Idealized BGPsec: Formally Verifiable BGP

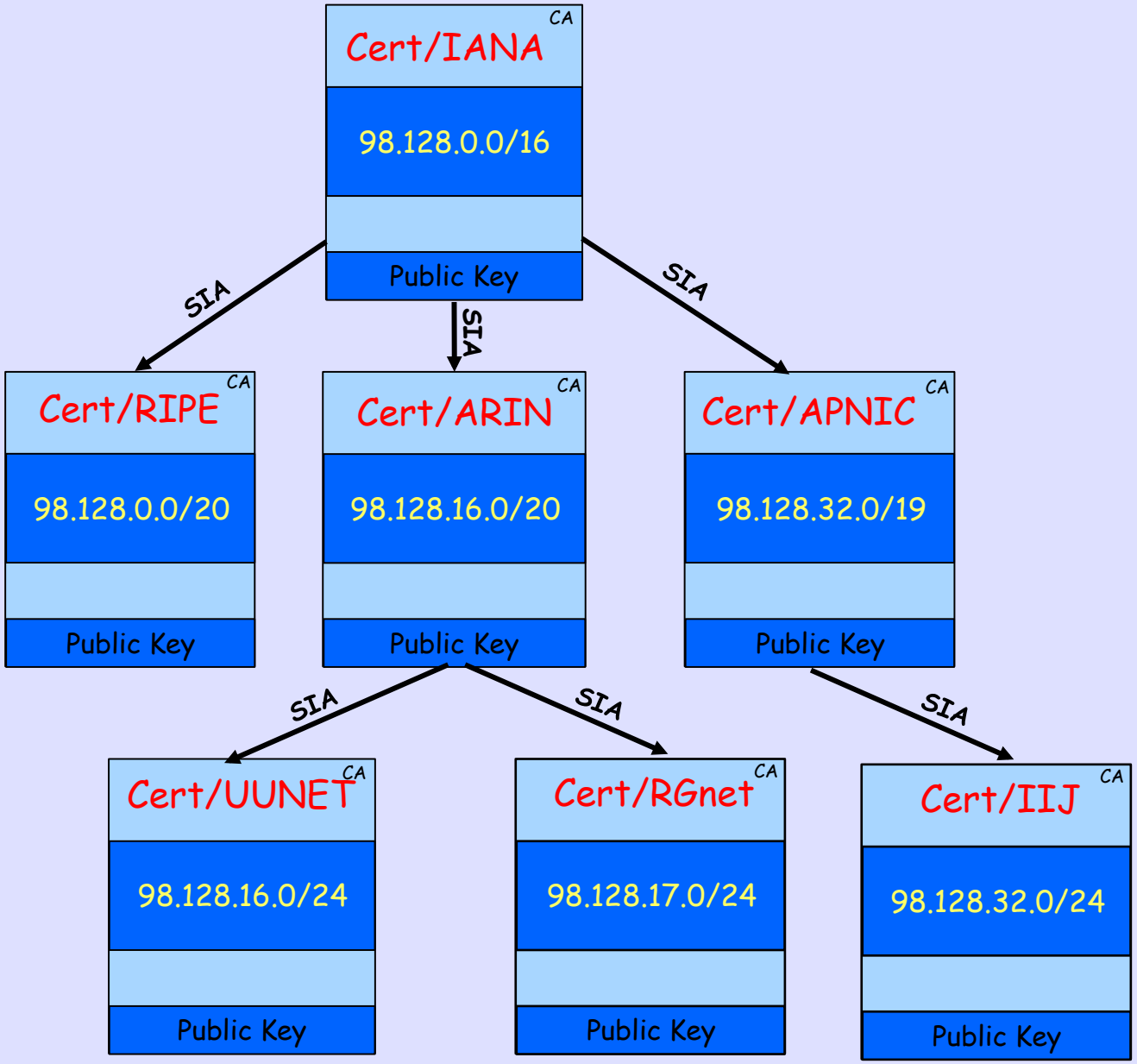
2011.03.27

Randy Bush <randy@psg.com>

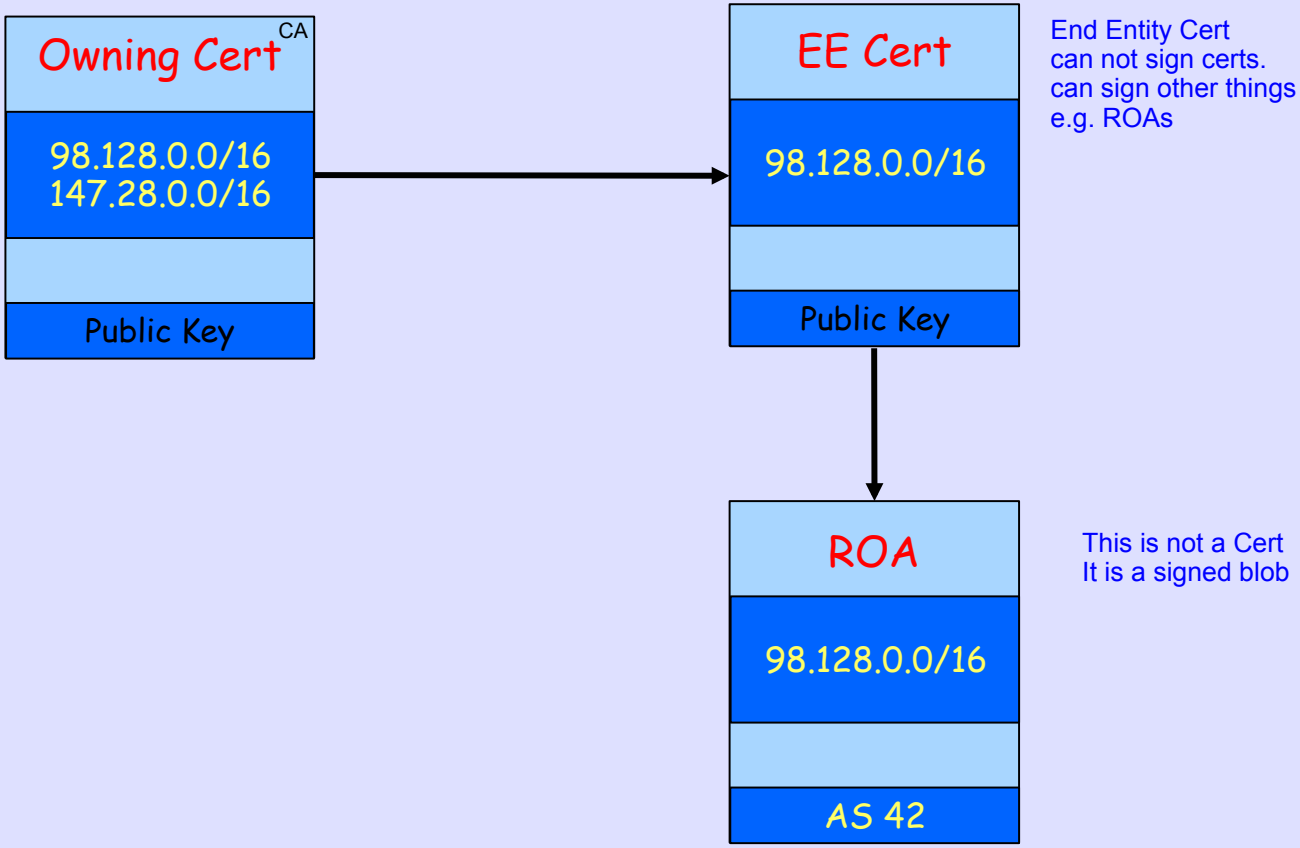
for the

Informal BGPsec Design Group

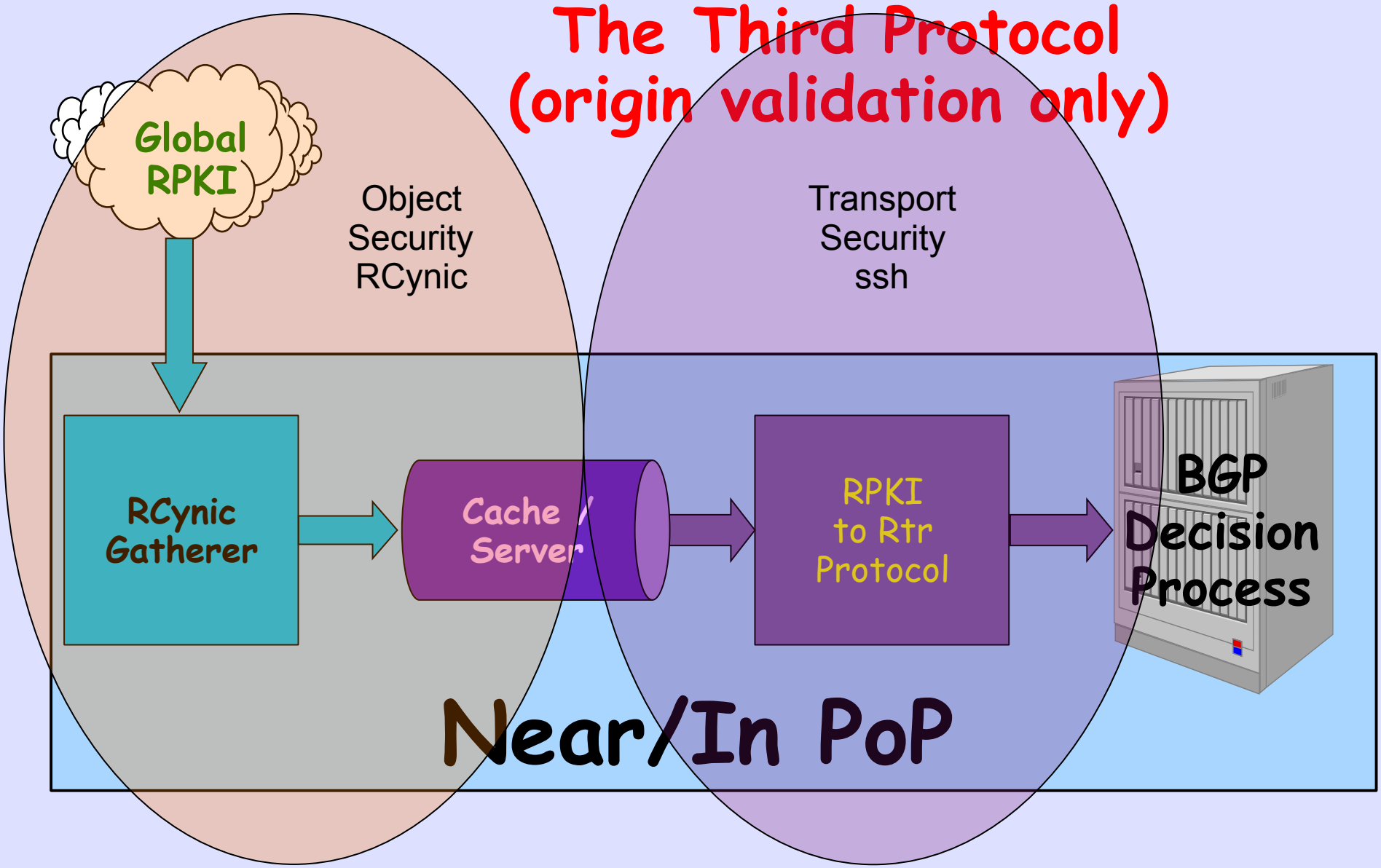
Assume RPKI is a Given



Assume ROAs are a Given



Assume RPKI-RTR Given



Assume Origin Validation

```
RP/0/1/CPU0:r0.dfw#sh bgp 64.9.224.0
BGP routing table entry for 64.9.224.0/20
Versions:
  Process              bRIB/RIB  SendTblVer
  Speaker                    0           0
Last Modified: Oct  2 17:38:27.630 for 4d22h
Paths: (6 available, no best path)
  Not advertised to any peer
  Path #1: Received by speaker 0
  2914 3356 36492
    157.238.224.149 from 157.238.224.149 (129.250.0.85)
      Origin IGP, metric 2, localpref 100, valid, external,\
origin validity state: invalid
      Community: 2914:420 2914:2000 2914:3000 4128:380
```

Origin Validation is Weak

- Today's Origin Validation only stops accidental misconfiguration, which is quite useful. But ...
- A malicious router may announce as any AS, i.e. forge the ROAed origin AS.
- This would pass ROA Validation as in draft-ietf-sidr-pfx-validate.

BGPsec to Fill the Gap

RPKI-based Origin Validation provides neither cryptographic assurance (announcements are not signed), nor assurance of the AS Path of the announcement

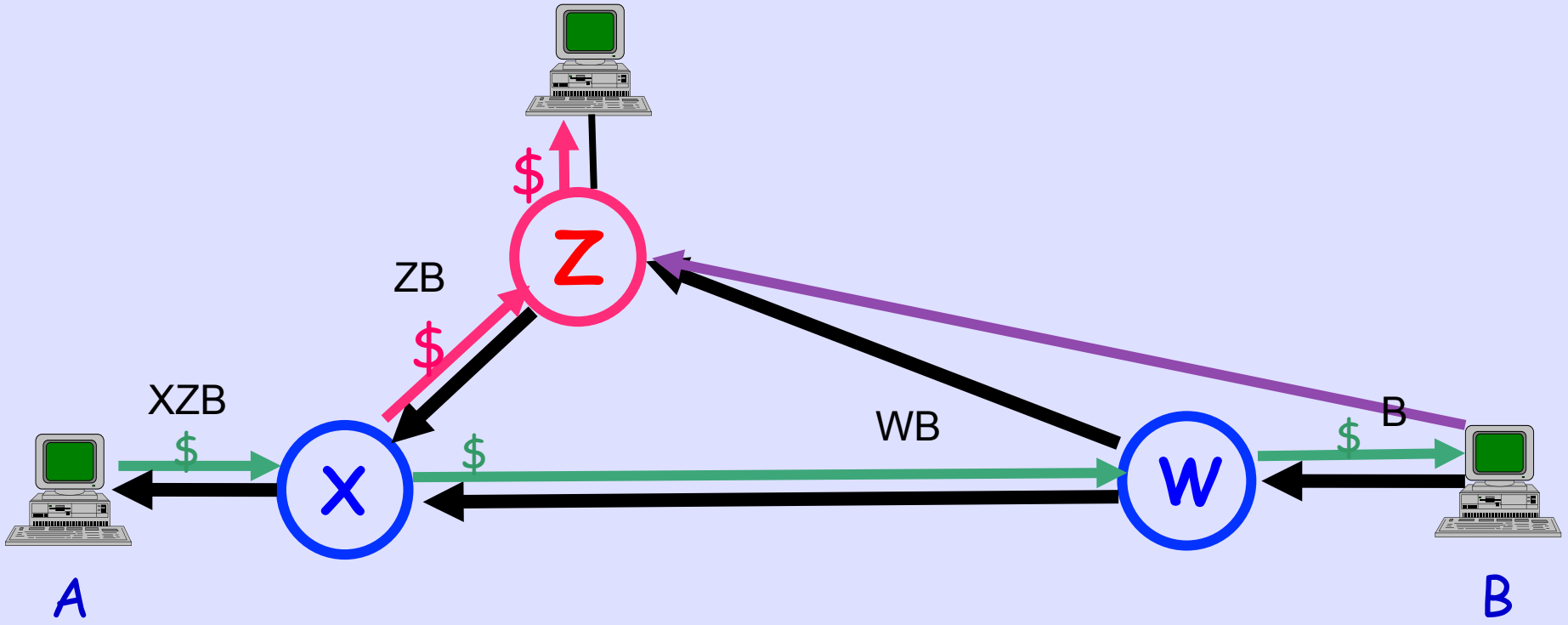
Protocol Not Policy

- 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 is all about validating that the protocol has not been violated, and not at all 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

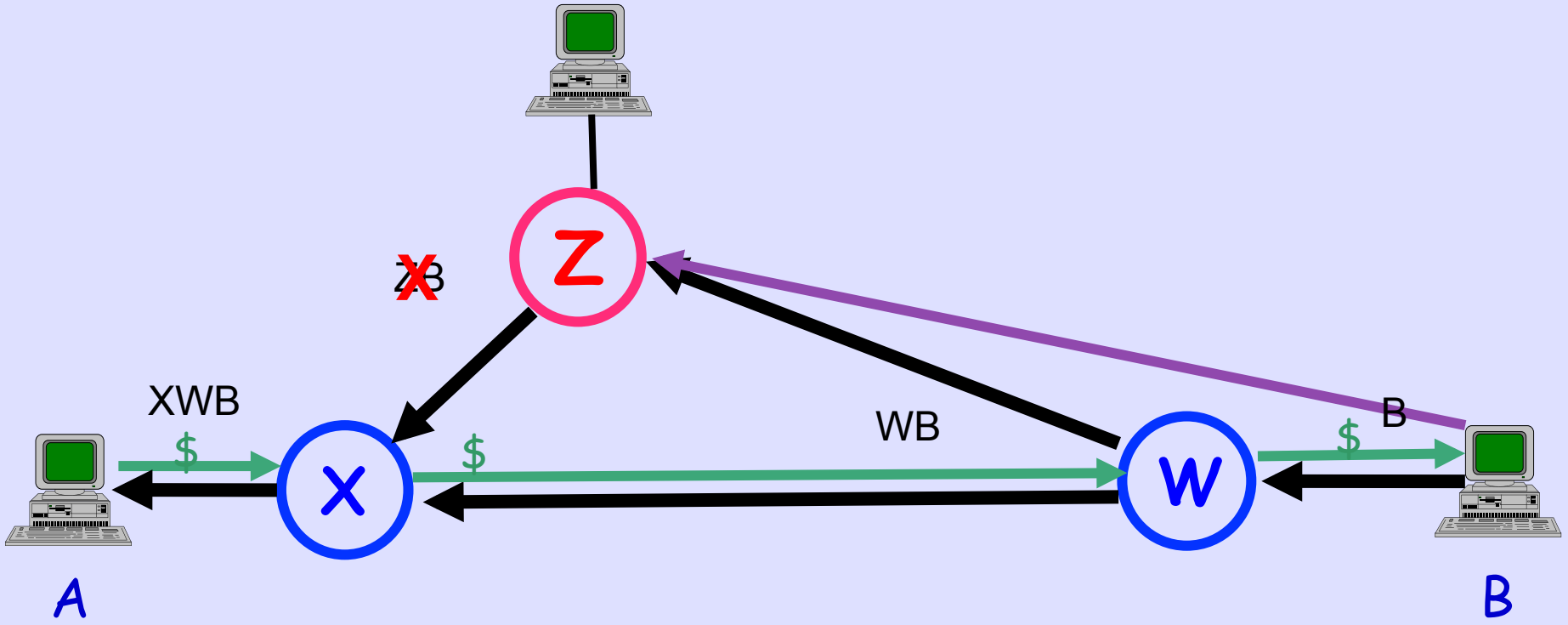
Diverted Path - A->X->Z->W->B

There Are Many Many Other Attacks

Forward Path Signing

AS hop N signing (among other things) that it is sending the announcement to AS hop N+1 by AS number, is believed to be fundamental to protecting against monkey in the middle attacks

Forward-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)))))

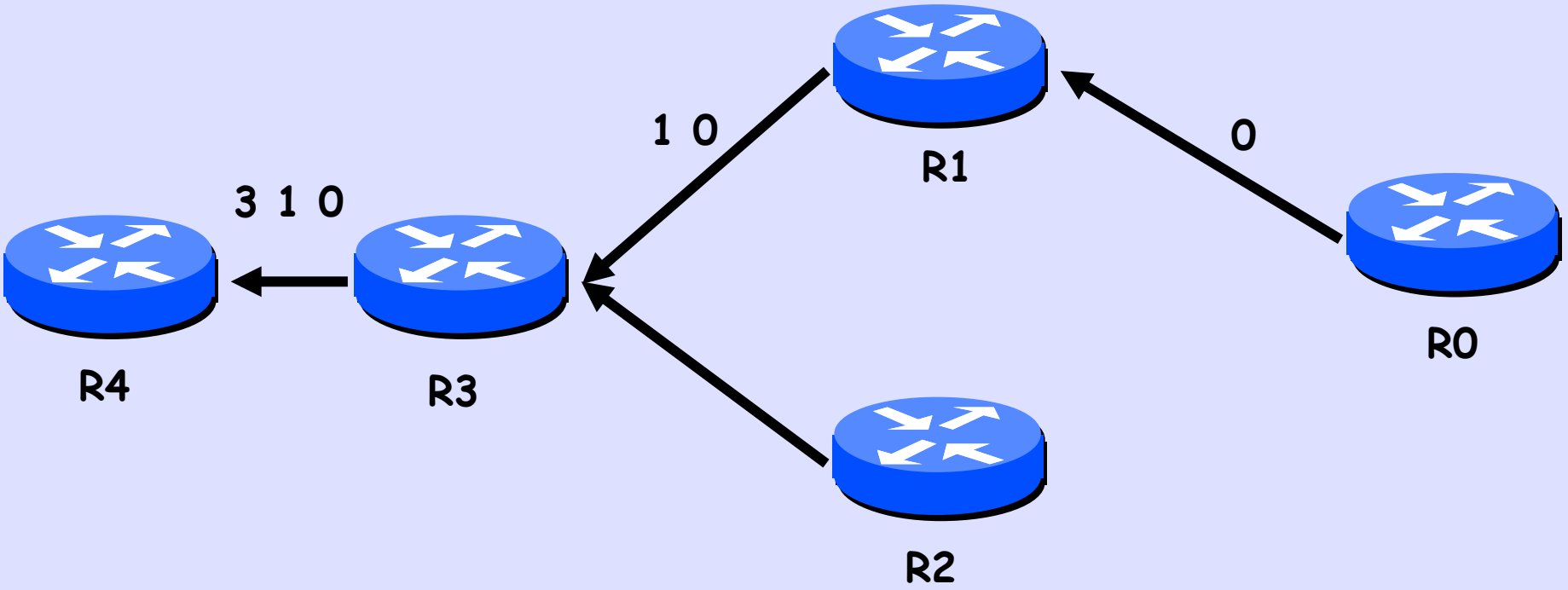
Capability Negotiation

- 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

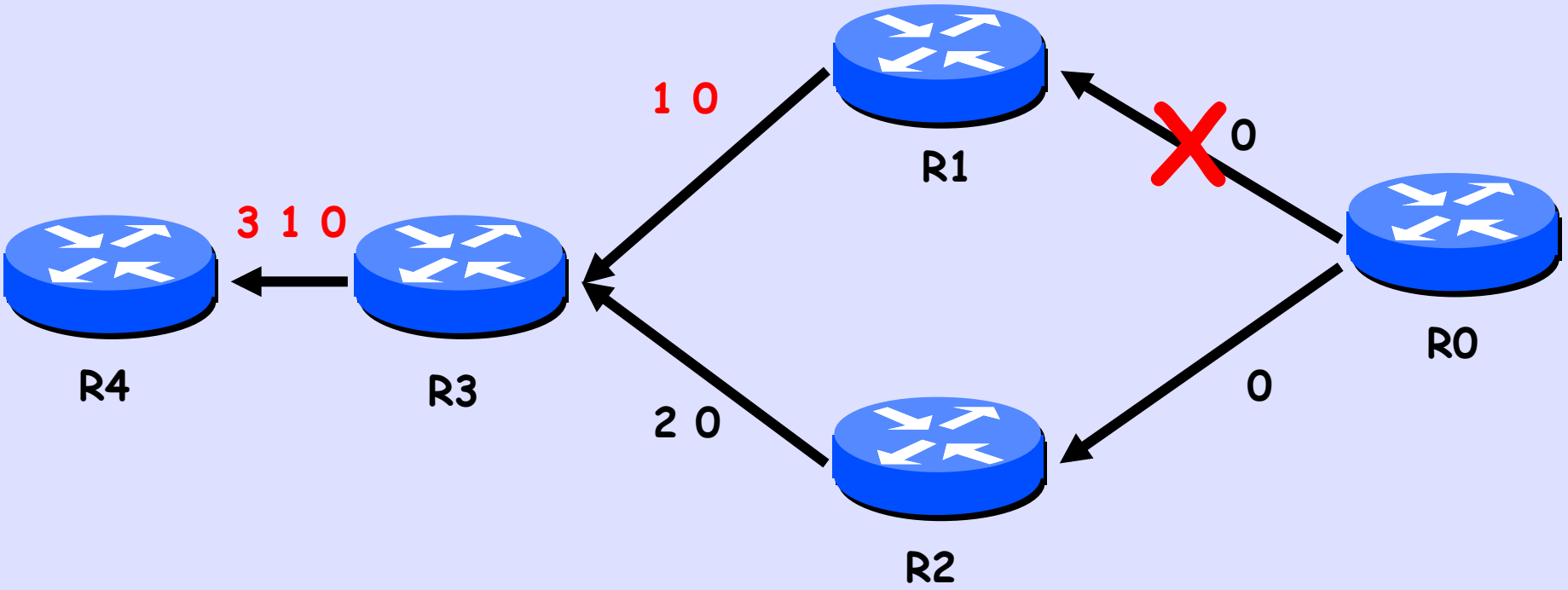
New BGP Attribute

This protocol uses a new transitive optional BGP attribute which contains signed assertions that the prefix and path update has been received by the signing AS and that it is forwarding the update to a specific next AS.

Replay Attack



Replay Attack



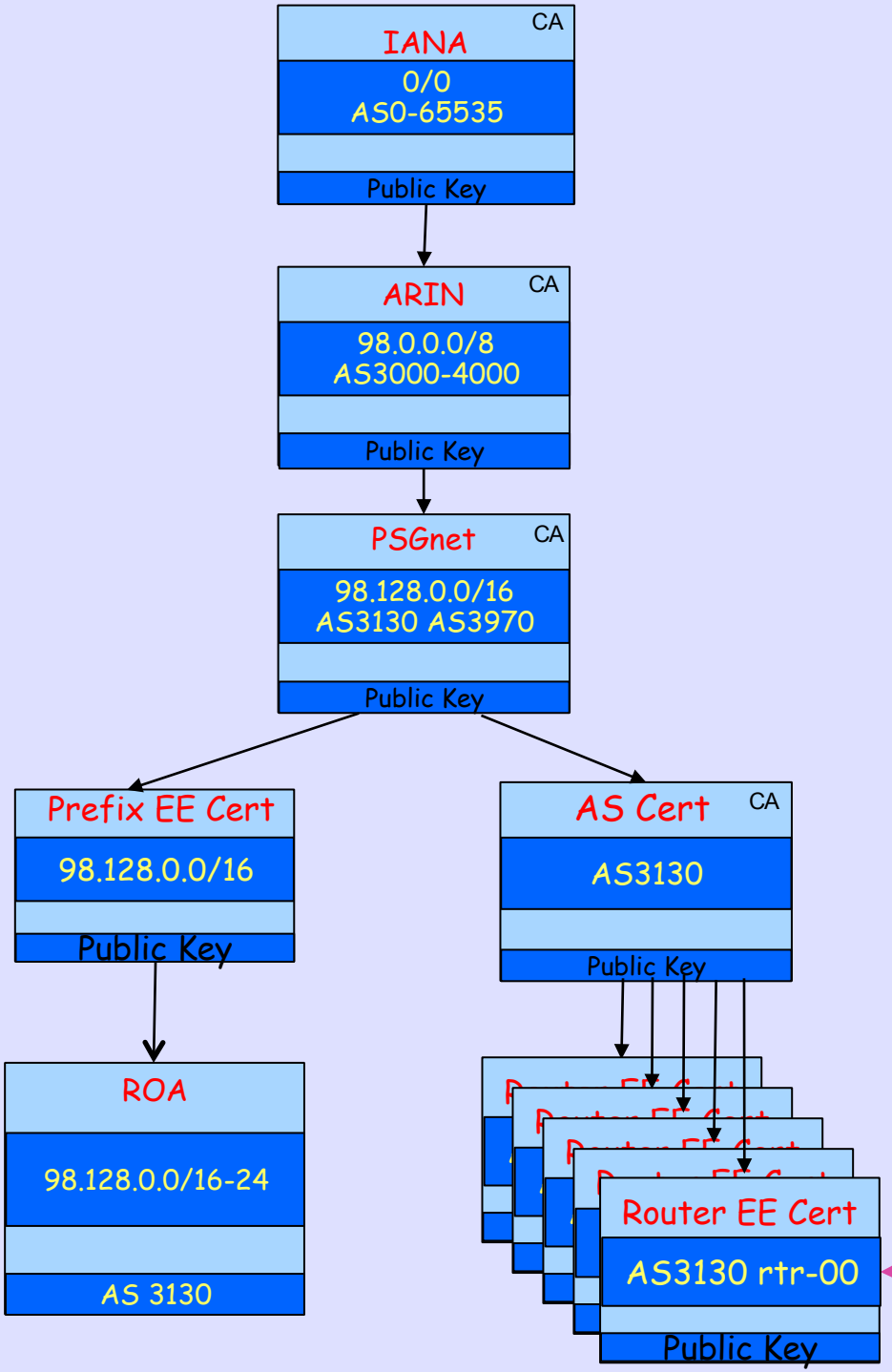
Replay Reduction

- 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

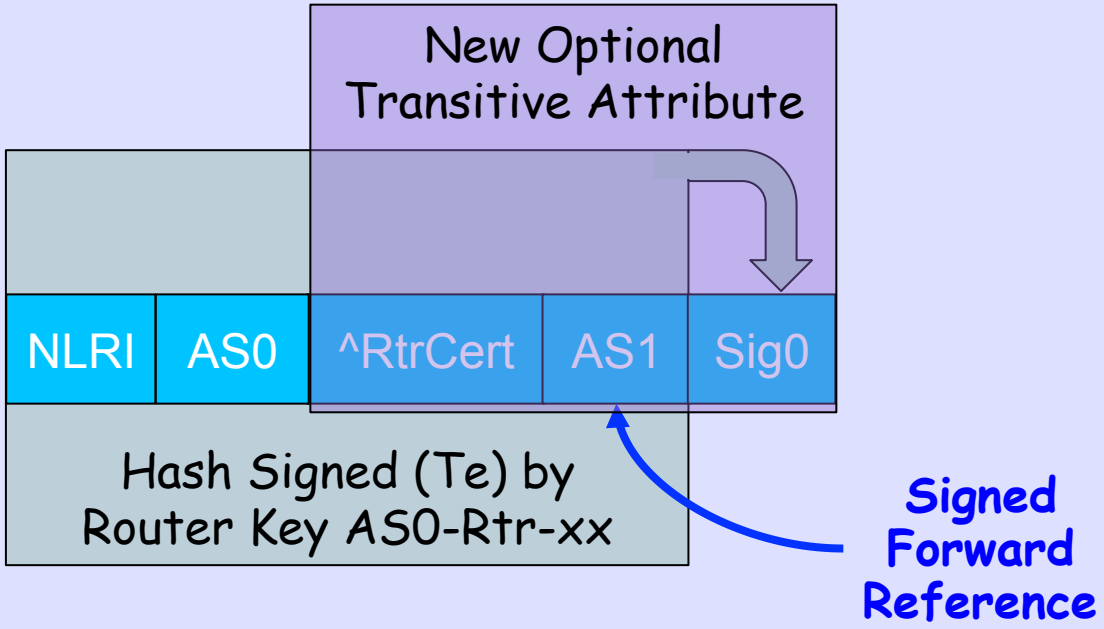
Per-Router Keys

- Needed to deal with compromise of one router exposing an AS's private key
- Implies a more complex certificate and key distribution mechanism
- A router could generate key pair and send certificate request to RPKI for signing
- Certificate, or reference to it, must be in each signed path element
- If you want one per-AS key, share a router key

Cert / Key Structure for an ISP

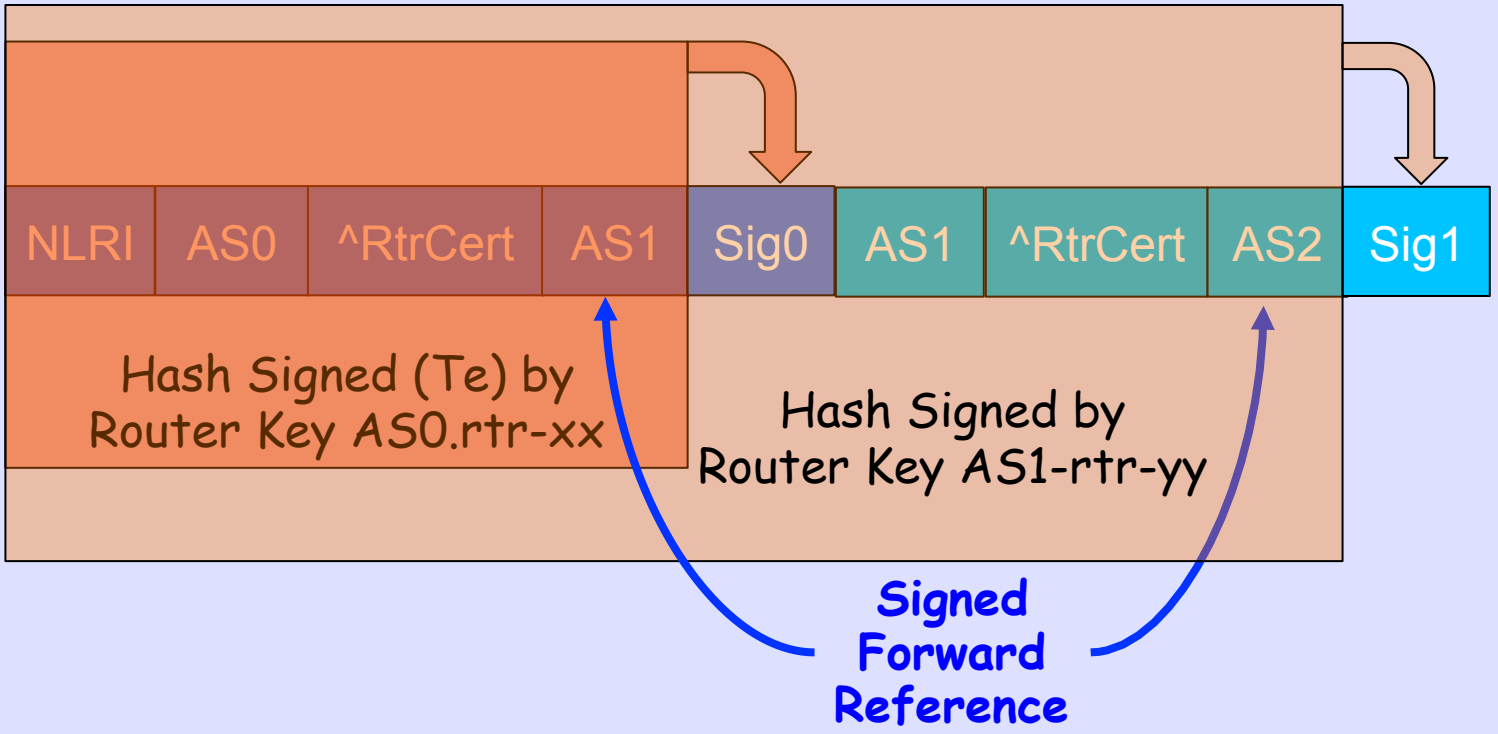


Origination by AS0 to AS1



- 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
- RtrCert is a reference to the signing router's certificate

Announcement AS1 to AS2

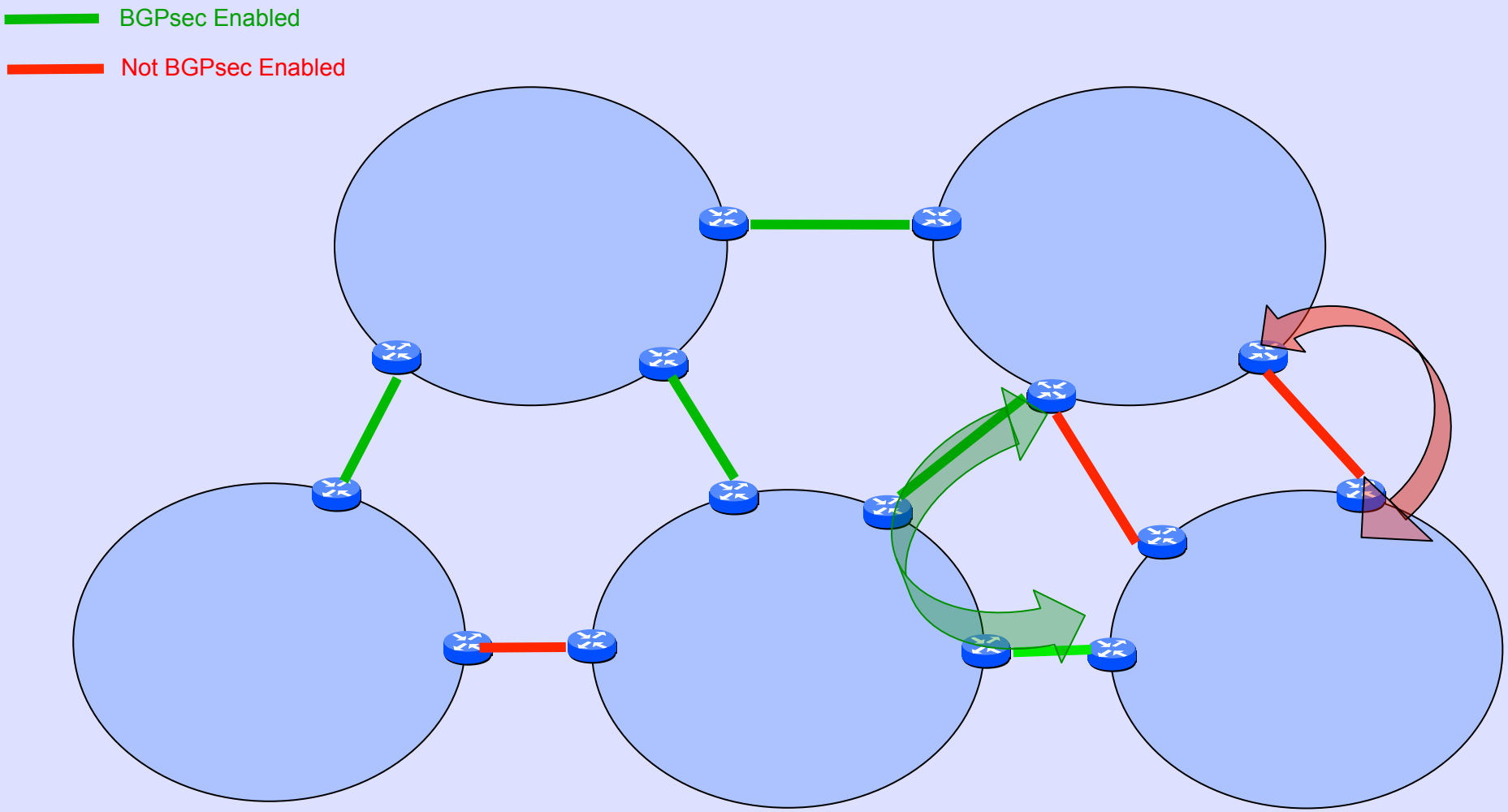


- Non-originating router signatures do not have validity periods
- But when they receive a beacon announcement, they must propagate it
- Therefore, non-originating routers do not re-announce, AKA beacon

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

Varied Peerings



Simplex End Site

- End Site can trust up-stream's policies
- But they want their origination signed
- So they announce capability to send but do not accept signed data
- They sign announcement and beacon
- This can be done without hardware upgrade!!

Incremental Deployment

Meant to be incrementally deployable in today's Internet, and does not require global deployment, a flag day, etc.

No Increase of Operator Data Exposure

- Operators wish to minimize any increase in visibility of information about peering and customer relationships etc.
- No IRR-style publication of customer or peering relationships is needed

iBGP & Confederations

- iBGPsec speakers who are also eBGPsec speakers naturally carry BGPsec data
- Route Reflectors must be non-signing iBGPsec speakers
- Confederations are eBGP boundaries, but a subAS should not sign to coreAS as that signature would have to be removed.

No Partially Signed Paths

- During incremental deployment, routers in the path may not be BGPsec capable
- A BGPsec capable router sending to one which is not BGPsec capable, does not pass, i.e. removes all, BGPsec data
- A BGPsec router receiving an unsigned path should not sign it when passing it on
- One can always tunnel past non-speakers

Only Prefix+AS-Path

- Until clear vulnerabilities demonstrate a need for more, only the prefix and the AS path are covered by the signature.
  - Other attributes are too variable, are ephemeral, or we do not understand the security needs.
  - I.e. don't sign what we don't understand.
- NO-EXPORT etc. are over a [secured] next-hop, and thus do not need signing.
  - Should all BGPsec links be over secure transport?

Utterly Un-Optimized

- This design very intentionally abjures premature, in fact any, optimization in an attempt to get the semantics of the protocol correct in a simple and understandable way
- It is assumed that optimization, prepends, packing, etc. will be worked out as the design is finalized

Crypto Flexible

- Choices among many hashing and other cryptographic algorithms, key lengths, etc. are assumed to be pro tempore and changeable as the the design is refined.
- Current design uses RSA-2048 and SHA-256
- Algorithm agility is built in
- But note that it is global, not hop by hop!

Uses Global RPKI

It is assumed that any needed global RPKI data can be delivered to routers (or ancillary devices) by augmenting the RPKI to Router Protocol described in draft-ietf-sidr-rpki-rtr-protocol, with the additional PDUs necessary to transport certificates, CRLs, etc.

Origin Validation Assumed

- We assume that prefix origin validation can be and/or is already being done by routers using ROAs from the RPKI
- We can leverage the ROA being in the router's prefix trie already, so need not include it in signed updates

Just Another BGP Decision

- The result of validation is similar to any other BGP decision
- Local policy decides what to do with the result of validity testing, a la origin validation
- And the vendors will give the ops too many knobs

Ideal BGPsec Consequences

New Hardware Generation

It is likely that routers will have to be upgraded to use this design, likely with much more memory and probably with hardware crypto assistance. It is accepted that this means that it will be some years, O(IETF process) before there is more than test deployment

No PDU Packing

- This 'idealized' protocol has only one prefix in each announcement PDU
- Routers currently unpack prefixes from PDUs, and subsequent re-announcement repacks and reorders rather arbitrarily
- PDU optimization can be studied after the protocol semantics are solid

Peer Groups

- A peer group signature would need to be over all ASNs in the forward AS set
- This would divulge relationships globally
- Therefore final processing for each peer must add that peer's AS and sign it
- Or give up peer groups as other than configuration syntactic sugar

Route Servers

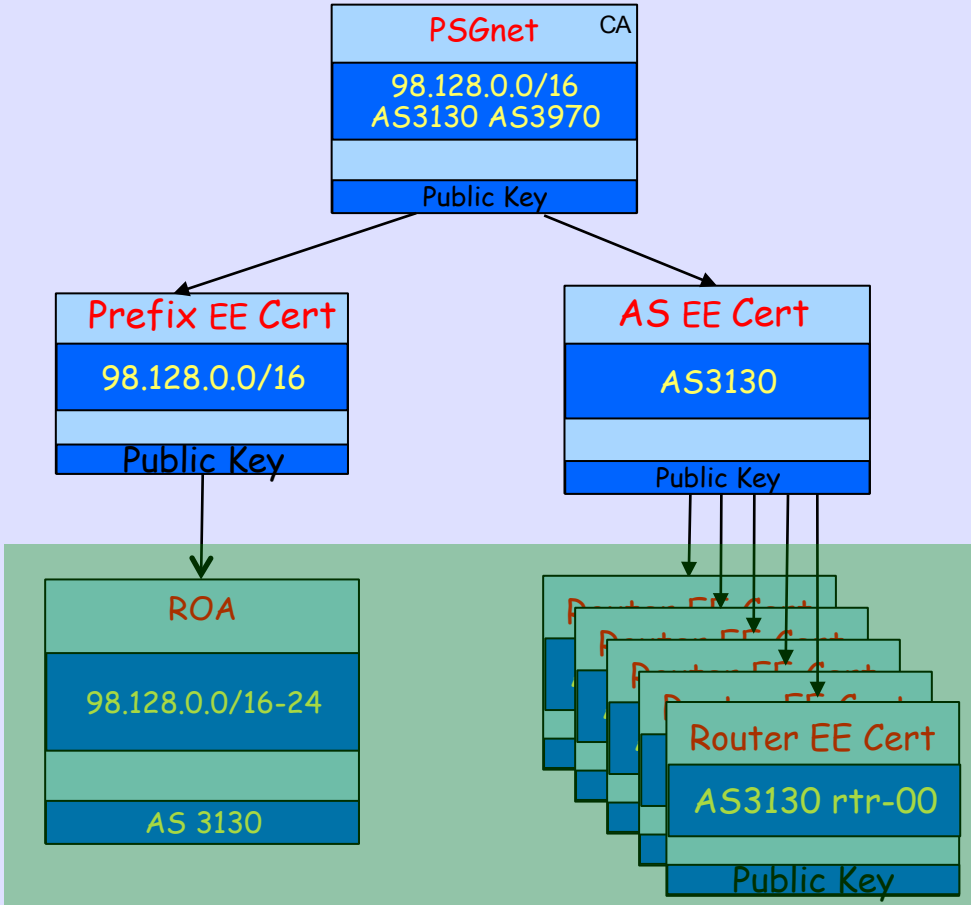
Can't BGPsec forward sign across an AS-transparent route server as you do not know the peerAS

Proxy Aggregation

Proxy Aggregation, i.e.

AS-Sets, is not supported

Expiration Could be Noisy



Expiration and Re-Issue of these ROAs & Router Keys Could Cause a Lot of Global BGP Noise

RPKI Signature Expiry

Notification/warning to owners of aging certificates becomes very important

Does Not Lock Data Plane

- It is acknowledged that rigorous control plane verification does not in any way guarantee that packets follow the control plane
- See IMC 2009 paper which shows that 70% of the ASs in the so-called 'default free zone' also have default

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)

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