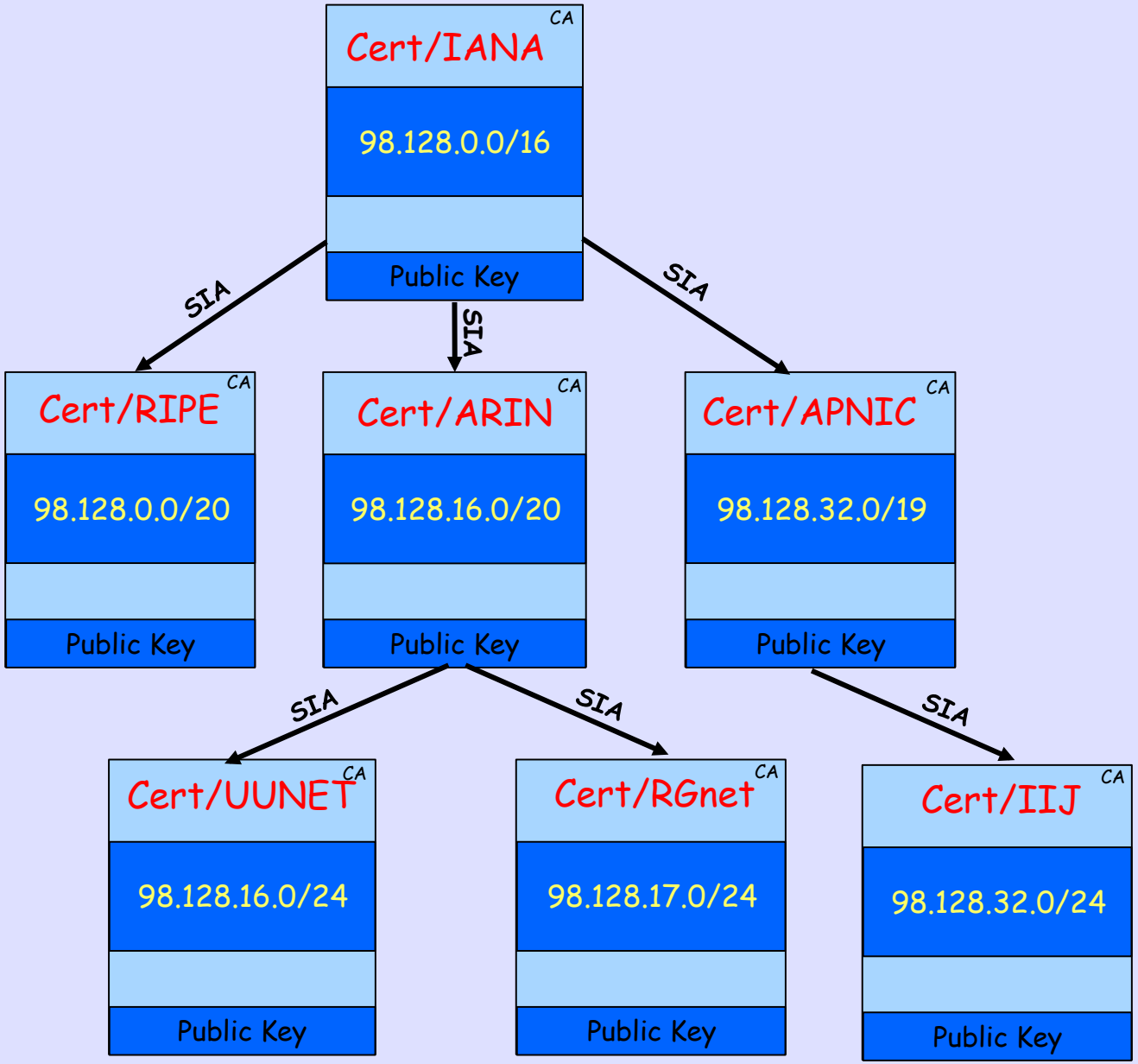
BGP Security – The Human Threat

RIPE / Amsterdam

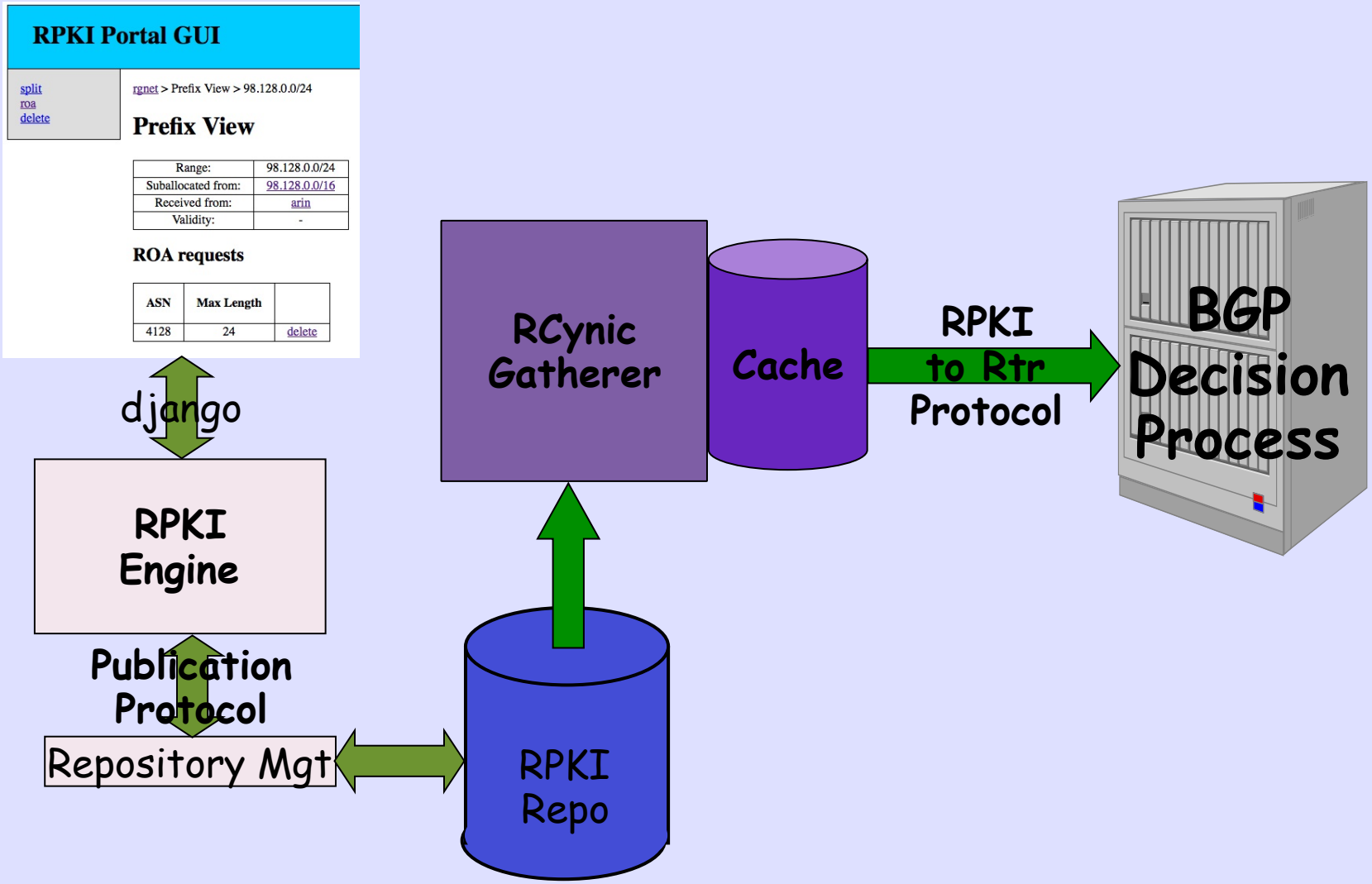
2011.05.02

Randy Bush <randy@psg.com>

Assume RPKI


Cert/IANA
CA
98.128.0.0/16
Public Key
SIA
SIA
SIA
Cert/RIPE
CA
98.128.0.0/20
Public Key
Cert/ARIN
CA
98.128.16.0/20
Public Key
Cert/APNIC
CA
98.128.32.0/19
Public Key
SIA
SIA
SIA
Cert/UUNET
CA
98.128.16.0/24
Public Key
Cert/RGnet
CA
98.128.17.0/24
Public Key
Cert/IIJ
CA
98.128.32.0/24
Public Key

Assume RPKI-RTR



Assume Origin Validation

```
R3#sh ip bg 98.128.0.0/24
BGP routing table entry for 98.128.0.0/24, version 94
Paths: (2 available, best #2, table default)
 65000 3130
    10.0.0.1 from 10.0.0.1 (65.38.193.12)
      Origin IGP, localpref 100, valid, external
      path 6802D4DC RPKI State invalid
  65001 4128
    10.0.1.1 from 10.0.1.1 (65.38.193.13)
      Origin IGP, localpref 100, valid, external, best
      path 6802D7C8 RPKI State valid
```

Origin Validation is Weak

- Today's Origin Validation provides neither cryptographic assurance (announcements are not signed), nor assurance of the AS Path of the announcement.
- A malicious router may announce as any AS, i.e. forge the ROAed origin AS.
- This would pass ROA Validation

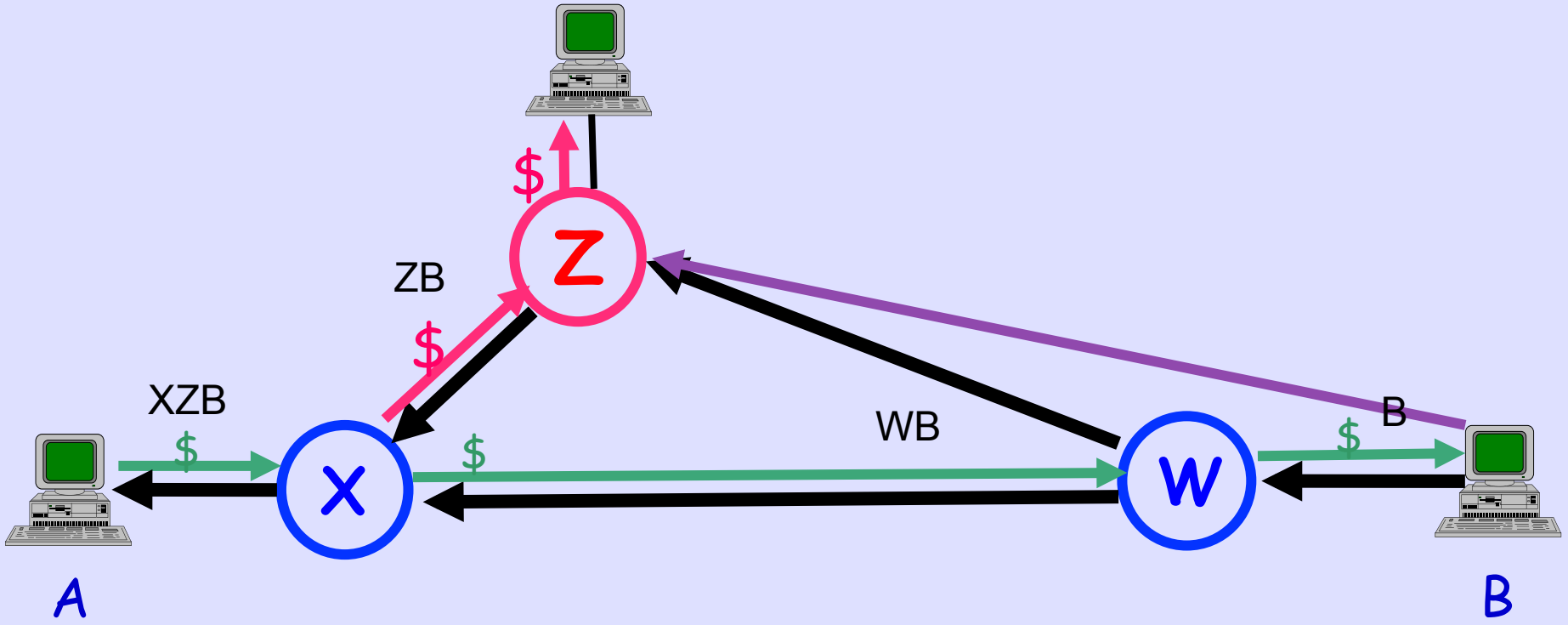
Protocol Not Policy

- Policy on the global Internet changes every 36ms
- We already have a protocol to distribute policy or its effects, it is called BGP
- We can not know intent, should Mary have announced the prefix to Bob
- But Joe can formally validate that Mary did announce the prefix to Bob
- BGPsec validates that the protocol has not been violated, and is not about intent or business policy

Full Path Validation

- Rigorous per-prefix AS path validation is the goal
- Protect against origin forgery and AS-Path monkey in the middle attacks
- Not merely showing that a received AS path is not impossible
- Yes, this is S-BGP-like not SO-BGP-like

Path Shortening Attack

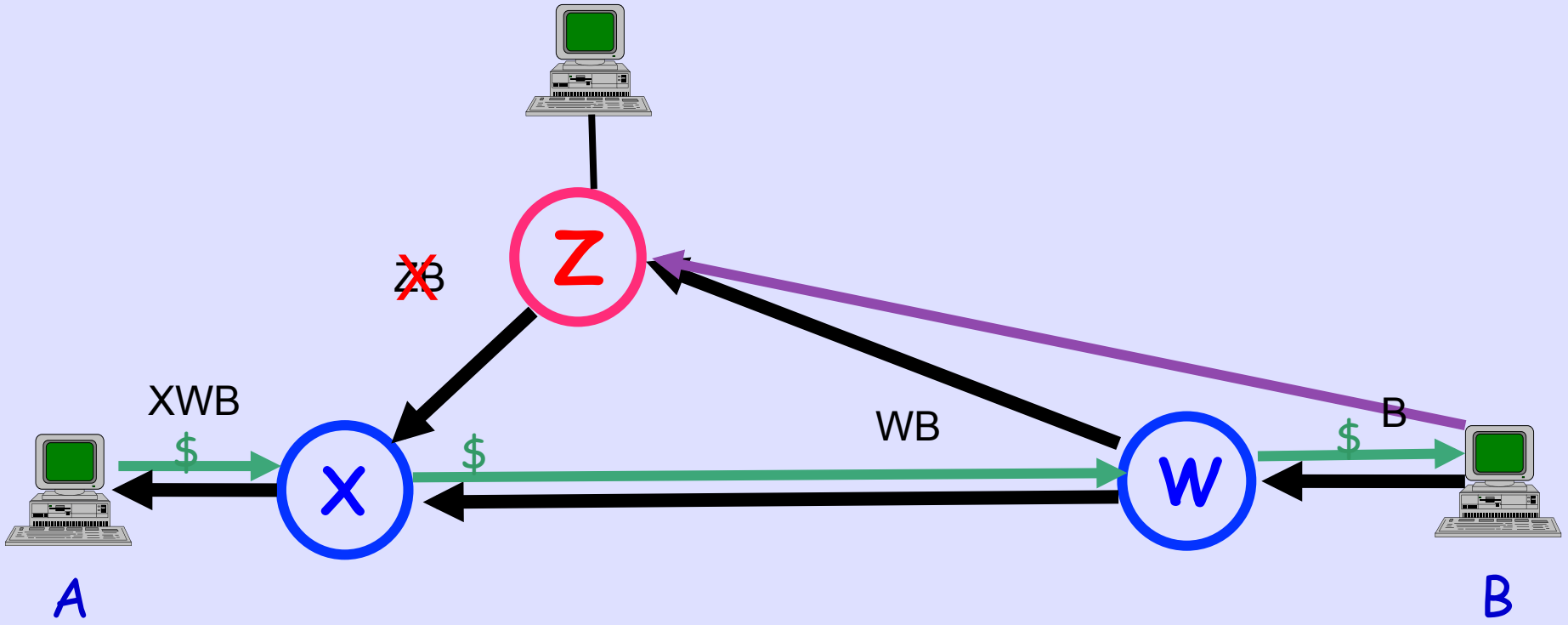


Expected Path - A->X->W->B

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

There Are Many Many Other Attacks

Forward Path Signing



B cryptographically signs the message to W Sb(B->W)

W signs messages to X and Z encapsulating B's message

Sw(W->X (Sb(B->W))) and Sw(W->Z (Sb(B->W)))

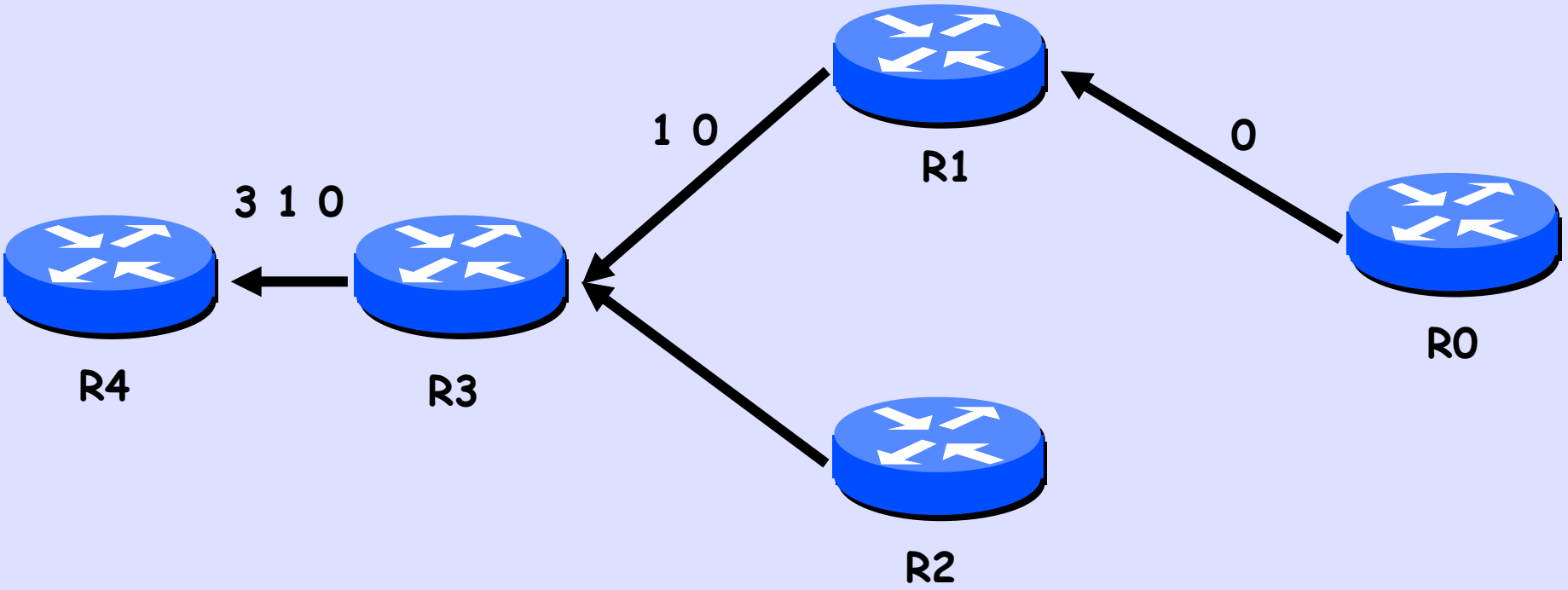
X signs the message to A Sx(X->A (Sw(W->X (Sb(B->W)))))

Z can only sign Sz(Z->X (Sw(W->Z (Sb(B->W)))))

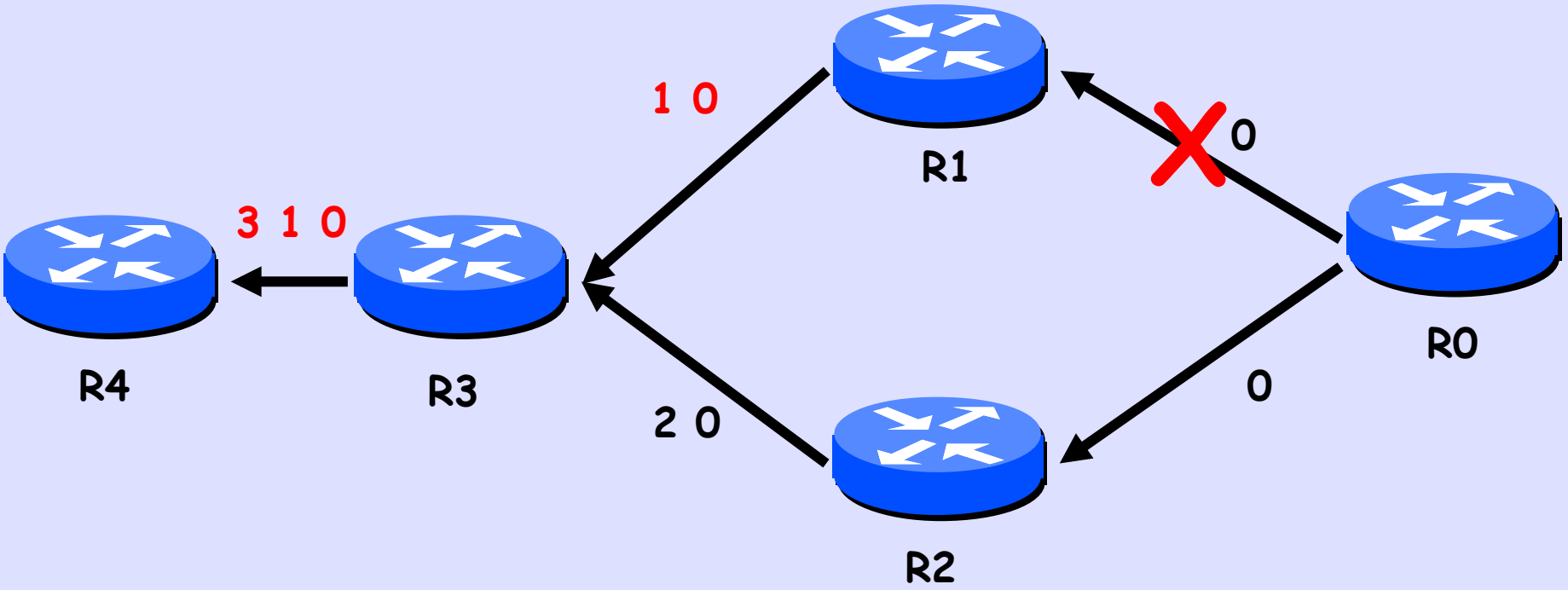
Capability Negotiation

- It is assumed that consenting routers will use BGP capability exchange to agree to run BGPsec between them
- The capability will, among other things remove the 4096 PDU limit for updates
- If BGPsec capability is not agreed, then only traditional BGP data are sent

Replay Attack



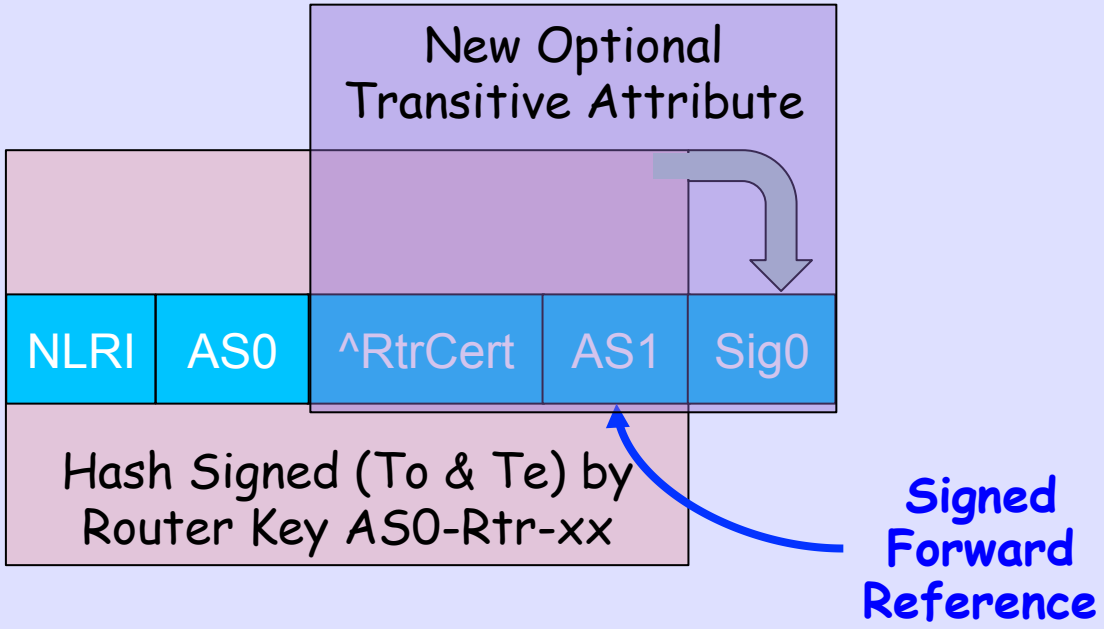
Replay Attack



Replay Reduction

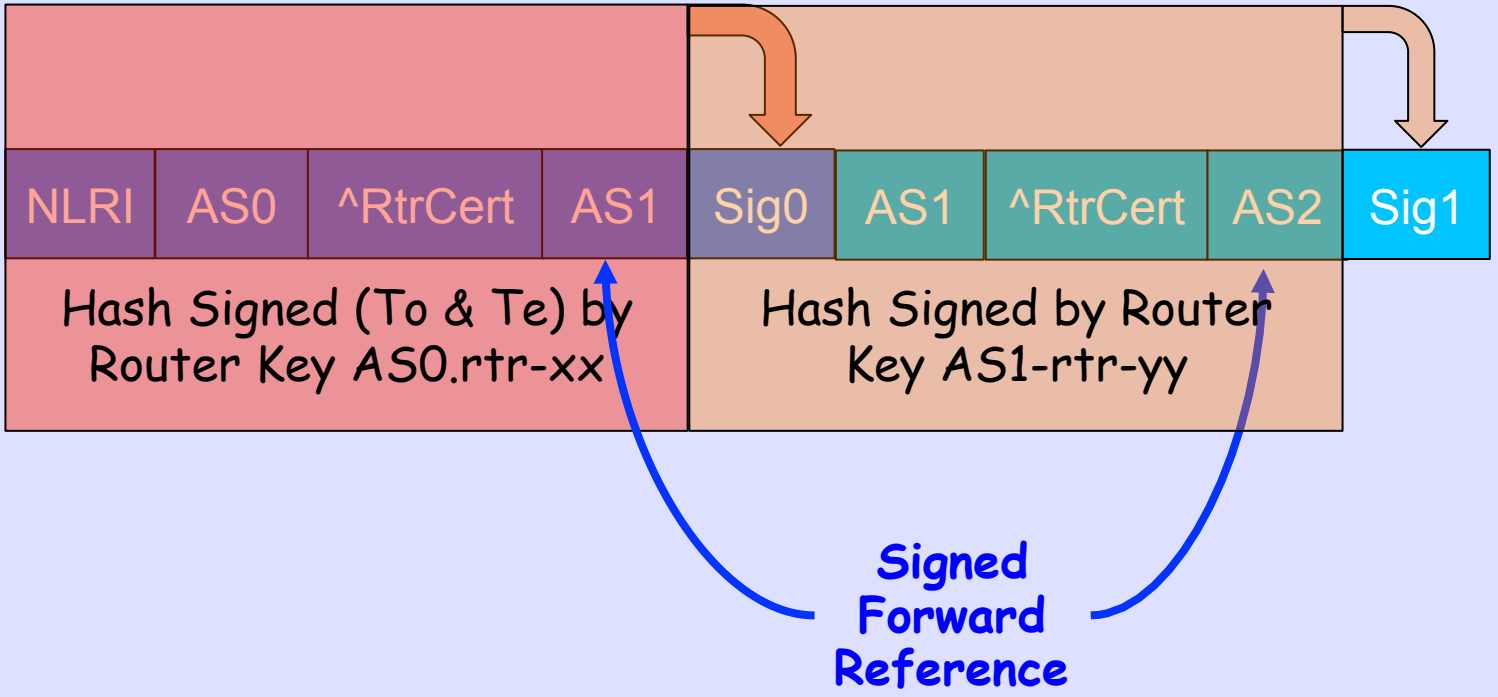
- Announcement replay is a vulnerability
- Therefore freshness is critical
- So originating announcer signs with a relatively short signature lifetime
- Origin re-announces prefix well within that lifetime, AKA ***beaconing***
- Suggested to be days, but can be hours for truly critical infrastructure

Origination by AS0 to AS1



- To and Te are times of signature origination and expiration
- Signature has a well-jittered validity end time, Te, of days
- Re-announcement by origin, AKA *beaconing*, every ~(Te-To)/3
- ROA is not needed as prefix is sufficient to find it in RPKI as today

Announcement AS1 to AS2

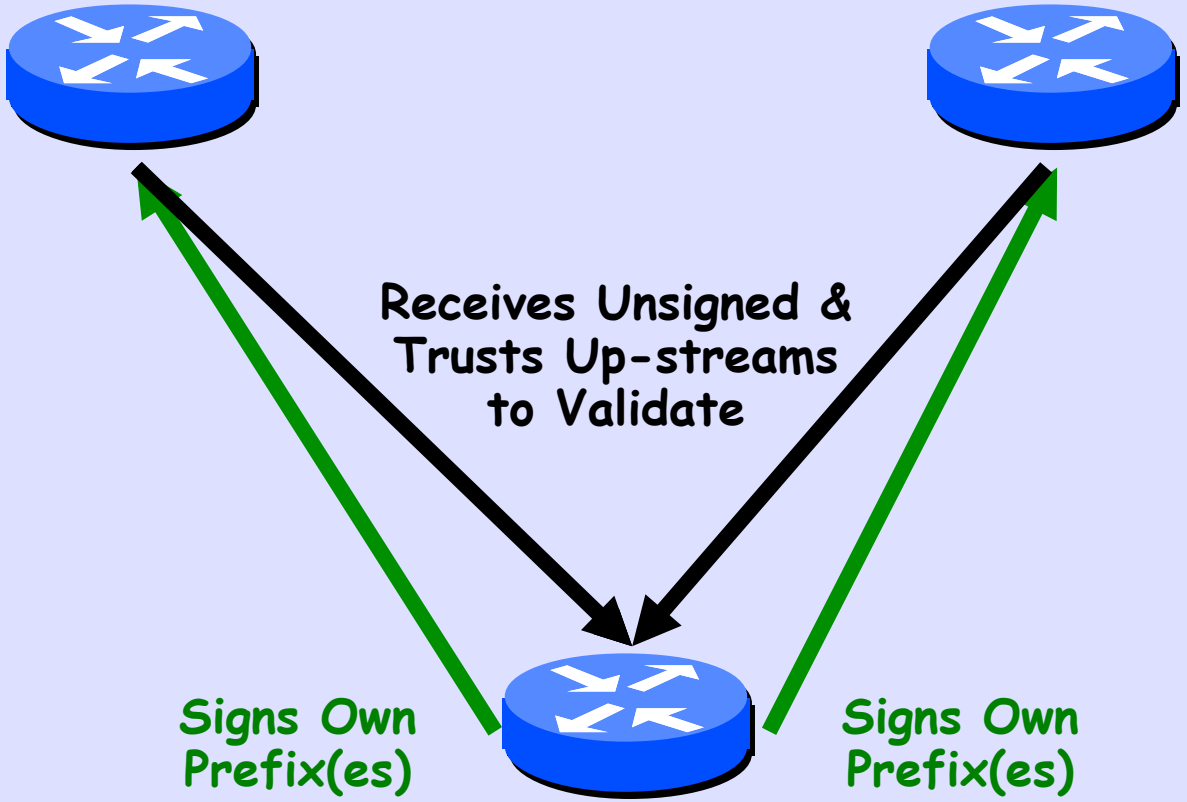


- R1 signing over R0's signature is same as signing over entire R0 announcement
- Non-originating router signatures do not have validity periods
- But when they receive a beacon announcement, they must propagate it

Only at Provider Edges

- This design protects only inter-domain routing, not IGPs, not even iBGP
- BGPsec will be used inter-provider, only at the providers' edges
- Of course, the provider's iBGP will have to carry the BGPsec information
- Providers and inter-provider peerings might be heterogeneous

Simplex End Site



Only Needs to Have Own Private Key, No Other Crypto or RPKI Data

No Hardware Upgrade!!

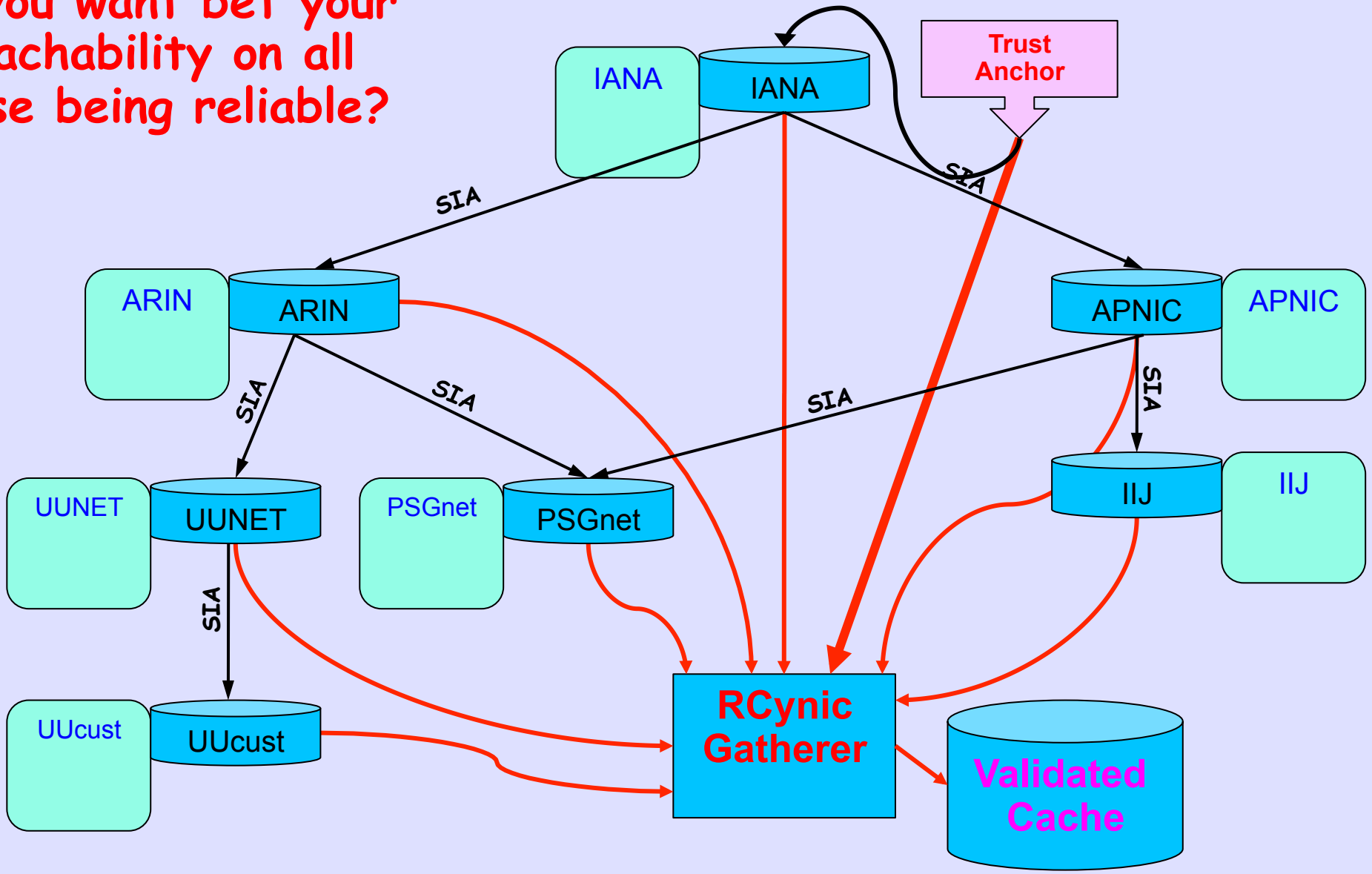
Informal BGPsec Group

chris morrow (google)
dave ward (juniper)
doug maugham (dhs)
doug montgomery (nist)
ed kern (cisco)
heather schiller (uunet)
jason schiller (uunet)
john scudder (juniper)
kevin thompson (nsf)
keyur patel (cisco)
kotikalapudi sriram (nist)
luke berndt (dhs)
matt lepinski (bbn)
pradosh mohapatra (cisco)
randy bush (iij)
rob austein (isc)
ruediger volk (dt)
russ housley (vigilsec)
russ mundy (sparta)
sam weiler (sparta)
sandy murphy (sparta)
sharon goldberg (boston uni)
steve bellovin (columbia uni)
steve kent (bbn)
warren kumari (google)

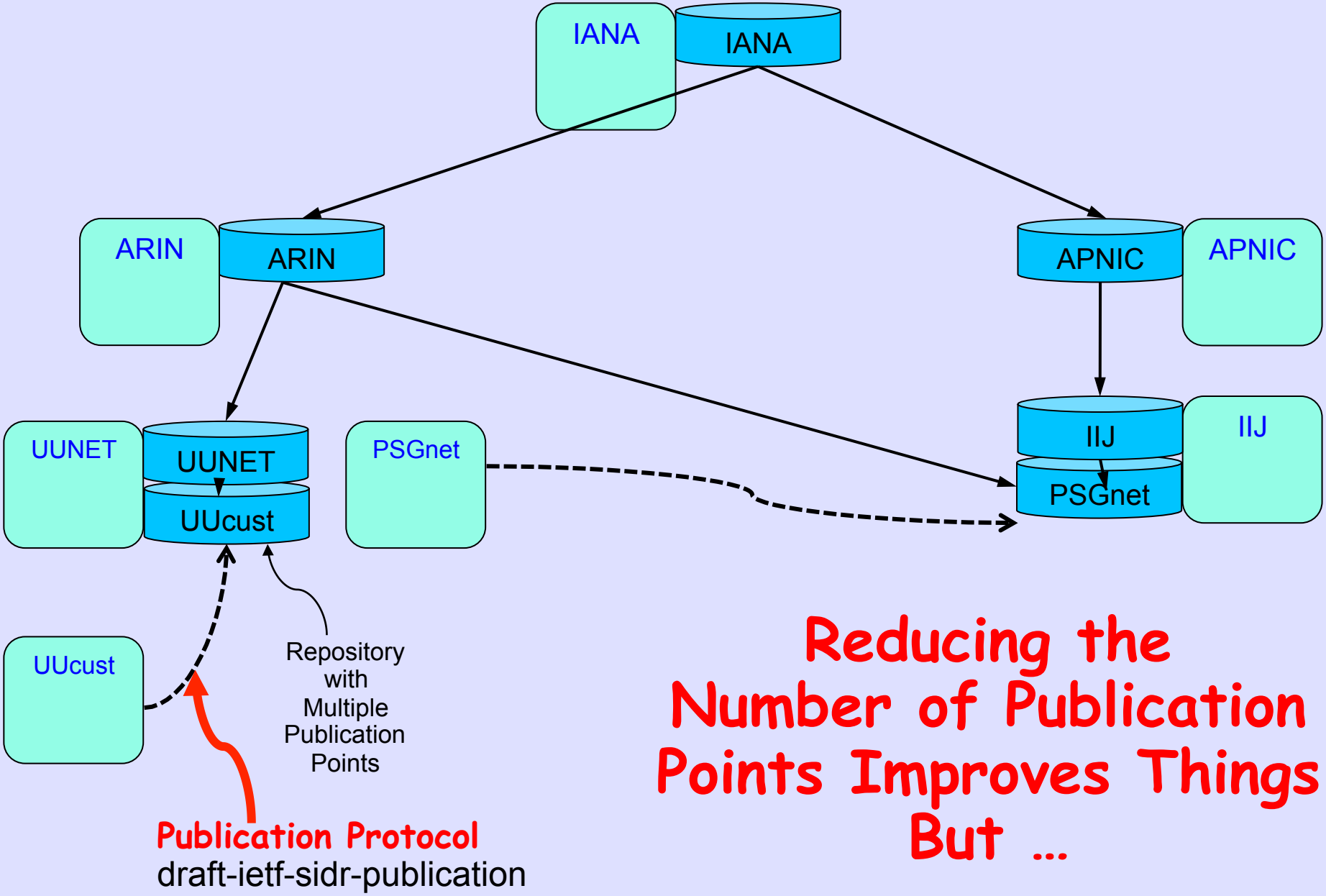
The Real Threats

RPKI Reliability

Do you want bet your reachability on all these being reliable?



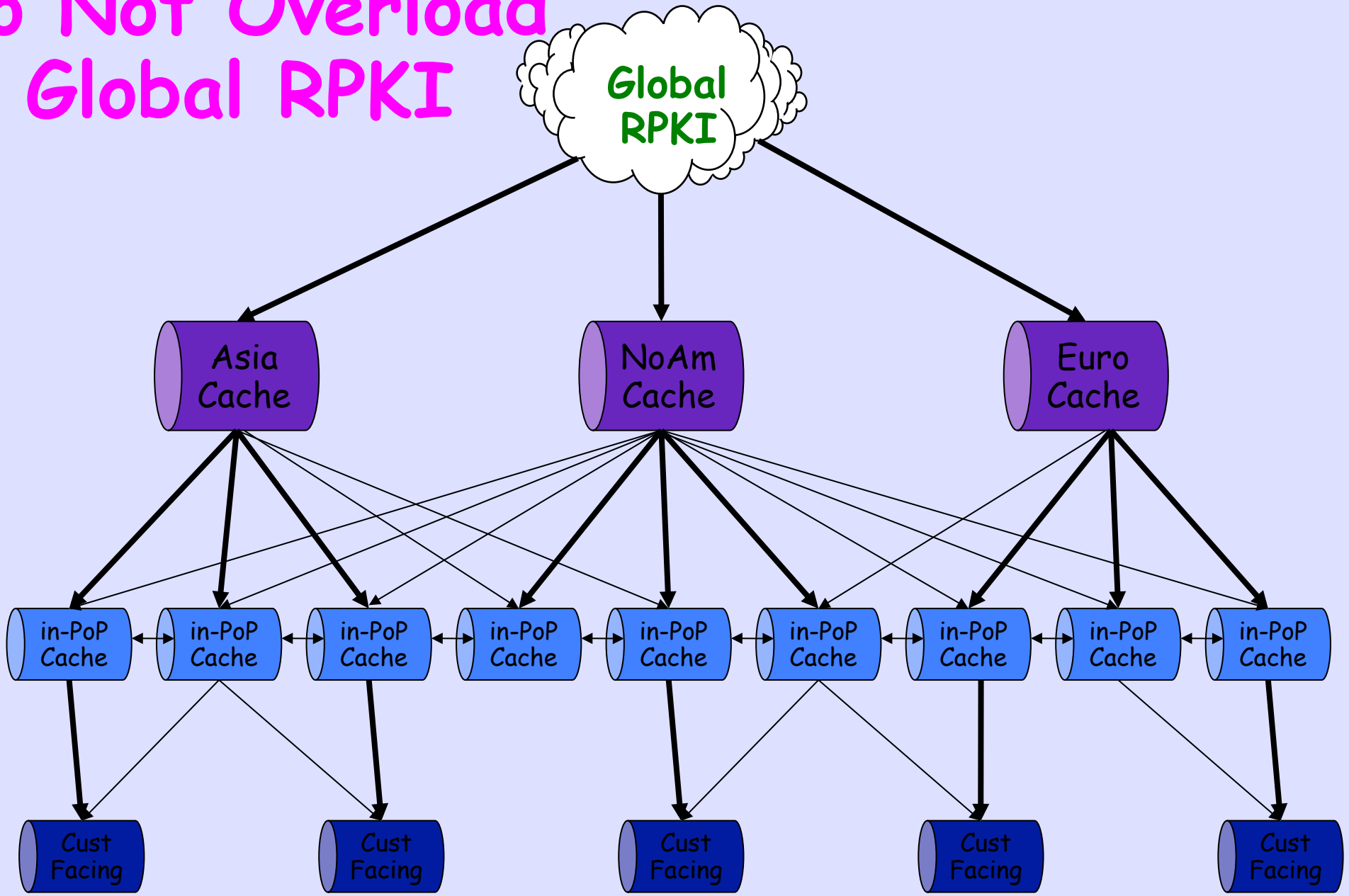
Reliability Via Hosted Publication



Reducing the Number of Publication Points Improves Things But …

Think DNS
Root Anycast &
ccTLD Anycast
…

Do Not Overload Global RPKI



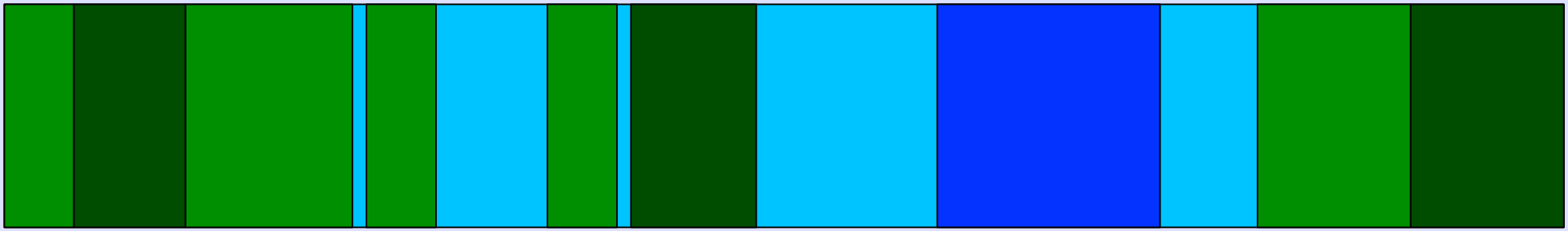
Have Cache in POP

High Priority

Lower Priority

Covering a Customer

I Issue a ROA for the Covering Prefix



I need to do this to protect
Static Customers and my Infrastructure

My Infrastructure

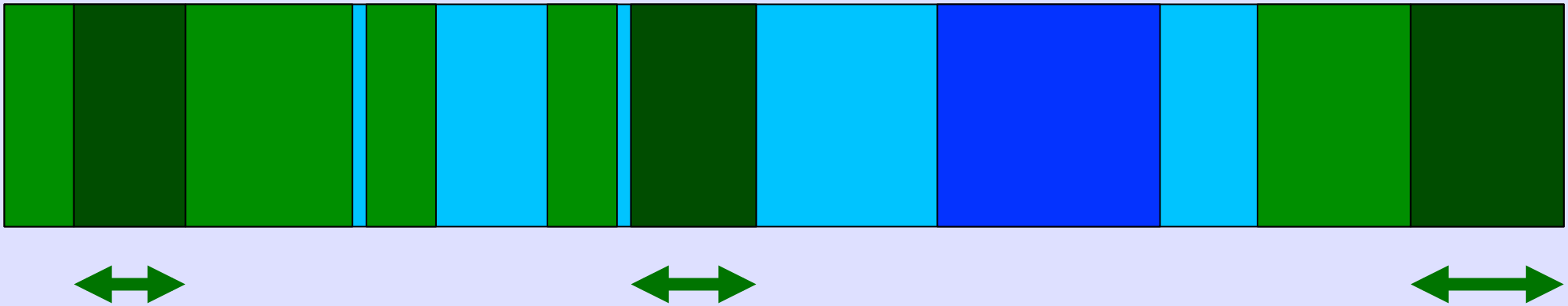
BGP Cust

Static (non BGP) Cust

Unused

Covering a Customer

But if I Issue a ROA for the Covering Prefix



Before My Customers issue ROAs for These

My Infrastructure

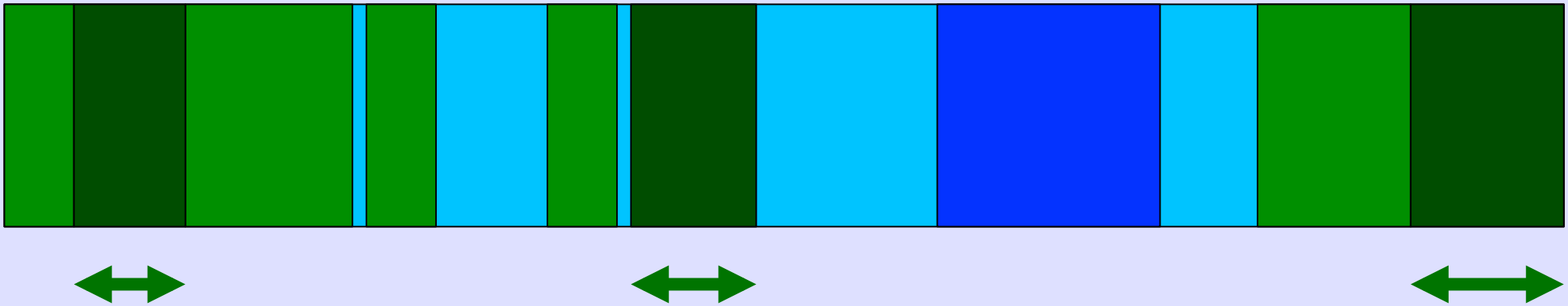
BGP Cust

Static (non BGP) Cust

Unused

Covering a Customer

If I Issue a ROA for the Covering Prefix



Before My Customers issue ROAs for These

Their Routing Becomes Invalid!

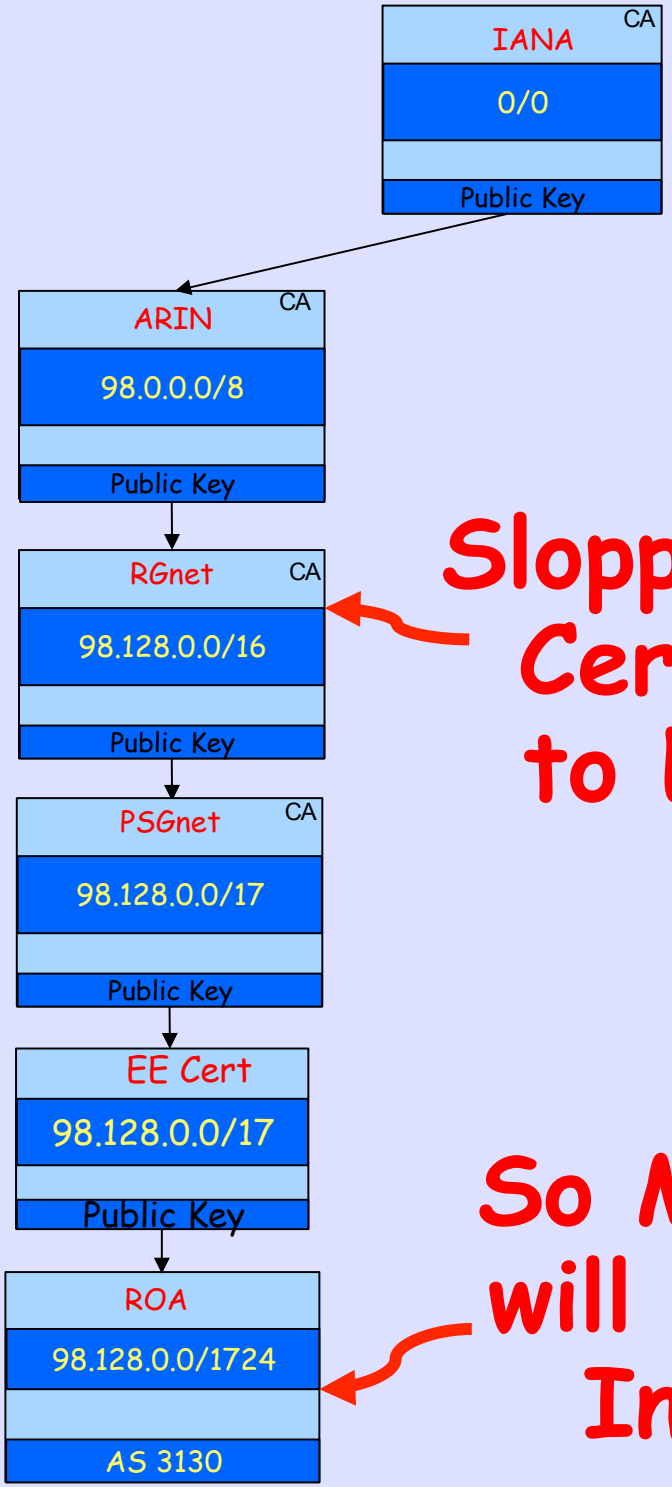
My Infrastructure

BGP Cust

Static (non BGP) Cust

Unused

Up-Chain Expiration



These are not Identity Certs

So Who Do You Call?

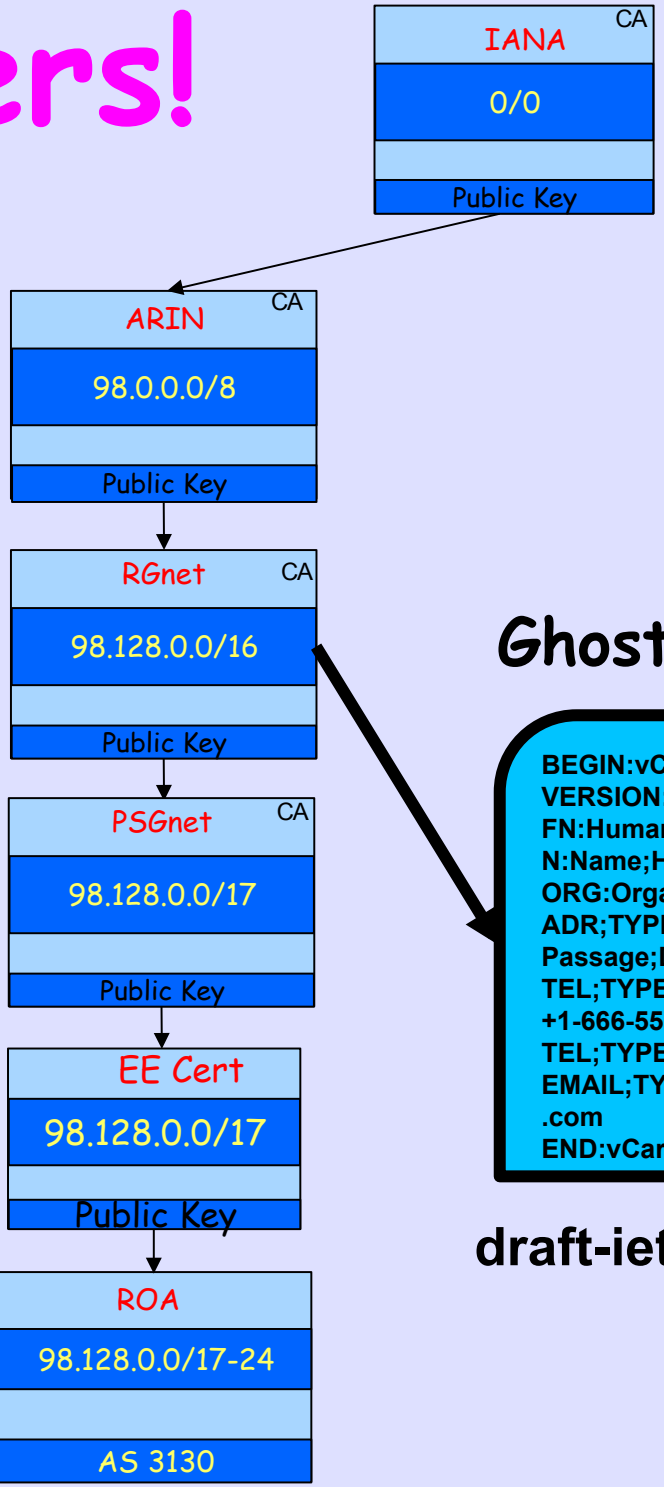
Sloppy Admin Cert Soon to Expire!

So My ROA will become Invalid!

ROA Invalid but I Can Route

- The ROA will become Invalid
- My announcement will just become NotFound, not Invalid
- Unless my upstream has a ROA for the covering prefix, which is likely

Ghostbusters!



Ghostbusters Record

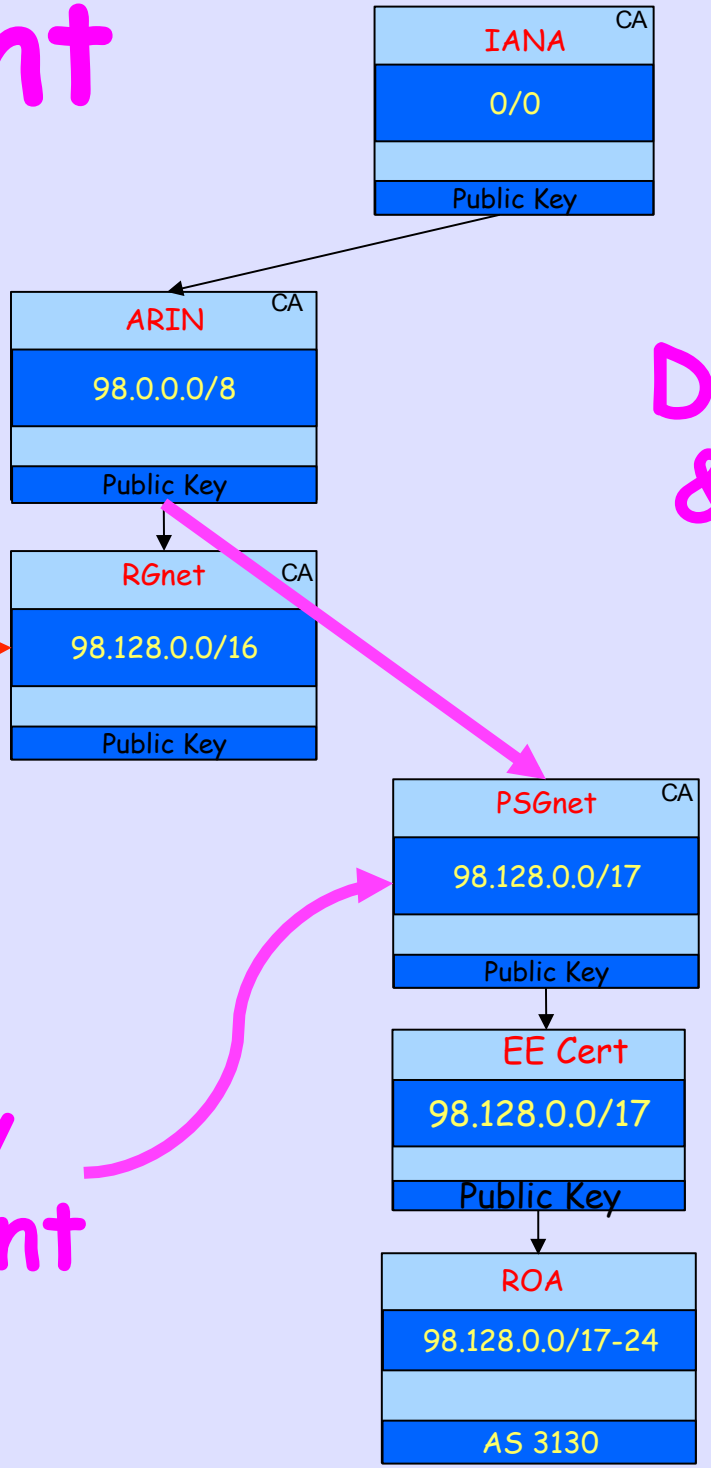
```
BEGIN:vCard
VERSION:3.0
FN:Human's Name
N:Name;Human's;Ms.;Dr.;OCD;ADD
ORG:Organizational Entity
ADR;TYPE=WORK:;;42 Twisty
Passage;Deep Cavern; WA; 98666;U.S.A.
TEL;TYPE=VOICE,MSG,WORK:
+1-666-555-1212
TEL;TYPE=FAX,WORK:+1-666-555-1213
EMAIL;TYPE=INTERNET:human@example
.com
END:vCard
```

draft-ietf-sidr-ghostbusters

What if No Answer

- What if the 'threatening' cert's maintainer does not answer or maintain their cert?
- Can I appeal up-stream of them?
- Will the grandparents take care of the children?

Grandparent Rescue

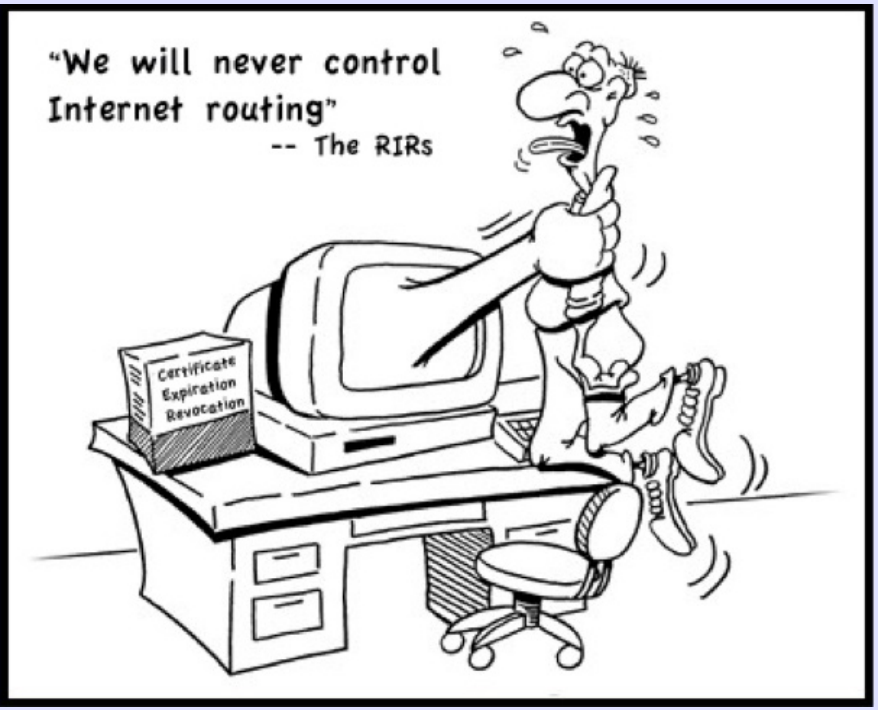


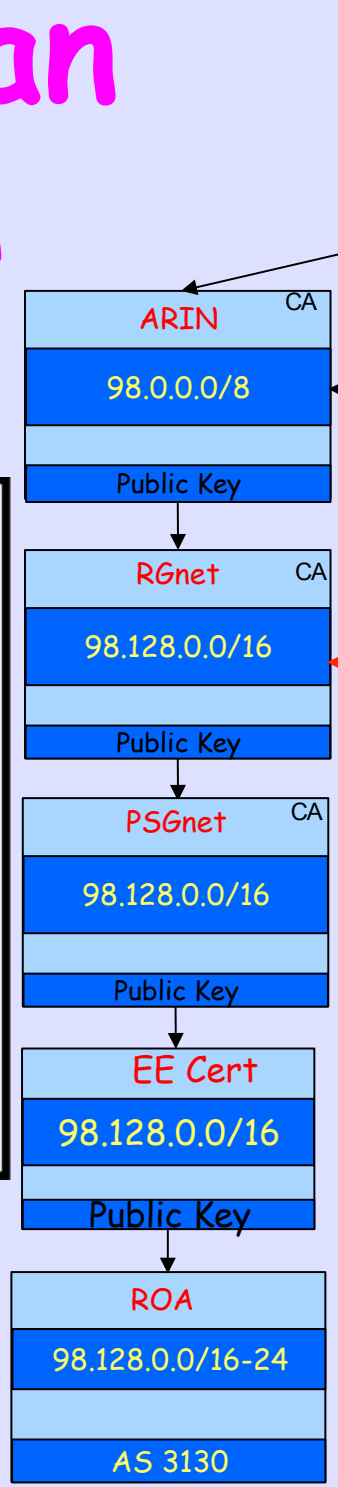
Sloppy Admin Cert Soon to Expire!

Deep Policy & Liability Issues

Saved by Grandparent

Authoritarian Expiration





Authoritarian Issuer

So My Cert is Soon to Become Invalid!

Who Do You Call?

Cert Task Force
Address Policy
Rob's New Policies

And if You Believe "Them is Us" Read the ARIN PPML Mailing List

But in the End, You Control Your Policy

"Announcements with Invalid origins MAY be used, but SHOULD be less preferred than those with Valid or NotFound."

-- draft-ietf-sidr-origin-ops

But if I do not reject Invalid, what is all this for?

THIS WORK IS SPONSORED IN PART BY THE DEPARTMENT OF HOMELAND SECURITY UNDER AN INTERAGENCY AGREEMENT WITH THE AIR FORCE RESEARCH LABORATORY (AFRL).

we Take your Scissors Away and turn them into plowshares