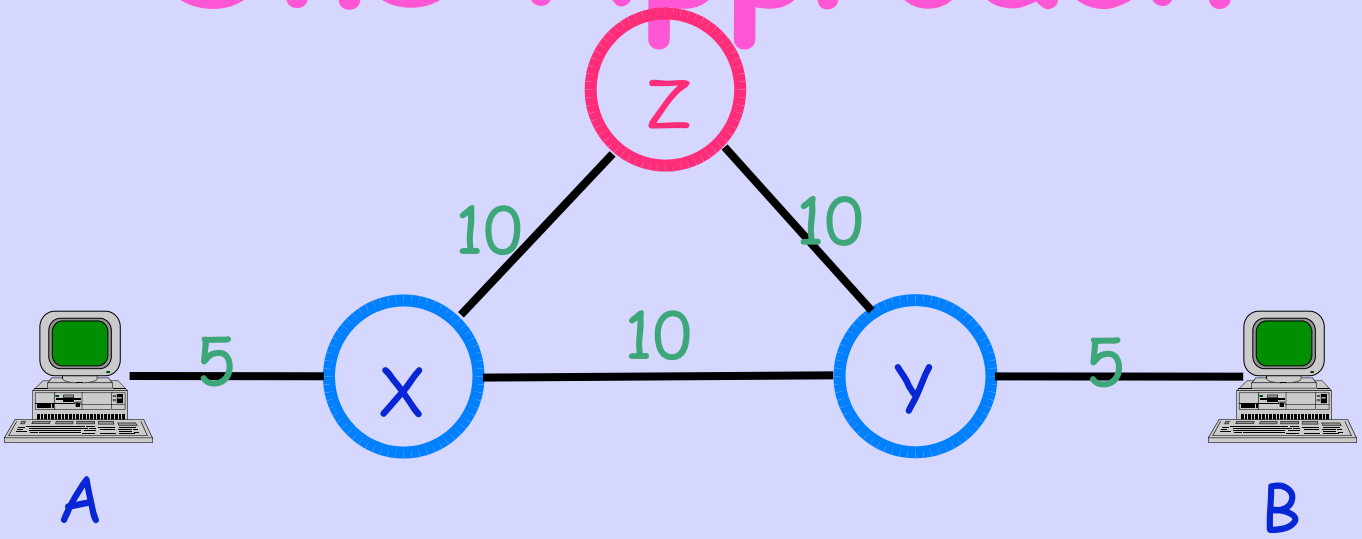


- X does not really know Z's links
- X does not really know Y's links
- They trust each other re costs!



- Validating IP prefix ownership does not help, as Z is not lying about B's owning it
- Using IRR-like peering map does not help, as Z is not lying about who connects to whom

One Approach



- B cryptographically signs the message to Y Sb(Y->B=5)
- Y signs messages to X and Z encapsulating B's message

  Sy(X->Y=10 Sb(Y->B=5)) and Sy(Z->Y=10 Sb(Y->B=5))
- Z can only sign Sz(X->Z=10 Sy(Z->Y=10 Sb(Y->B=5)))
- Now X can verify paths and costs
- **Forward path signing** solves the 'simple' case

Costs

- Crypto-CPU-intensive
- Use caching
- Use pre or delayed validation
- Moore's 'Law' is our friend
- Crypto chips are cheap
- Most announcements are boring

Path Validation

- S-BGP is the right direction. It is congruent with BGP and does about all that we know how to do today
- But it needs work, e.g. not per router but per AS, etc.

The Path(s) Forward

- Finish RPKI code
- Finish/ship sidr drafts
- RPKI testbed deployment
- Origin-only validation for routers
- S-BGP prototype and spec
- S-BGP testbed and ISP socialization

Thanks To

PLNOG

Internet Initiative Japan

ARIN

The Internet Society

Thanks To

PLNOG

Internet Initiative Japan

A Cisco Research Grant

Thanks To

PLNOG

Internet Initiative Japan

A Cisco Research Grant

Thanks To

PLNOG

Internet Initiative Japan

A Cisco Research Grant

Thanks To

PLNOG

Internet Initiative Japan

A Cisco Research Grant