

RPKI-Based Origin Validation, Routers, & Caches

JaNOG / Osaka
2013.07.03

Randy Bush <randy@psg.com>
Rob Austein <sra@hactrn.net>
Michael Elkins <me@sigpipe.org>

Agenda

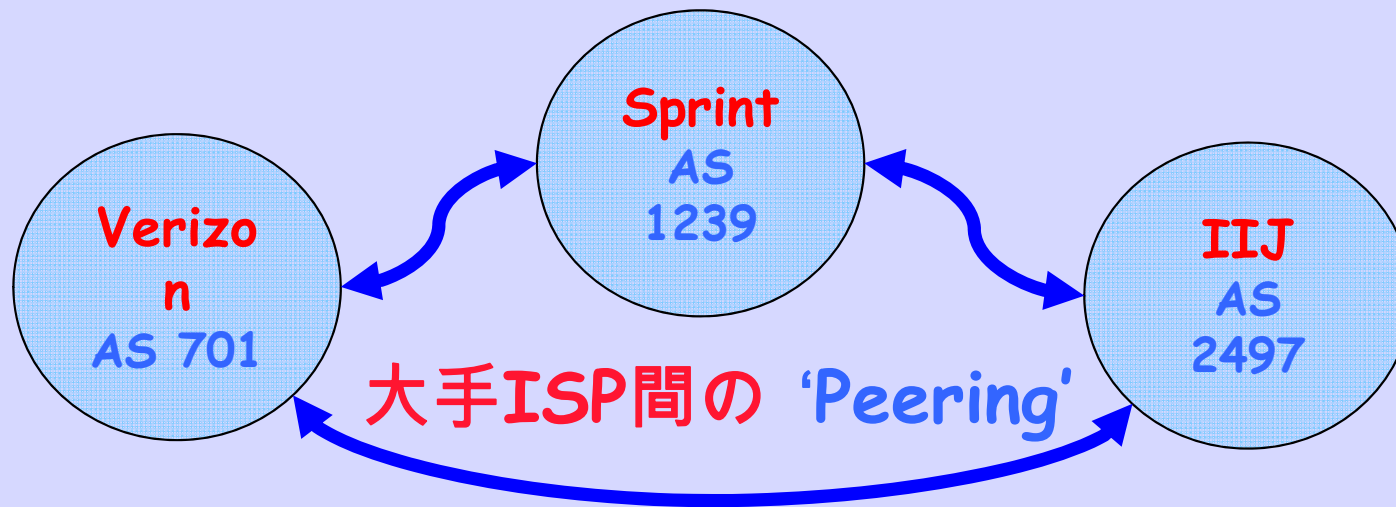
- 技術的な背景
- Mis-Origination - YouTube 事件
- The RPKI - 必要な技術基盤
- RPKI-Based Origin Validation
- GUIを利用したROAの作成とルータでの見え方
- RPKIに関する体験後の議論

最近始まったものではない

- 1986 - Bellovin & Perlman がDNSとRoutingでの脆弱性を特定
- 1999 - National Academies 調査で取り上げた
- 2000 - S-BGP - X.509 PKIでのSecure BGP対応
- Kent, Lynn, et al.
- 2003 - NANOG S-BGP Workshop
- 2006 - RPKI.NET(for ARIN) & APNIC がRPKIに向けた対応開始. RIPE は2008年より開始.
- 2009 - RPKI.NET でTestbed と試験ルータへの
running code を提供

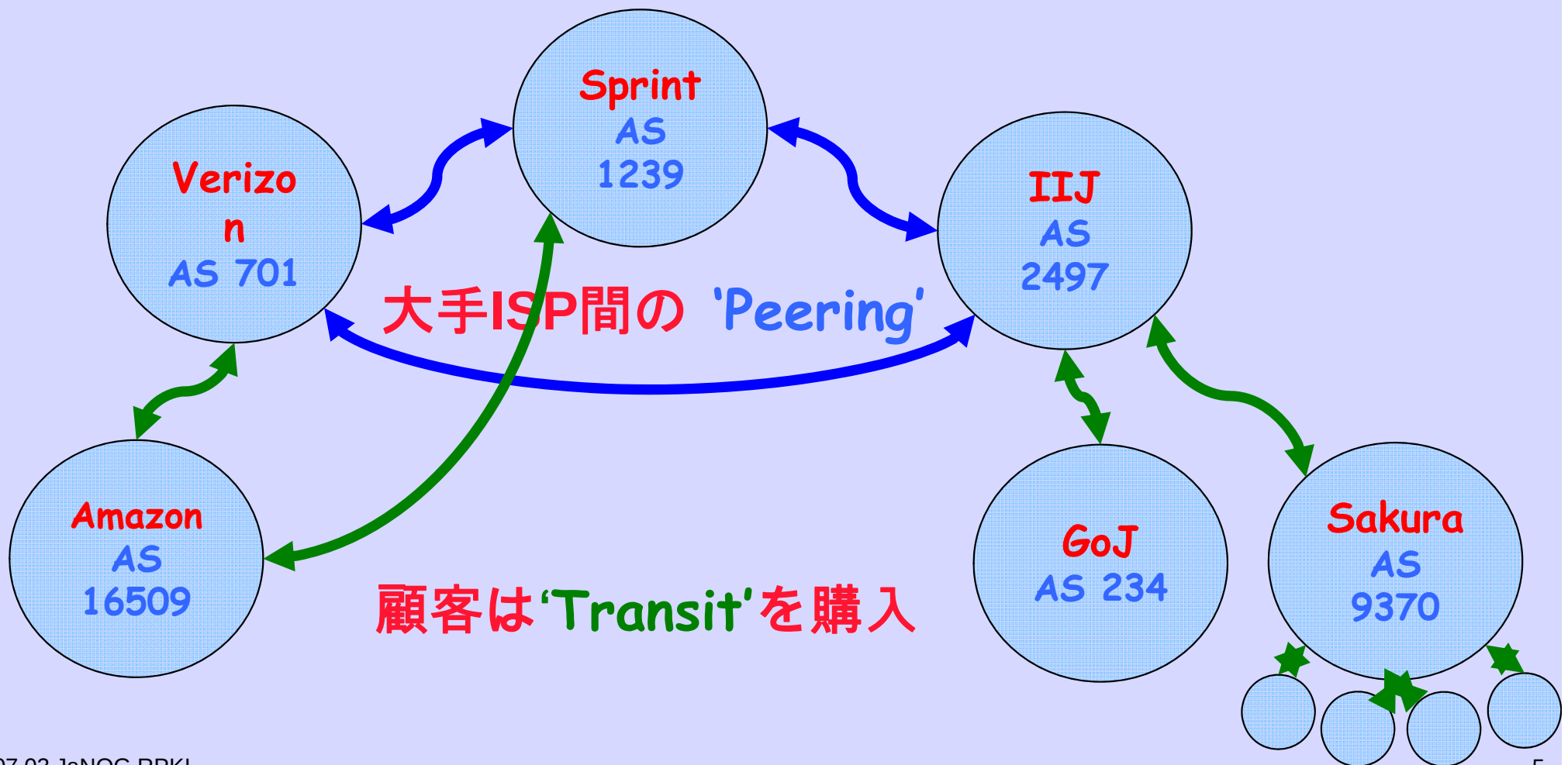
What is an AS?

An ISP or End Site

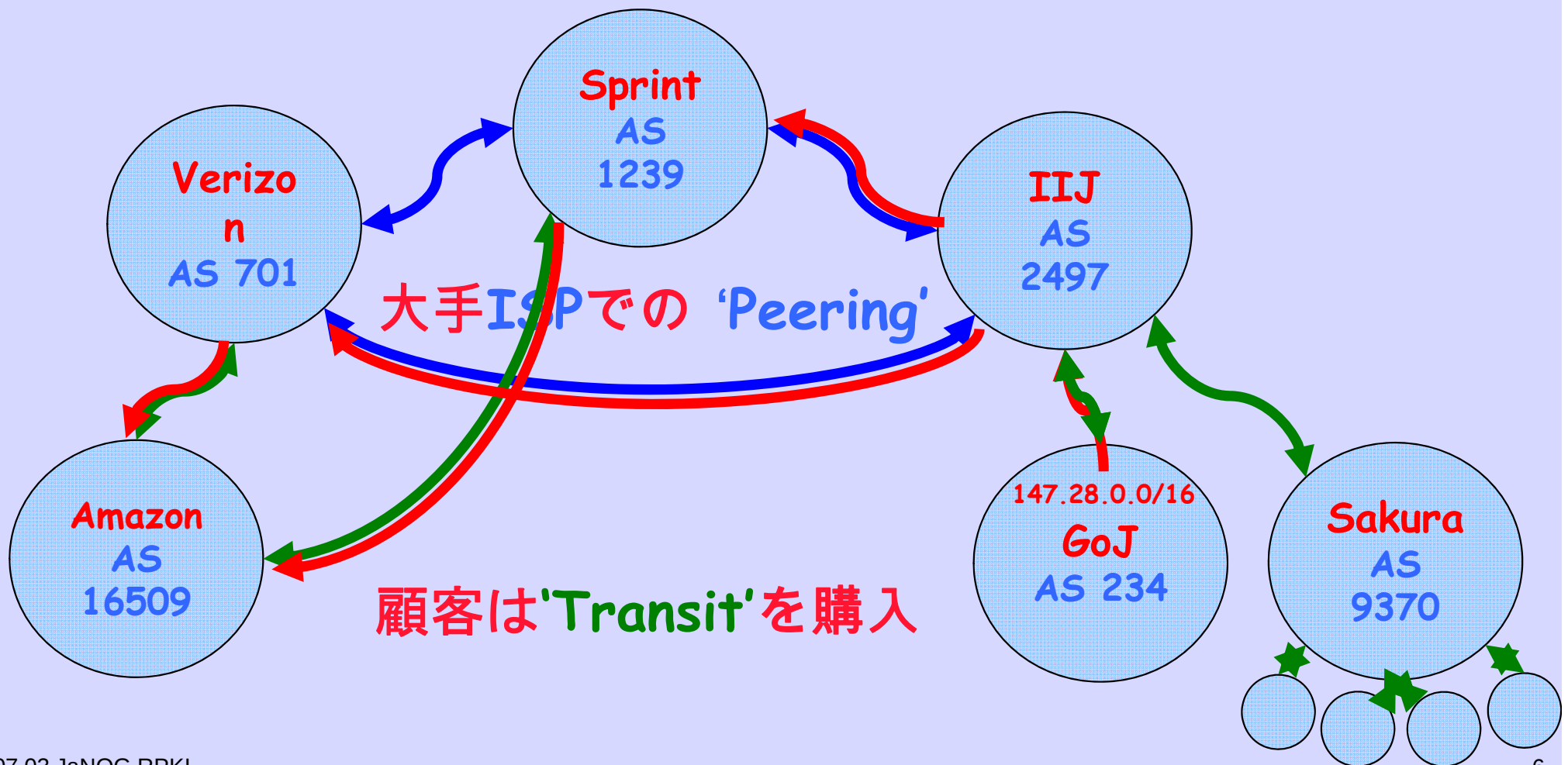


What is an AS?

ISPや企業等エンドサイト



IP Prefixは広告され、徐々に伝播されていきます



Routerの中では

BGP routing table entry for **147.28.0.0/16**



実機ではこう見えたり😊

```
r1.iad#sh ip bgp 147.28.0.0/16
```

```
BGP routing table entry for 147.28.0.0/16, version 21440610
```

```
Paths: (2 available, best #1, table default)
```

```
  Advertised to update-groups:
```

```
    1
```

```
Refresh Epoch 1
```

```
16509    1239    2497    234
```

```
  144.232.18.81 from 144.232.18.81 (144.228.241.254)
```

```
    Origin IGP, metric 841, localpref 100, valid, external, best
```

```
    Community: 3297:100 3927:380
```

```
    path 67E8FFCC RPKI State valid
```

```
Refresh Epoch 1
```

```
16509    701    2497    234
```

```
  129.250.10.157 (metric 11) from 198.180.150.253 (198.180.150.253)
```

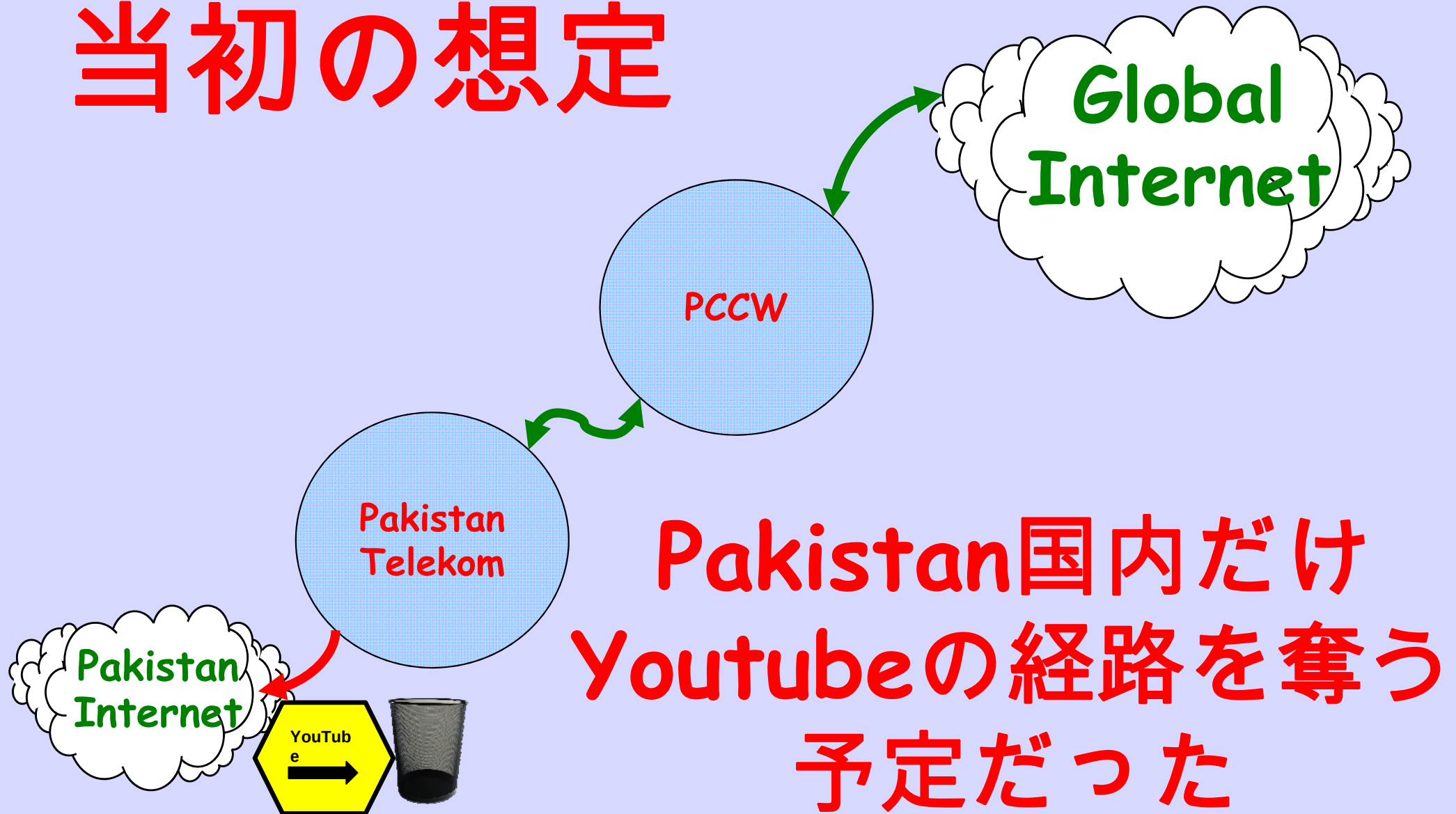
```
    Origin IGP, metric 95, localpref 100, valid, internal
```

```
    Community: 2914:410 2914:1007 2914:2000 2914:3000 3927:380
```

```
    path 699A867C RPKI State valid
```

The YouTube 事件

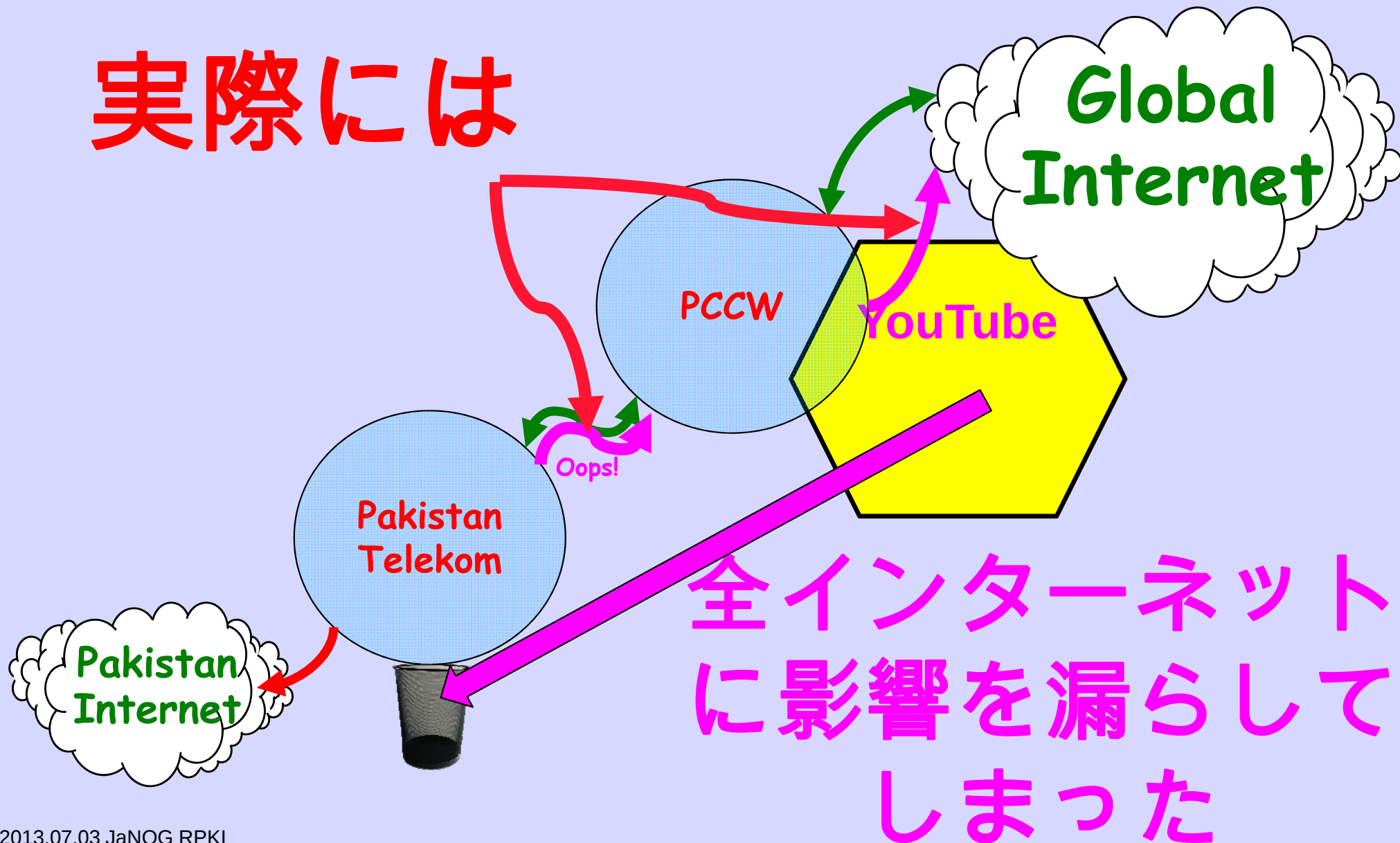
当初の想定



Pakistan国内だけ
Youtubeの経路を奪う
予定だった

The YouTube 事件

実際には



これを

Mis-Origination

と呼んでいます

IPアドレスの保持者では
ないASによる経路の
Originate

Hijackingとは言いません

意図的な悪意がある印象を
与えるため

このような事件は頻繁に
発生しています

だいたい小規模です
たまに大規模になります

さて、 どうしましょう

3つの技術要素

- **RPKI** - 他の要素をサポートするPKIの基盤 (すべてのRIRsでは対応済み)
- **Origin Validation** - RPKIを使ってmis-originationを検知 (普及進行中)
- **AS-Path Validation AKA BGPsec** - BGP AS-PATH攻撃に対応 (将来対応)

Why Origin Validation?

- YouTube事件やそれよりひどい事件を防ぐ
- AS7007事件を防ぐ, UUnet/Sprint 2 days!
- 経路広報に関する様々な問題を防ぐ
- Kapela/Pilosov DefCon attackのような悪意を持つAS-PATH攻撃は防げない
- そのような攻撃を防ぐにはPATH Validationが必要であるが準備に数年が必要

ルーティング運用者は、誰
がIP Prefixの保持者で、
どのASがそのPrefixを経
路広報してよいか、正当性
の証明が求められている

Prefixの所有権はIPアドレス 割り振り階層にしたがっ ている

(訳者注：アドレスに所有権という表現は賛否あるが、原文を尊重)

そこで！

X.509-Based IP Resource PKI

RFCはいっぱい発
行されてきた

すべてのRIRに
普及した

ROAは1000以上の経路
運用者によってすでに
作成されている

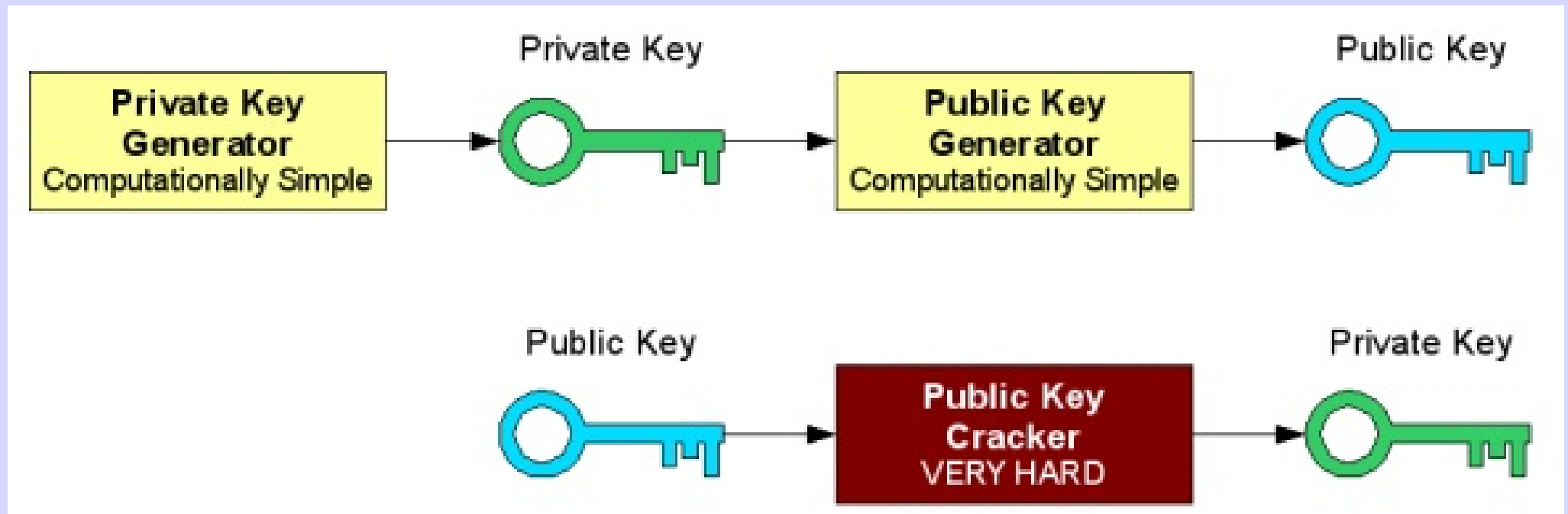
実環境のルータは？

Public-Key Concepts

- **秘密鍵:** この鍵はその保持者しか知らない。
- **公開鍵:** この鍵は万人に知られる。(それゆえ公開)
- **relation between both keys:** ひとつの鍵は暗号化、ほかの鍵は復号に使う。誰かが私の公開鍵で何かを暗号化したら、私は私の秘密鍵で何かを平文に戻します。

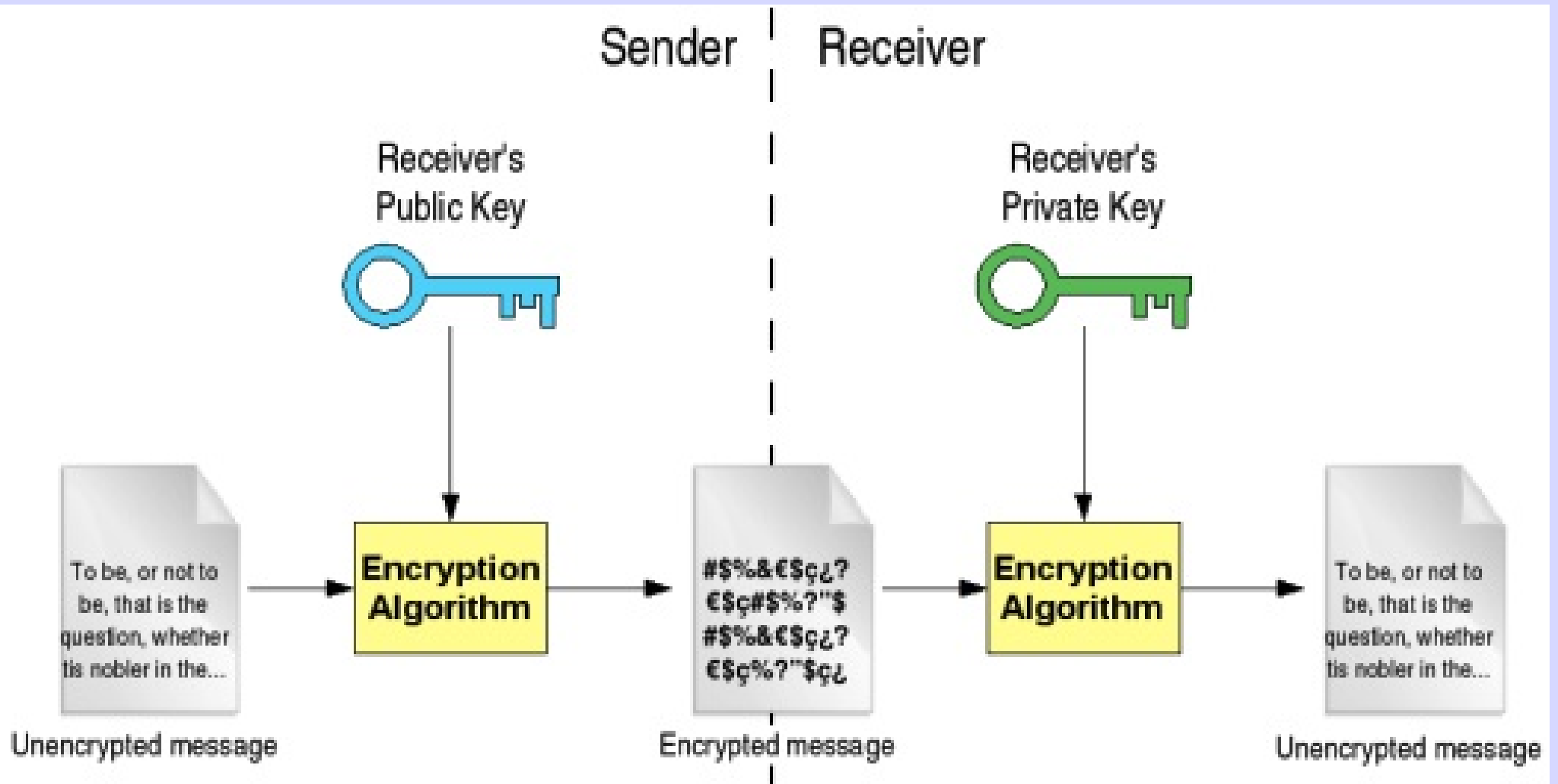
鍵の生成

公開鍵から秘密鍵の推測は困難

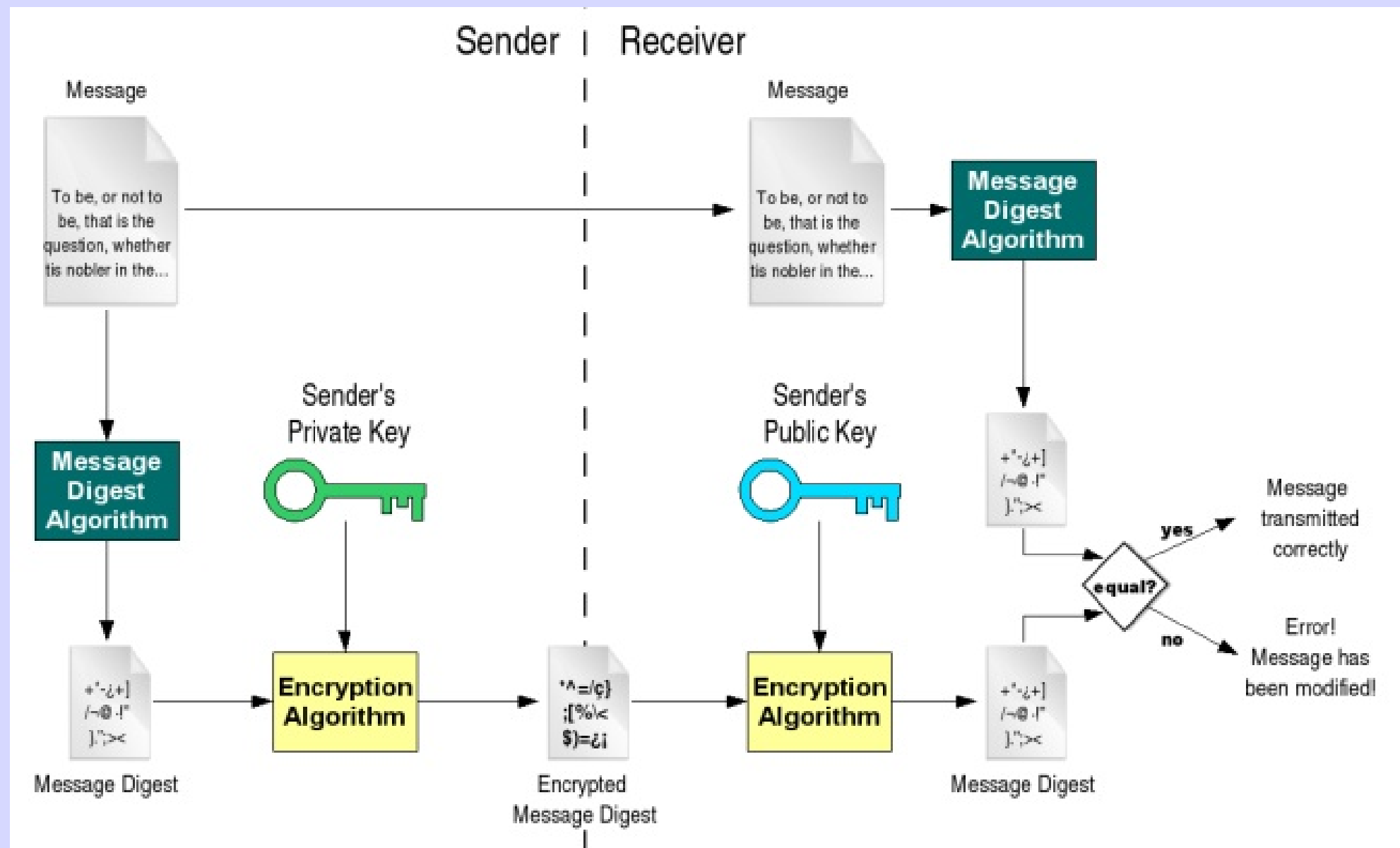


Stolen from - <http://gdp.globus.org/gt4-tutorial/multiplehtml/ch09s03.html>

暗号化・復号

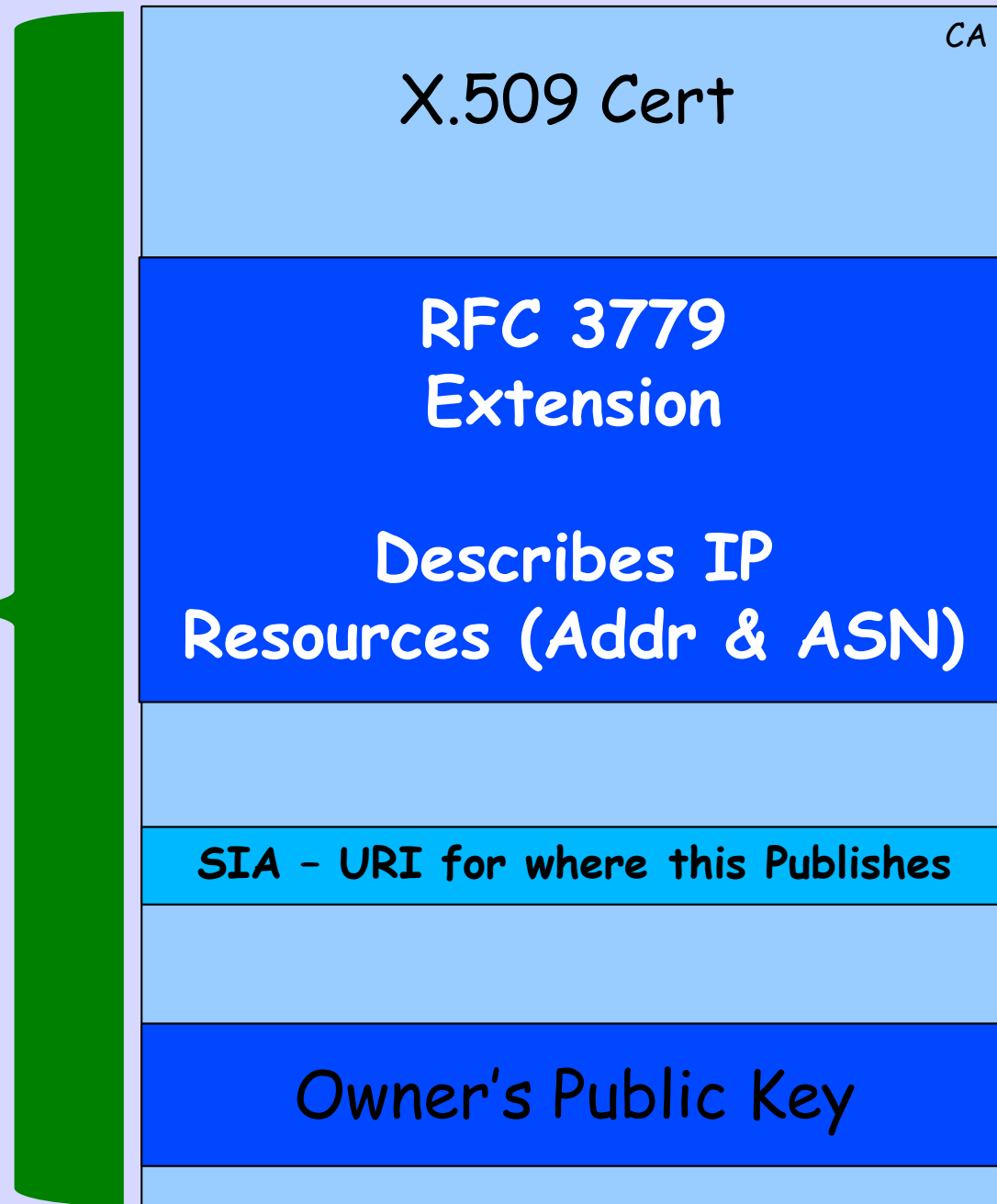


デジタル署名

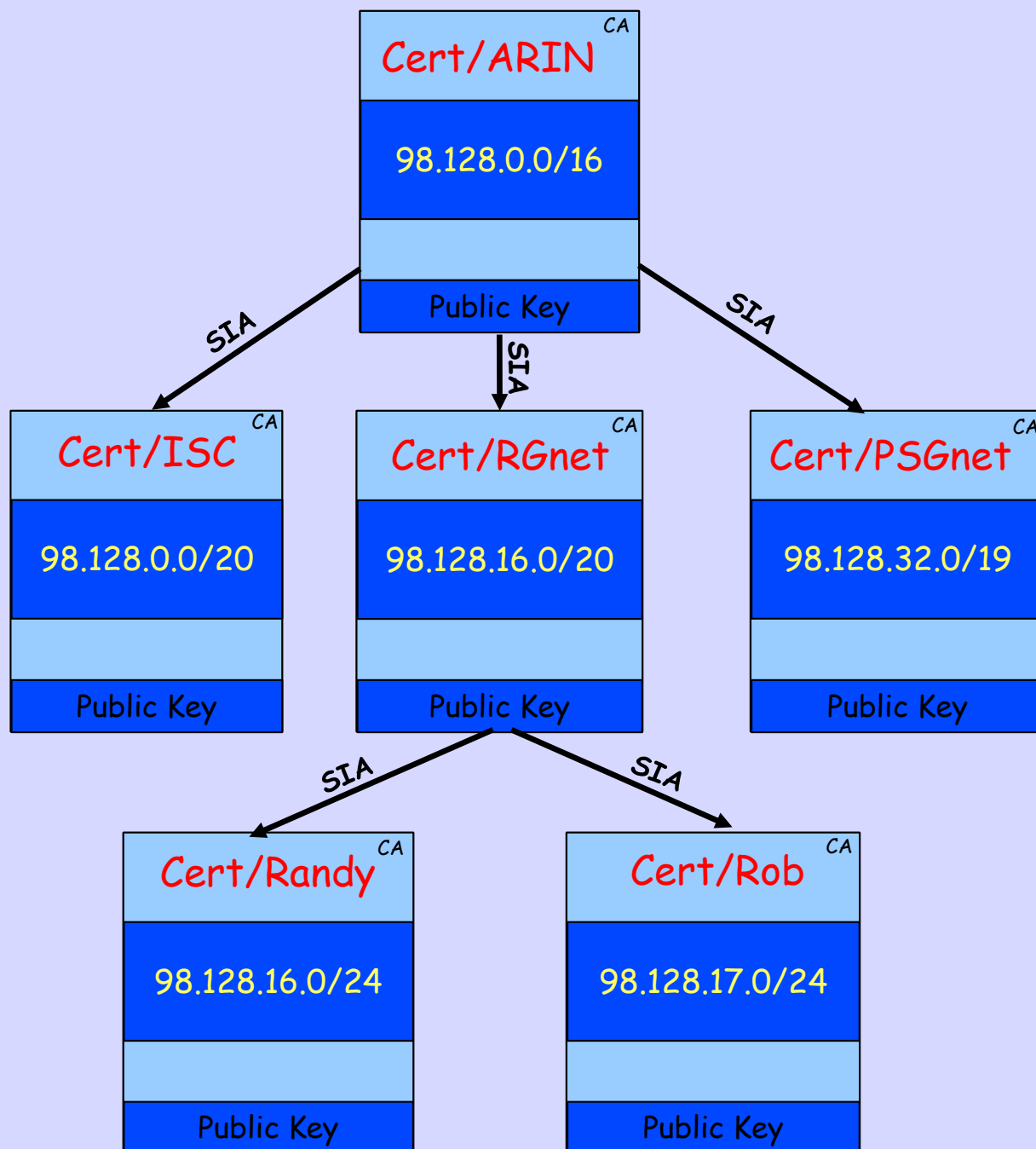


X.509 証明書とRFC3779拡張

Signed
by
Parent's
Private
Key

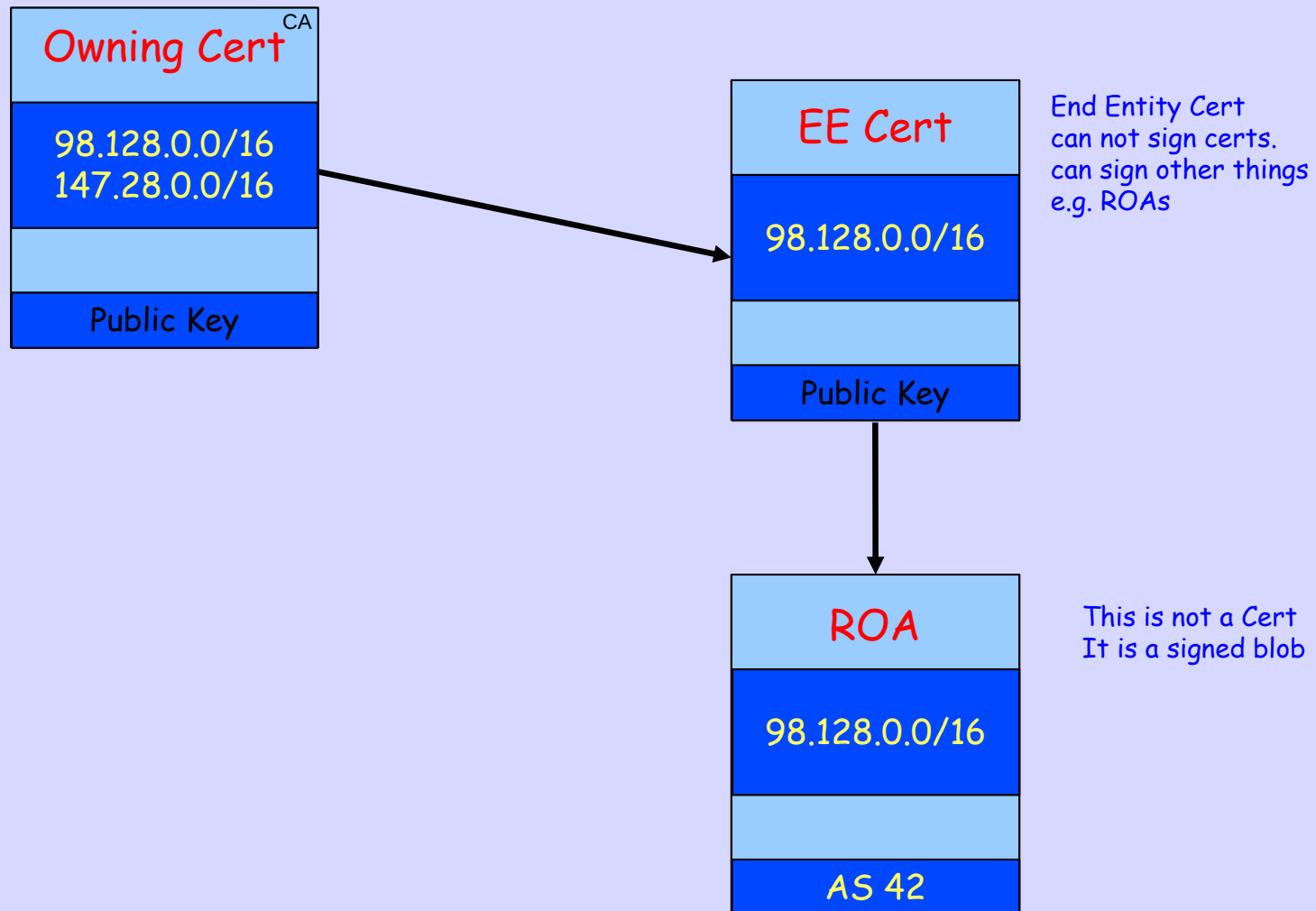


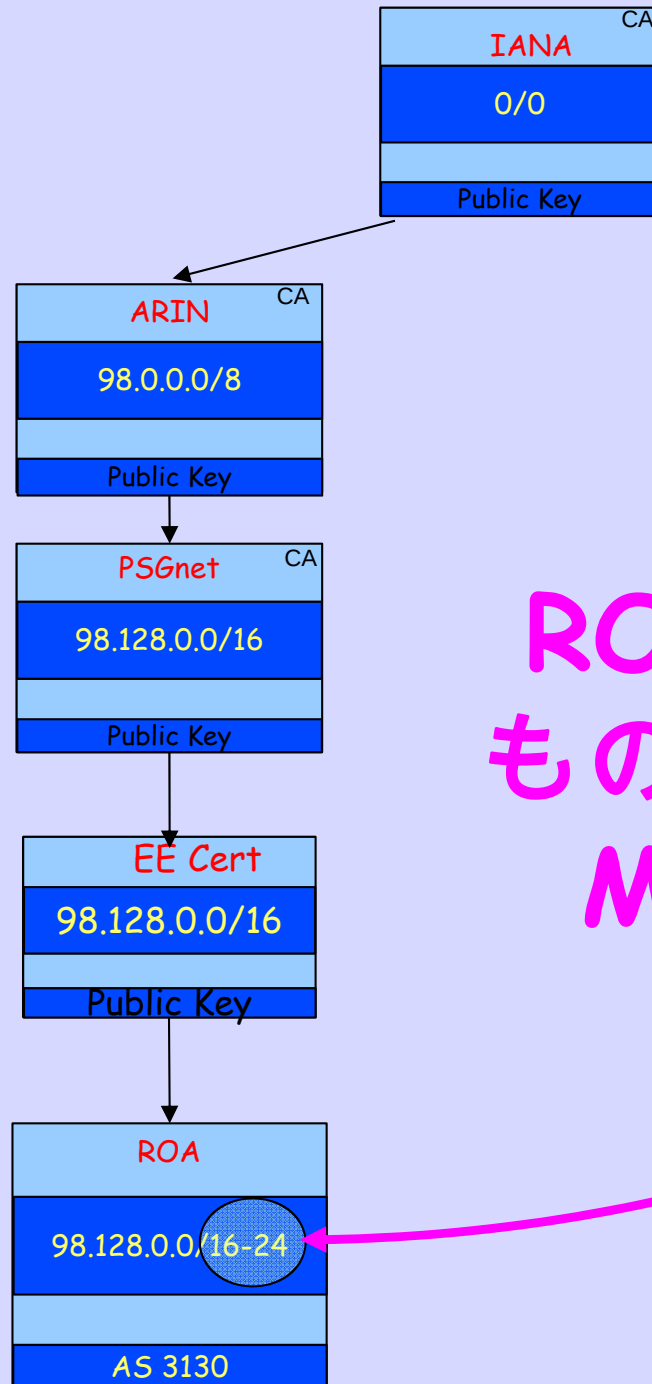
アドレス管理 階層に則る 証明書構造



誰がアドレスの所有者か
わかった
で、誰がルーティングして
いいの？

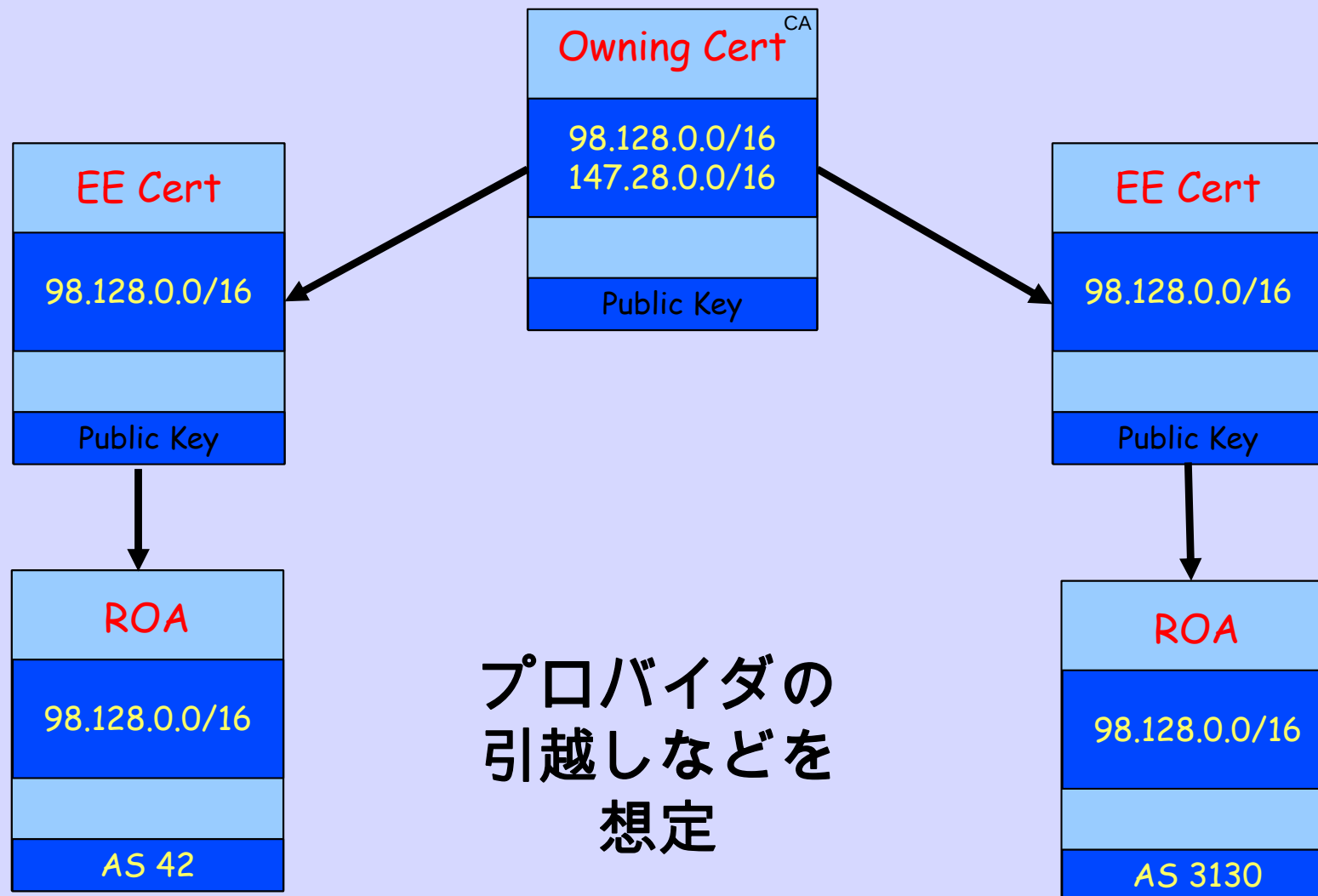
Route Origin Authorization (ROA : 発音 : ロォアー)



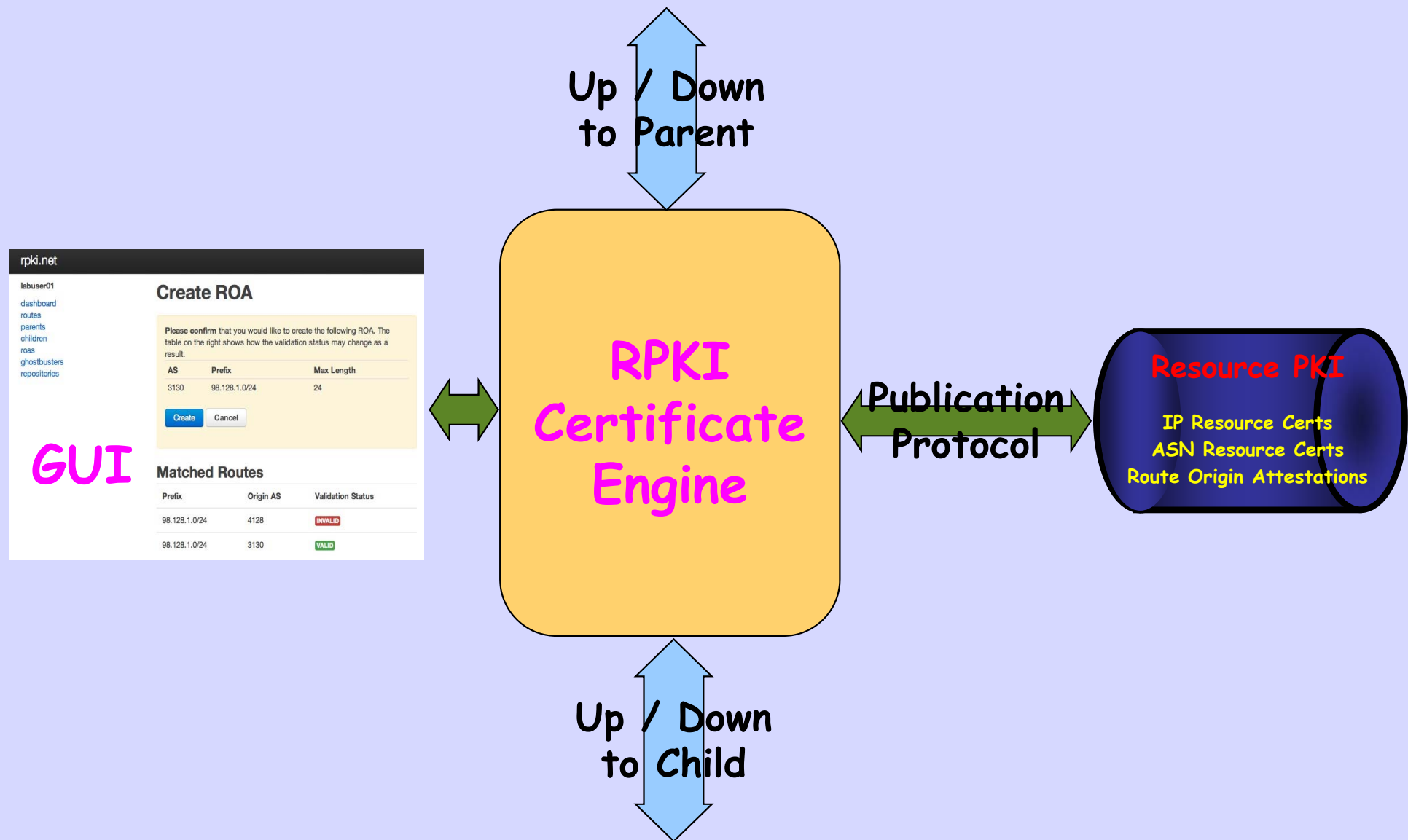


ROAはPrefix長の違う
ものをまとめて表現可能
Max Prefix Length

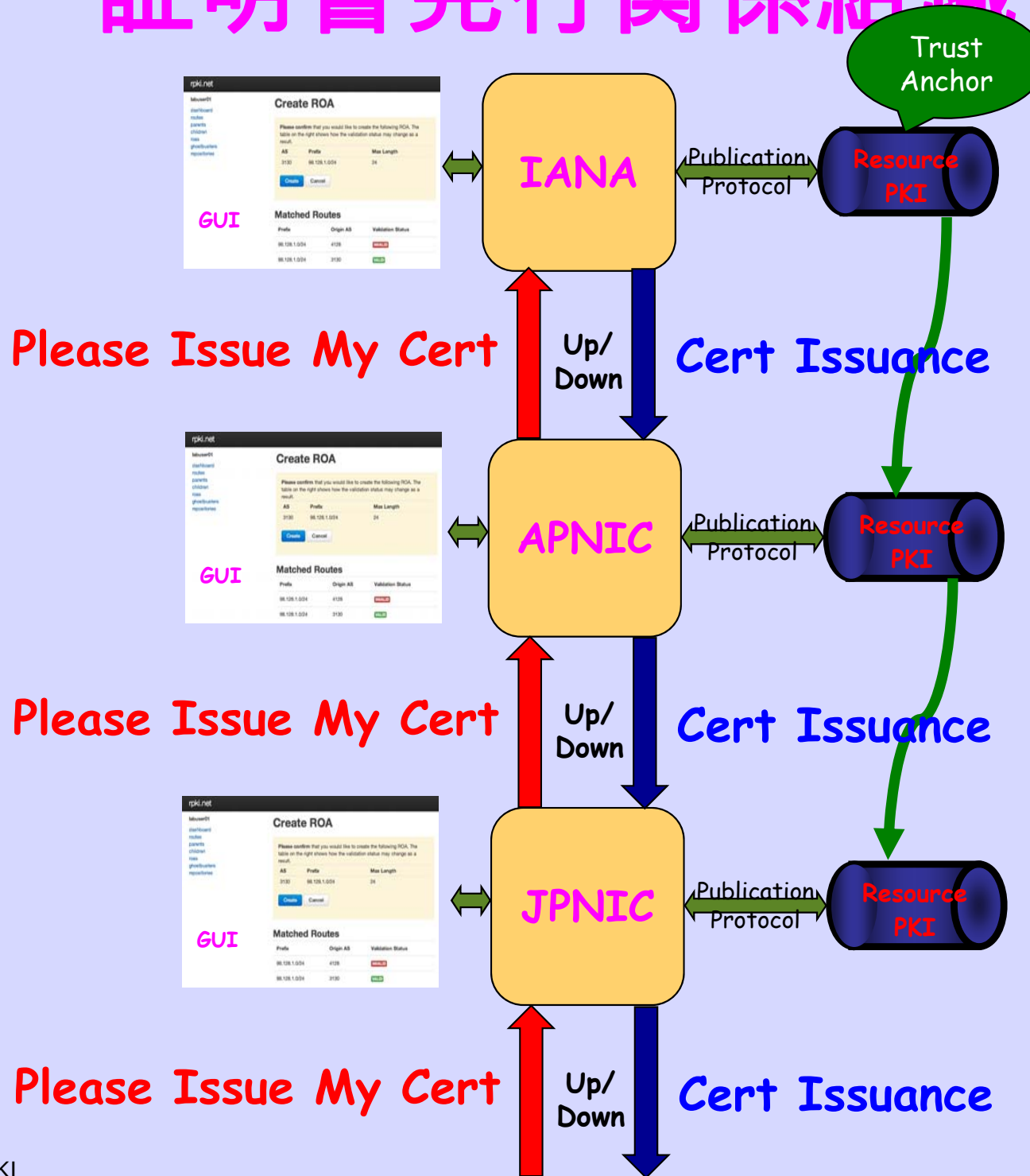
複数 ROAsの生成例



RPKIの生成のされ方



証明書発行関係組織



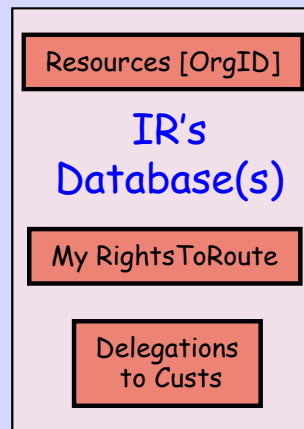
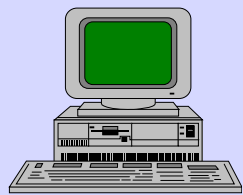
誰かの傘下 vs 自ら委任受ける



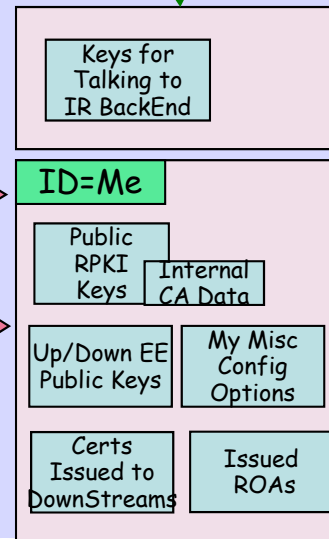
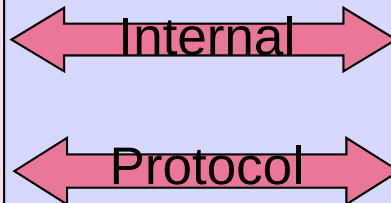
GUI

Hosted
Web GUI

98% of an RIR's Users
10% of an RIR's IP Space



Local Data
Management



RPKI
Engine



Contract
Out?

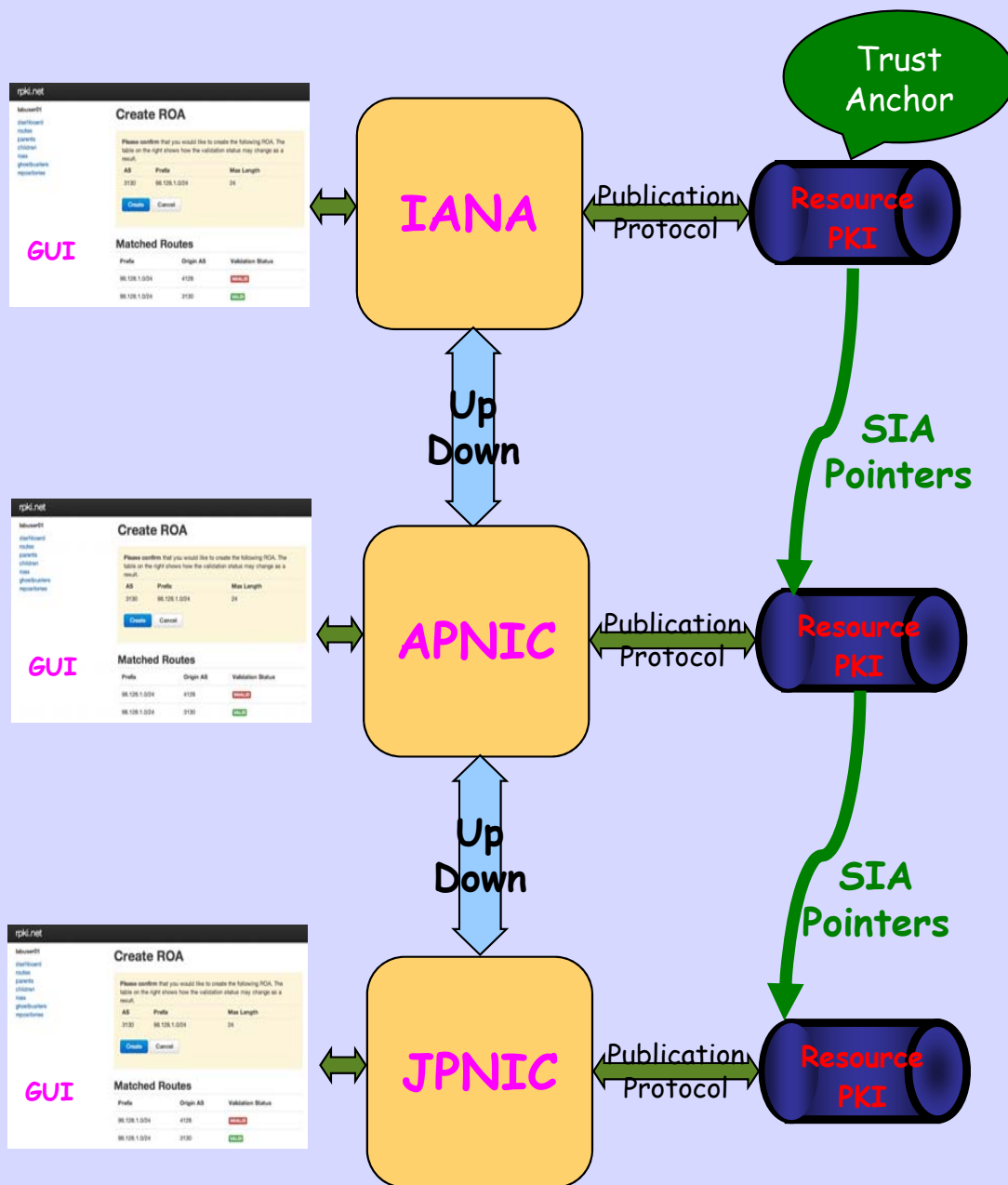


Delegated
a la DNS

Up / Down
Protocol

2% of an RIR's Users
90% of an RIR's IP Space

証明書発行組織



Trust Anchor Locator (ルート証明書のロケーター)

`rsync://ca0.rpki.net/tal/root.cer`

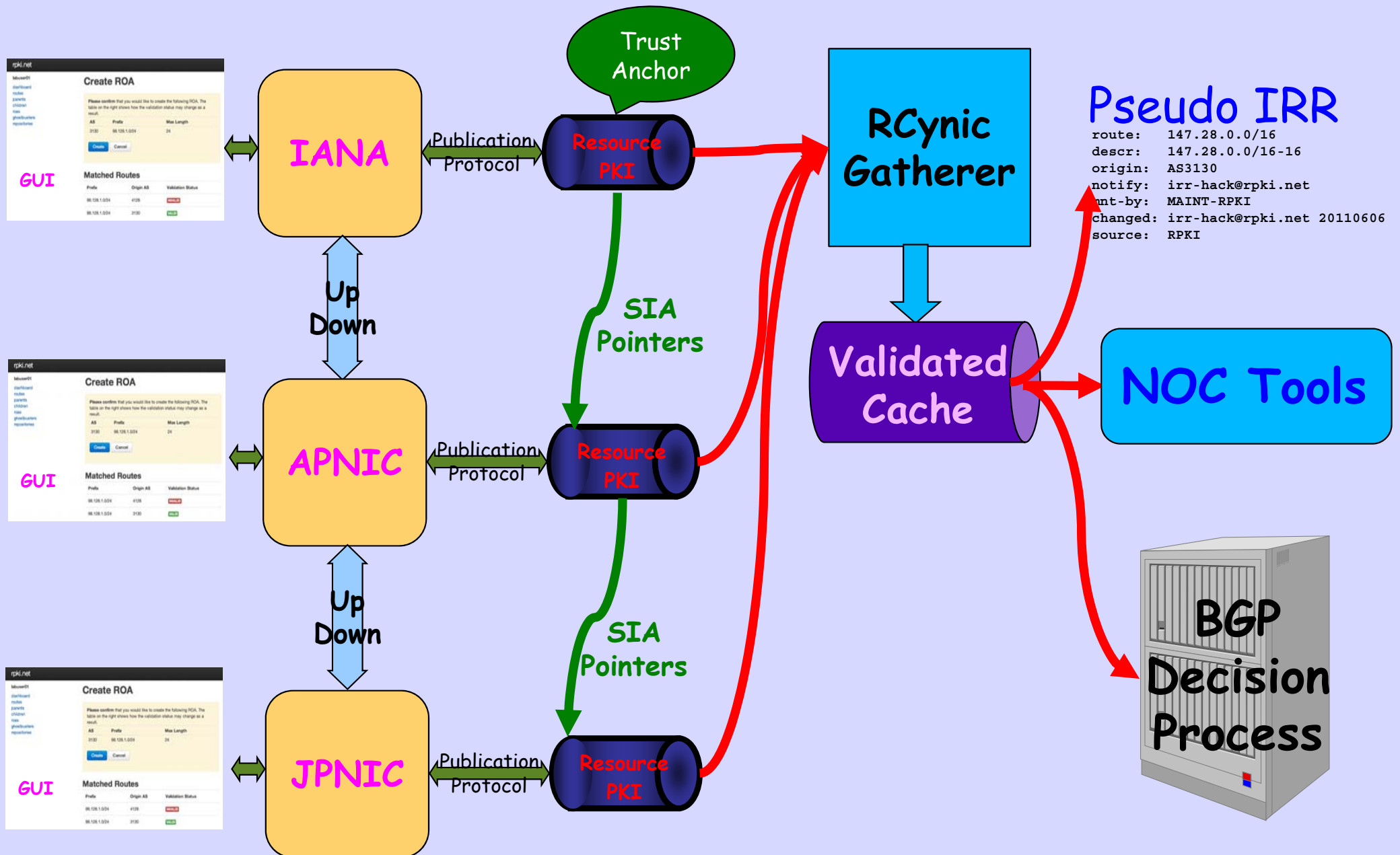
```
MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAzPSPpQxa0rxz9sbbvYGr
UlpgyBVxSIt+k/WDKbr+VW7CjUoz6cc5KMFANKQWw3D6ER4kCwX4WJkD58AGGbw/
WeAe6m3aHcORUVRkr45a4qSrYiG7Wq9RAXtwbhlXofB3zo+O90IIXDaVP2U9bw+Q
yoJBJuAmZONt0bRgrktv8QhVtKvuYkH5ZIE7DkXJcJzBn6gv09dZsdwZm3xV3soX
HEKrz5pY6Sb2xoL1CyPqzGOfVFxl0G5+dmcD/degPKxrEycAzjnHUzN1gus2jg26
dtkix7KG/Mn1h/k53j0FdQD+zqPwakgwqjvCOdSdHMRmsikj0EF9WrZIOjZUXV6q
6wIDAQAB
```

あなたが信頼する認証局のURLとその認証局証明書の検証が可能な公開鍵のセット

A URL and a Public Key that must be able to Decrypt
the Certificate that is found at the URL so you
know you can trust it

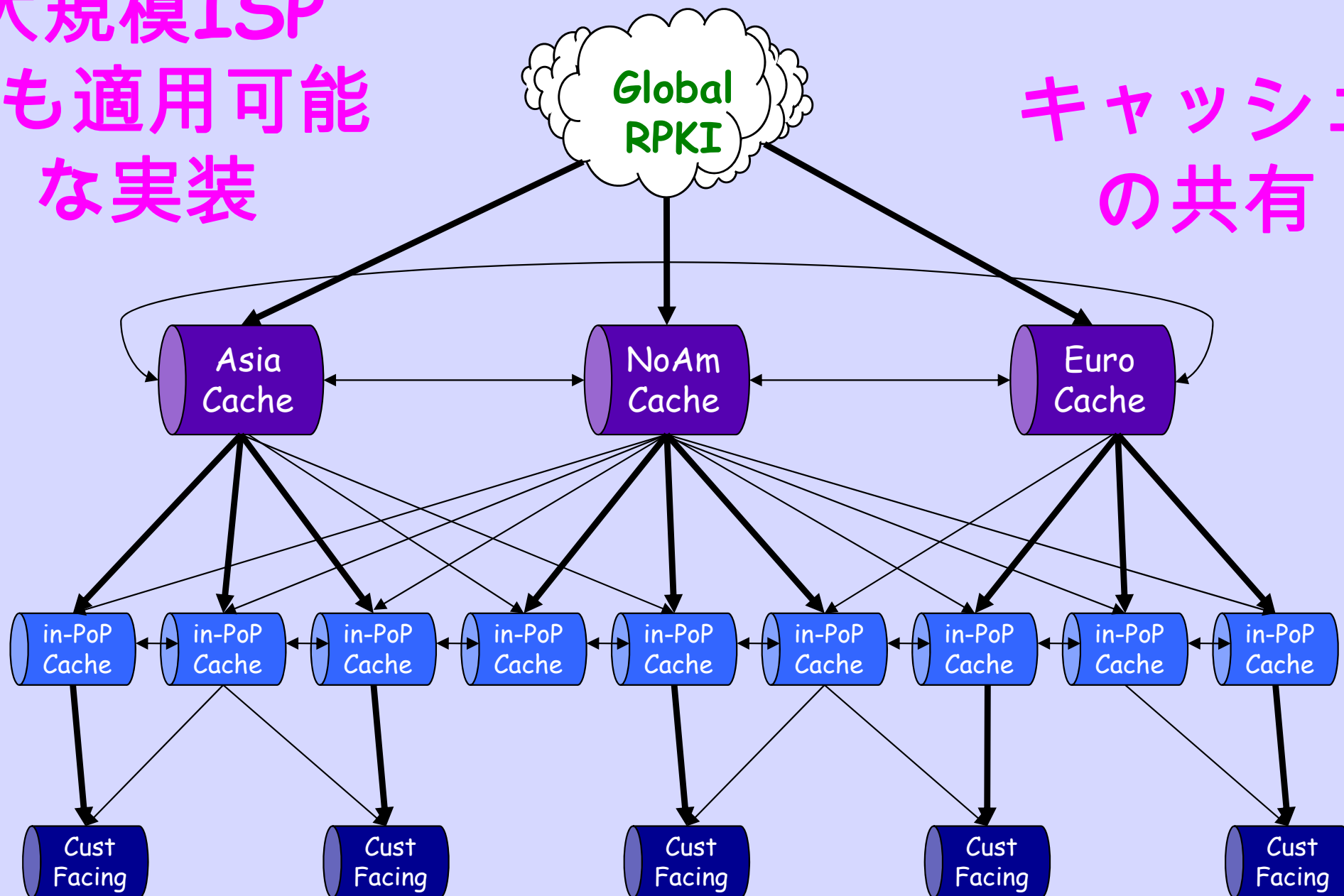
証明書発行組織

利用組織



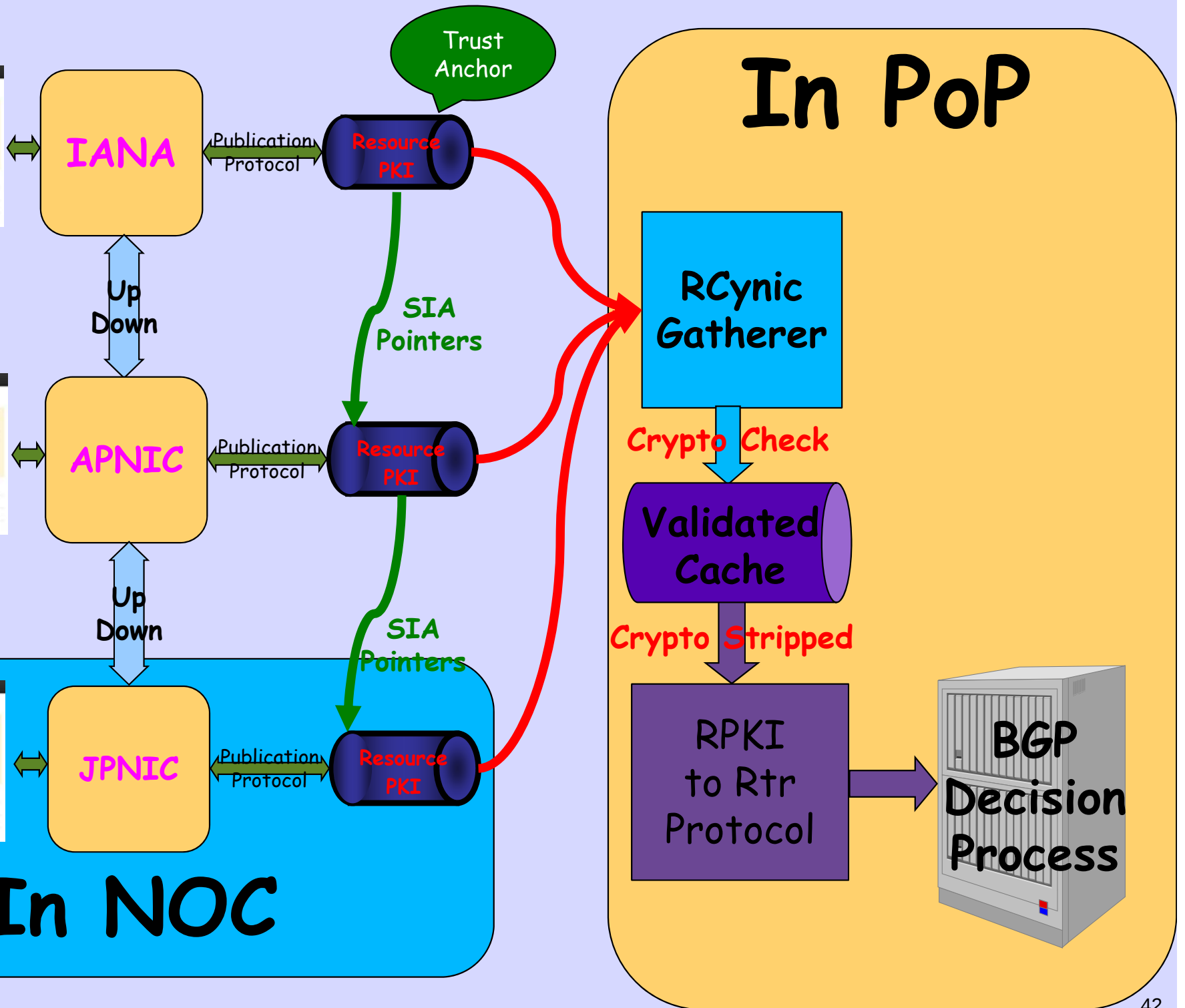
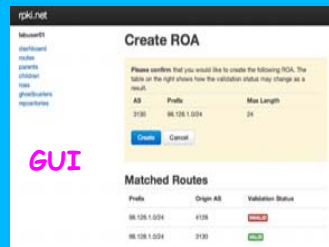
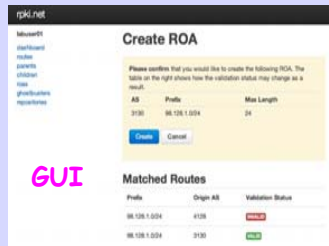
大規模ISP にも適用可能 な実装

キャッシュ
の共有



———— High Priority
———— Lower Priority

ROAsはBGPのUpdate
に、どのように
影響するのか



ROAs Become Router VRPs (VRP: Validate ROA Payloads)

既存のハードウェアで
実行したい

RPKI-Rtr
Protocol



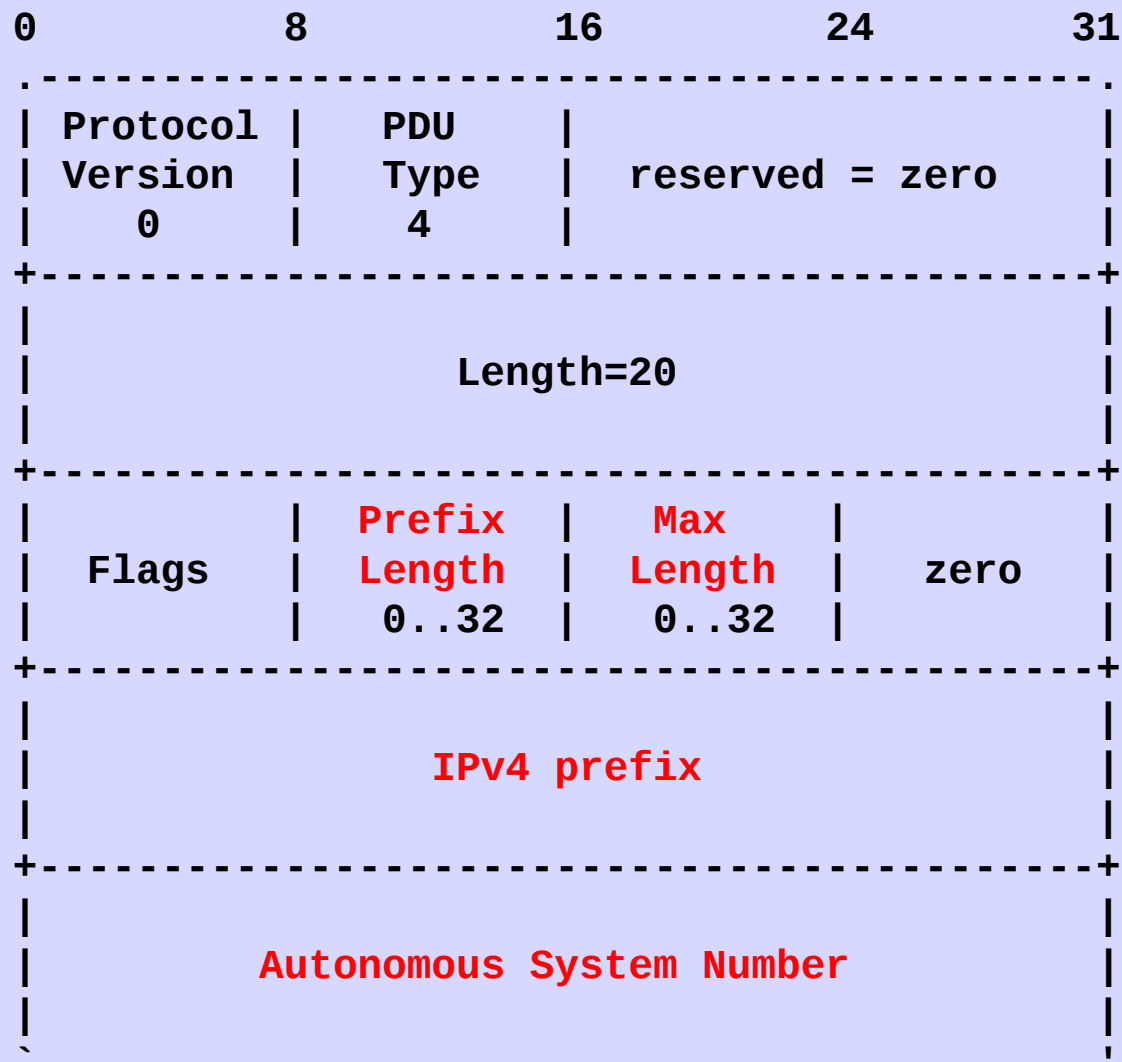
RPKI
Cache



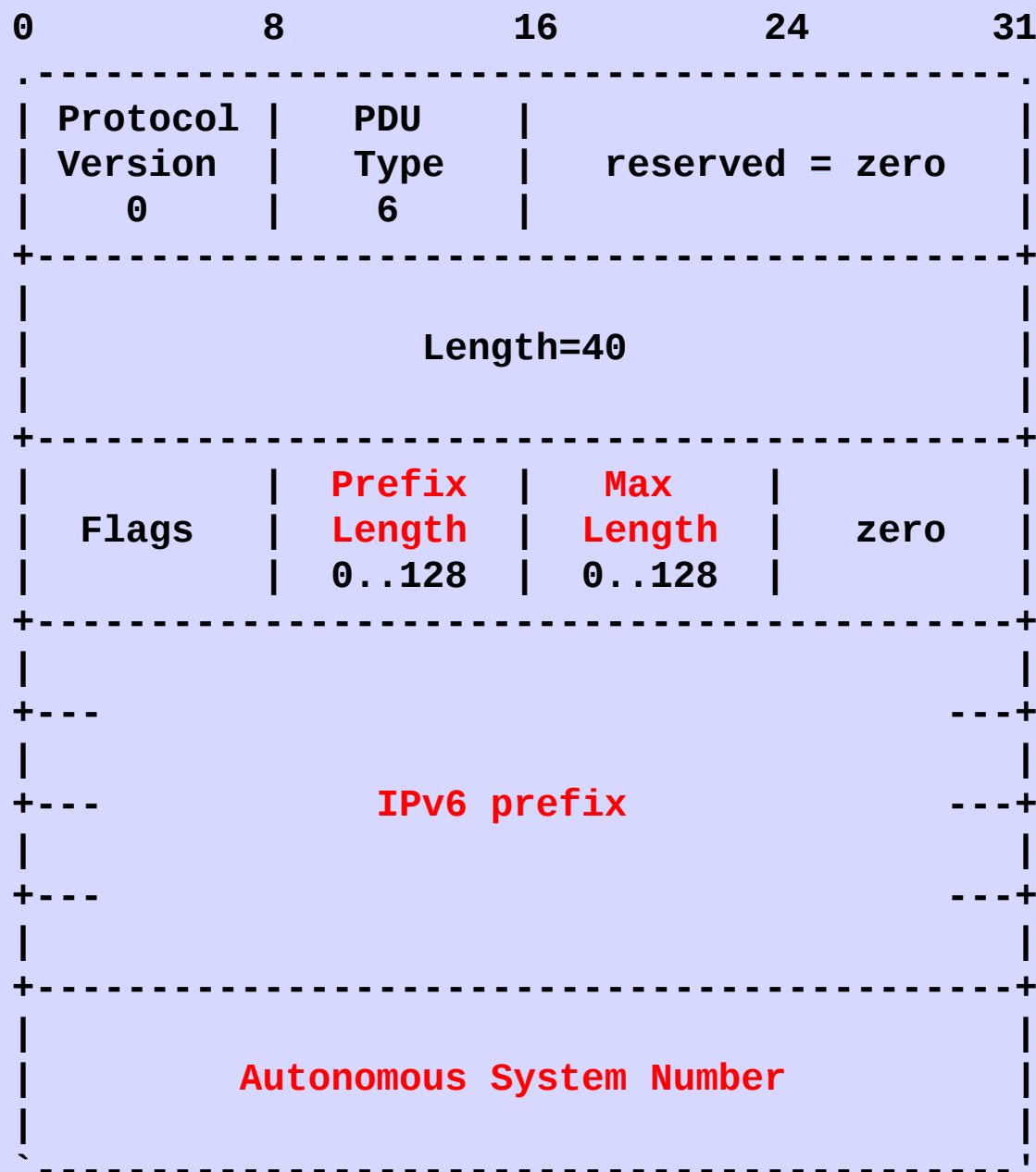
RPKI
VRPs

暗号や署名は削除して
PrefixとASの組あわせだけに
加工 : Validate ROA Payloads

IPv4 Prefix



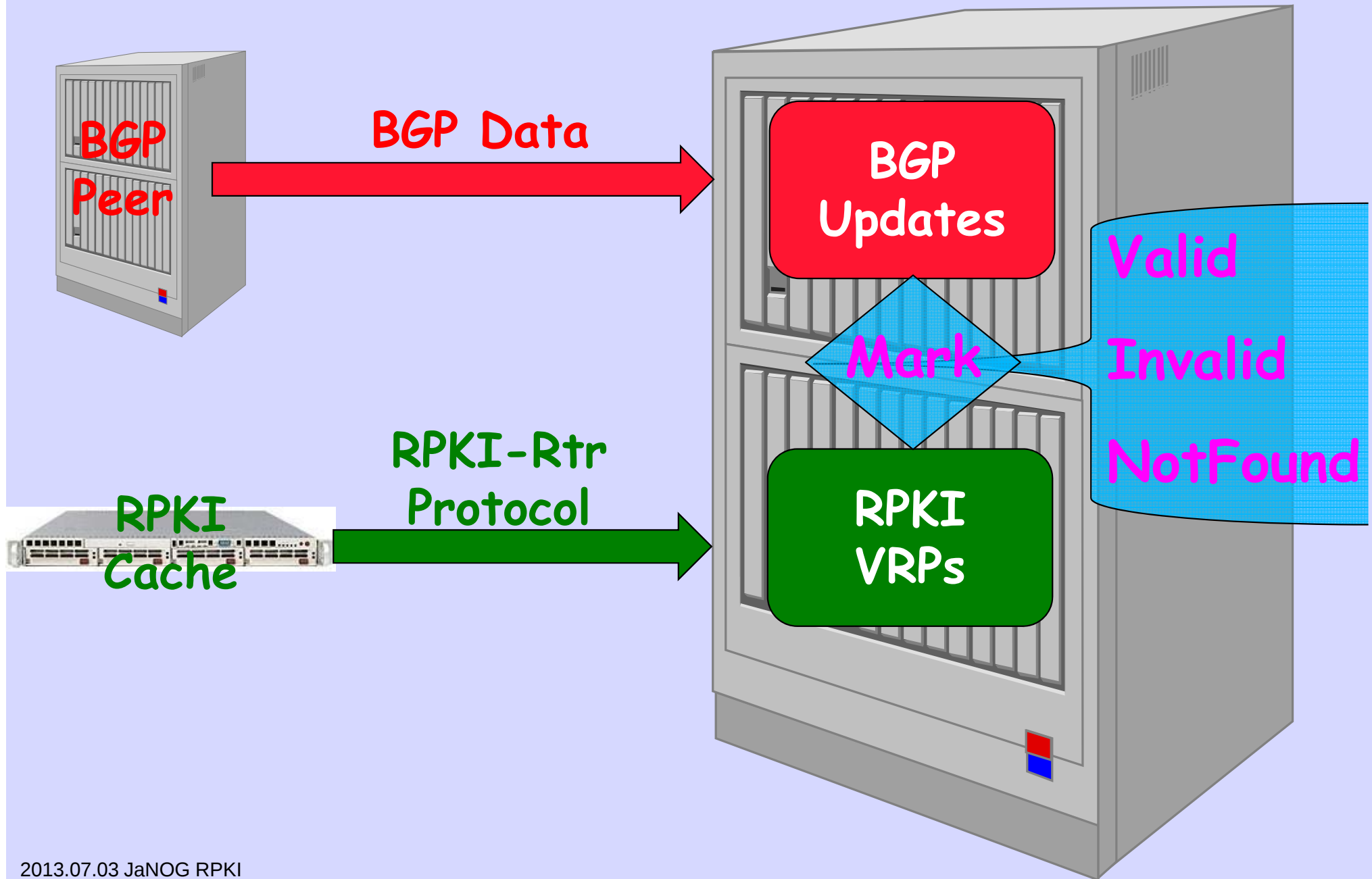
IPv6 Prefix



96 More Bits
No Magic

BGP Updateと ROAを比較する

BGP Updateのマーキング処理



ROA比較チェックの結果

- **Valid** - UPDATEに対して、AS番号が一致またはアドレス範囲に含まれるROAが存在
- **Invalid** - IPアドレス範囲は含まれるが、Updateと異なるROAしか存在しない常置亜
- **NotFound** - ROAが存在しないUpdate 現在の多数となるのはこの状態

Validの場合!

```
r0.sea#show bgp 192.158.248.0/24
```

```
BGP routing table entry for 192.158.248.0/24, version 3043542
```

```
Paths: (3 available, best #1, table default)
```

```
6939 27318
```

```
206.81.80.40 (metric 1) from 147.28.7.2 (147.28.7.2)
```

```
Origin IGP, metric 319, localpref 100, valid, internal,  
best
```

```
Community: 3130:391
```

```
path 0F6D8B74 RPKI State valid
```

```
2914 4459 27318
```

```
199.238.113.9 from 199.238.113.9 (129.250.0.19)
```

```
Origin IGP, metric 43, localpref 100, valid, external
```

```
Community: 2914:410 2914:1005 2914:3000 3130:380
```

```
path 09AF35CC RPKI State valid
```

Invalidの場合!

```
r0.sea#show bgp 198.180.150.0
```

```
BGP routing table entry for 198.180.150.0/24, version 2546236
```

```
Paths: (3 available, best #2, table default)
```

```
  Advertised to update-groups:
```

```
      2          5          6          8
```

```
Refresh Epoch 1
```

```
1239 3927
```

```
  144.232.9.61 (metric 11) from 147.28.7.2 (147.28.7.2)
```

```
    Origin IGP, metric 759, localpref 100, valid, internal
```

```
    Community: 3130:370
```

```
    path 1312CA90 RPKI State invalid
```

NotFoundの場合

```
r0.sea#show bgp 64.9.224.0
```

```
BGP routing table entry for 64.9.224.0/20, version 35201
```

```
Paths: (3 available, best #2, table default)
```

```
  Advertised to update-groups:
```

```
    2          5          6
```

```
Refresh Epoch 1
```

```
1239 3356 36492
```

```
  144.232.9.61 (metric 11) from 147.28.7.2 (147.28.7.2)
```

```
    Origin IGP, metric 4, localpref 100, valid, internal
```

```
    Community: 3130:370
```

```
    path 11861AA4 RPKI State not found
```

BGP / VRPマッチング ルールは？

Prefixが、ROAの範囲内に収まる状態のこと

(訳注) 下の例では、BGP 98.128.0.0/16に対して

98.128.0.0/12-16は98.128.0.0/16が合う

98.128.0.0/16-24も同じく/16が合う

98.128.0.0/20-24は/16よりも小さいVRPなので範囲外

BGP

98.128.0.0/16

VRP

98.128.0.0/12-16

○ BGPはこのVRPの範囲内

VRP

98.128.0.0/16-24

○ 同じく範囲内

VRP

98.128.0.0/20-24

×範囲外

Prefixが、VRPのアドレス範囲に収まり、AS番号が一致している状態

BGP

98.128.0.0/16 AS 42

VRP

98.128.0.0/12-16 AS 42

○ PrefixもASも一致

VRP

98.128.0.0/16-24 AS 666

× ASが違う

VRP

98.128.0.0/20-24 AS 42

× マスク長が範囲外

範囲の比較と正当性検証

VRP₀

98.128.0.0/16-24 AS 6

VRP₁

98.128.0.0/16-20 AS 42

BGP	98.128.0.0/12	AS 42	NotFound, shorter than VRPs
BGP	98.128.0.0/16	AS 42	Valid, Matches VRP ₁
BGP	98.128.0.0/20	AS 42	Valid, Matches VRP ₁
BGP	98.128.0.0/24	AS 42	Invalid, longer than VRP with AS 42
BGP	98.128.0.0/24	AS 6	Valid, Matches VRP ₀

経路運用者はROAと経路
を比較し、印をつけて
各組織のポリシーに則り
適用すればよい

(訳注：印をつける=BGP Communityなど)

かなり Secure

```
route-map validity-0
```

```
  match rpki valid
```

```
    set local-preference 100
```

```
route-map validity-1
```

```
  match rpki not-found
```

```
    set local-preference 50
```

```
! invalid is dropped
```

超硬派

route-map validity-0

match rpki valid

set local-preference 110

! everything else dropped

Securityマニア、、えっ？

```
route-map validity-0
```

```
match rpki invalid
```

```
set local-preference 110
```

```
! everything else dropped
```

MEDを変える (ASPATH長評価の次に)

```
route-map validity-0 match rpki  
not-found
```

```
set metric 100
```

```
route-map validity-1
```

```
match rpki invalid
```

```
set metric 150
```

```
route-map validity-2
```

```
set metric 50
```

Communityをつける

```
route-map validity-0
```

```
  match rpki valid
```

```
  set community 3130:400
```

```
route-map validity-1
```

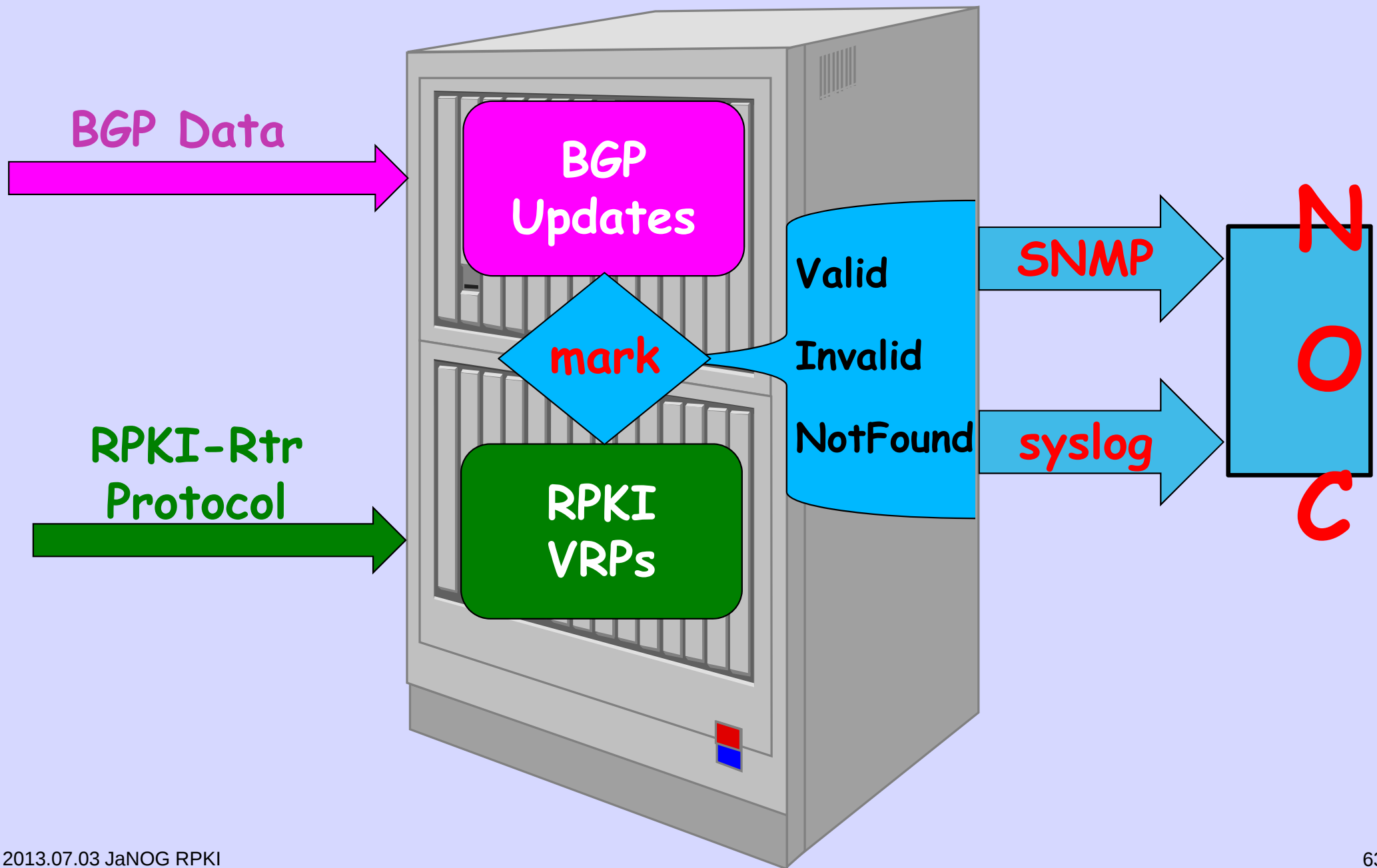
```
  match rpki invalid
```

```
  set community 3130:200
```

```
route-map validity-2
```

```
  set community 3130:300
```

それから、すべての経路を監視



最後に決めるのは、 あなたの運用・ポリシー

“Invalidな経路広報は参照すべきではないが
運用者の特別な事情によっては使ってもよい
。そのような事情でInvalidな経路を使用す
る時には、ValidやNotfoundよりも優先度を
下げるべきだ。”

-- draft-ietf-sidr-origin-ops

でもInvalidをすべて
拒否はできない・・・

レジストリとRPKI

- RIPEはかなりまじめにLIRに普及を促し、何千ものROAが作成されている
- APNICは商用サービス化して進行中
- ARINは全力で普及に対応中
- LACNIC は100組織レベルの規模で 対応LIRが増加中
- AFRINIC は25組織 ~ 同上

Origin ASValidationの対応状況

- Cisco IOS -15.2で対応確認済み (訳注 : IOX-XE)
- Cisco IOS/XR - shipped in 4.3.2
- Juniper - shipped in 12.2
- AlcaLu - in development

RPKI実装

- RIPE/NCC - CA (一部非公開) & RP (一部公開)
- APNIC - CA only - Closed Source
- RTRlib/Berlin - RP only - Open Source
- BBN - RP Only - Open Source
- RPKI.NET - CA & RP - Open Source

本日の環境 - RPKI.NET

- Open Source BSD License
- CA - Hosted and Delegated Models, GUI
- RP - RPKI-RTR, NOC Tools, IRR Gen
- FreeBSD, Ubuntu, Debian, ... Packaged (ドキュメントは改善中)



rpki.net project site

This is the Trac site for the rpki.net project. The project provides a free, BSD License, open source, complete system for the Internet Registry components which may be combined to suit your needs:

- Certification Engine
- Relying Party Cache (sometimes called a 'validator')
- rpki-rtr protocol, to feed the data to routers doing RPKI-based origin validation
- GUI for use by users of the 'hosted' model (i.e. customers who do not run their own CA)
- Web Reporting Pages so you can see what your cache has found
- Creation of pseudo-IRR data for those who wish to feed RPSL toolchains

Downloads

See [the documentation](#) for how to download and install the code.

We now have [⇒ Ubuntu packages](#) and [⇒ FreeBSD ports](#) of the code.

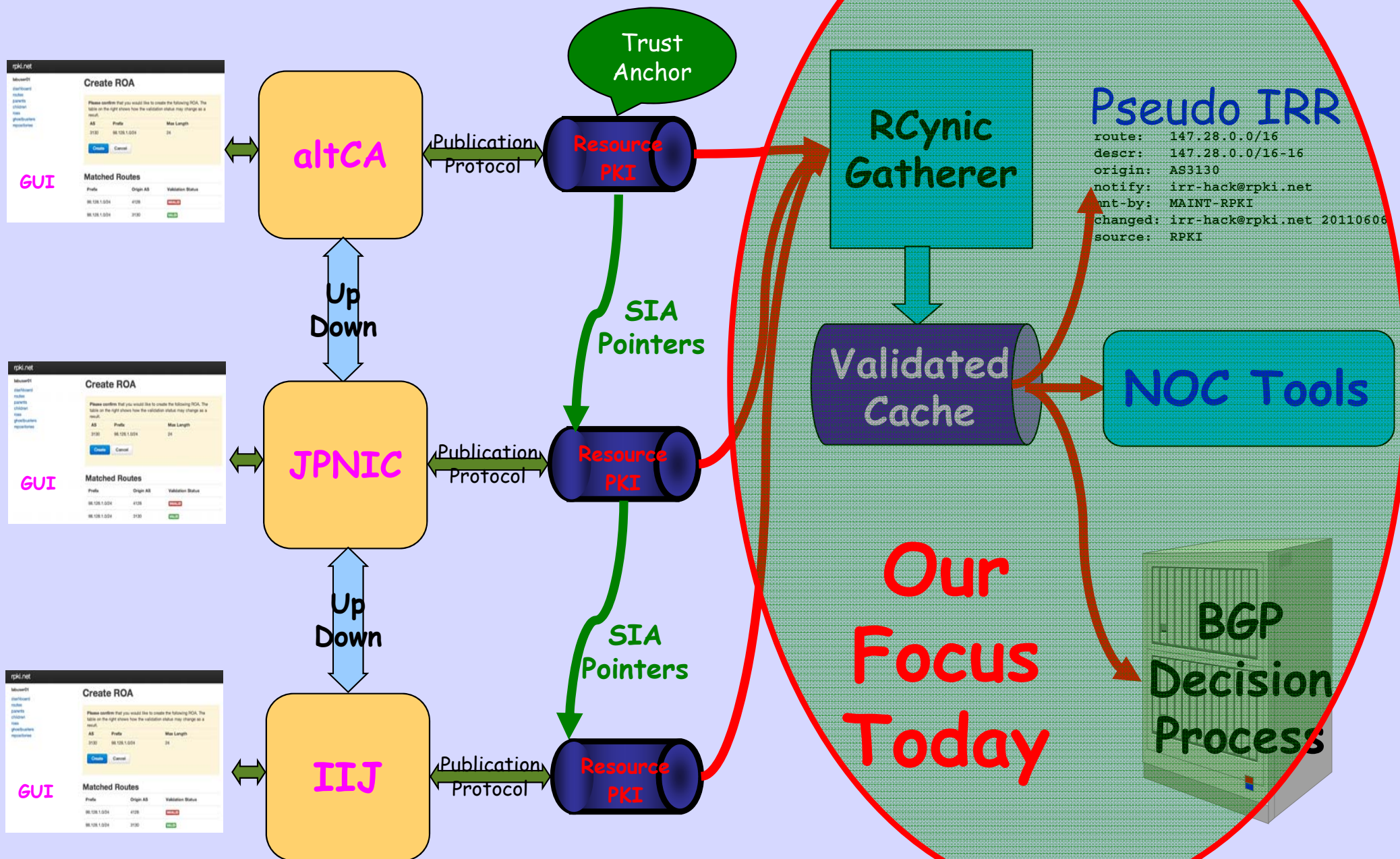
You can also [browse the source code](#).

Documentation

Primary [documentation for the code](#) is here, in the Trac wiki. PDF and flat text forms derived from are available in [the source code repository](#).

Issuing Parties

Relying Parties



今日

- 私たちが準備したPrefixをCAへ登録
- CAのWeb PortalからROAの作成
- ROAキャッシュとルータの設定
- CAから取得した情報でRP Cachesの生成

実験環境の概要

rpki.net

labuser01

- dashboard
- routes
- parents
- children
- roas
- ghostbusters
- repositories

Create ROA

Please confirm that you would like to create the following ROA. The table on the right shows how the validation status may change as a result.

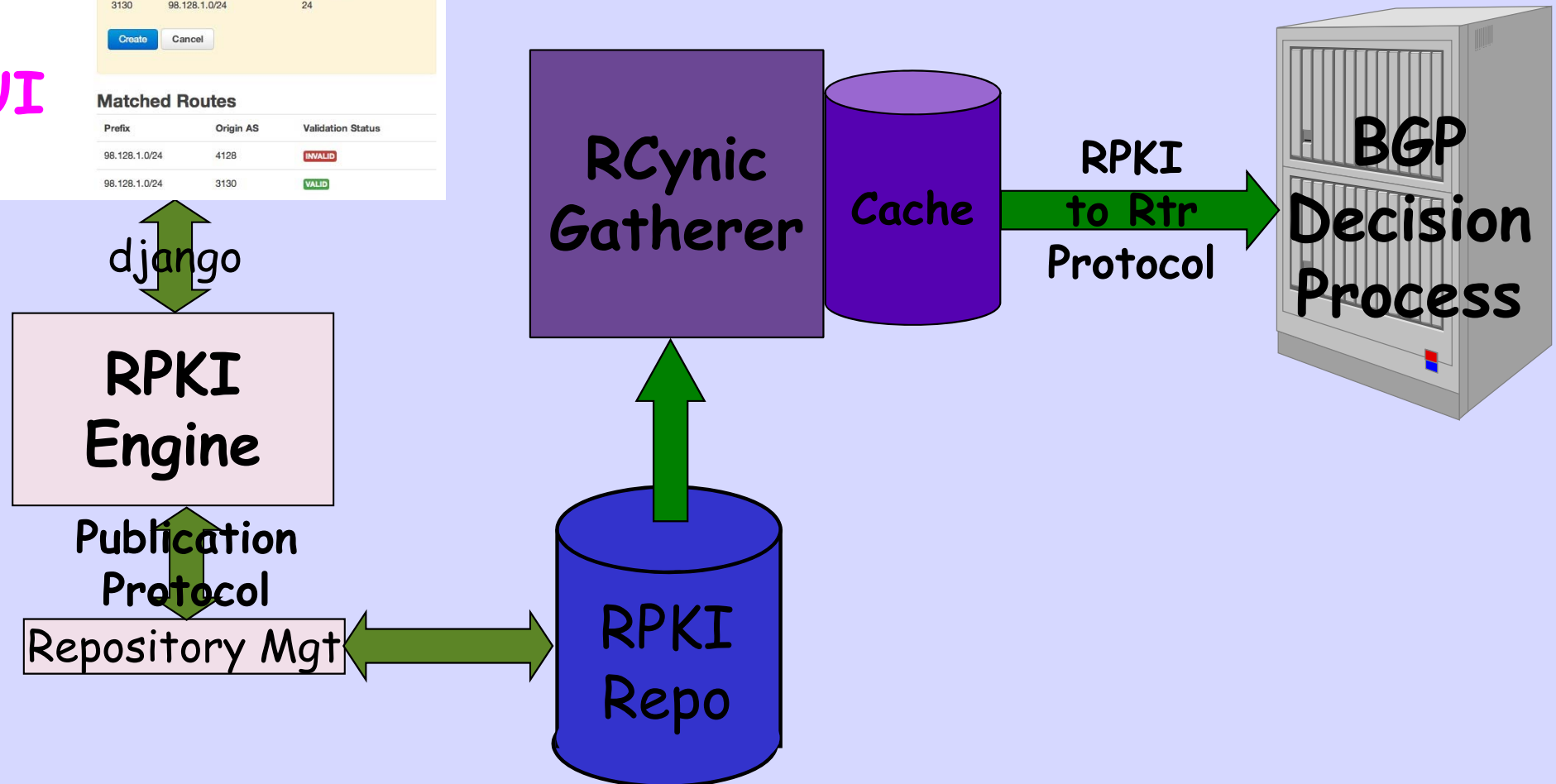
AS	Prefix	Max Length
3130	98.128.1.0/24	24

Create Cancel

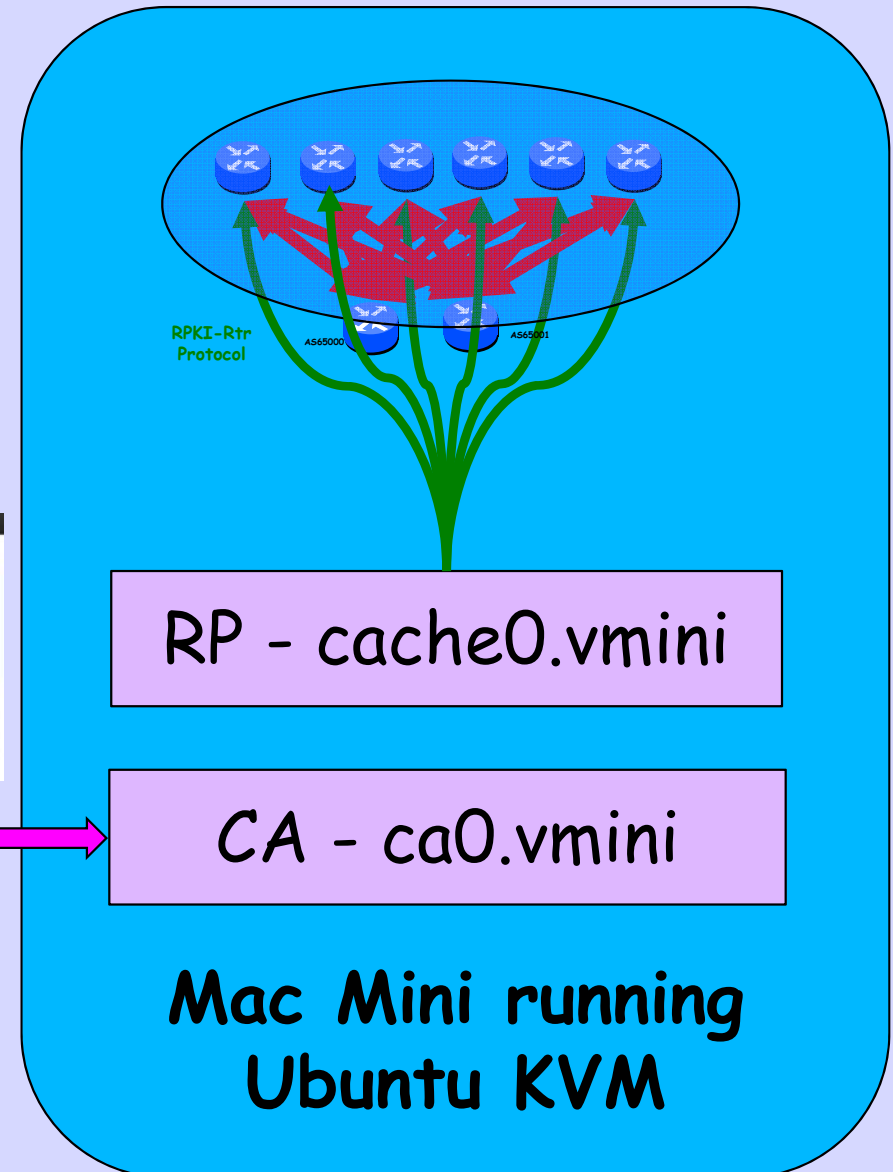
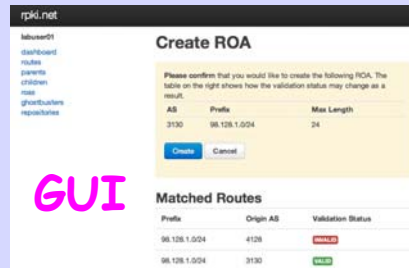
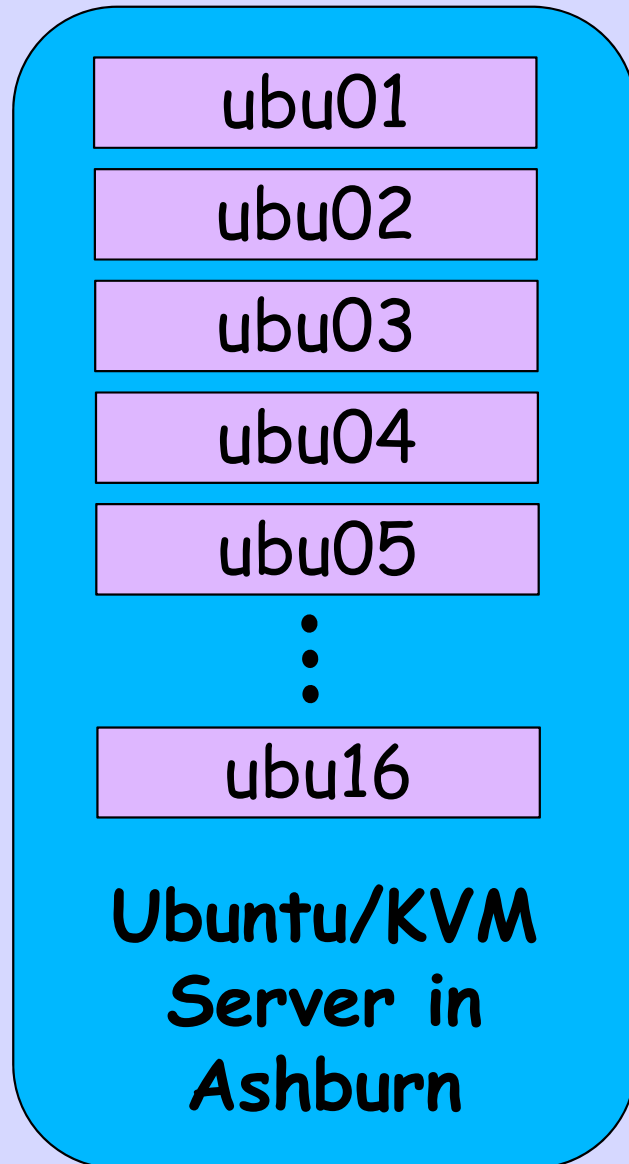
Matched Routes

Prefix	Origin AS	Validation Status
98.128.1.0/24	4128	INVALID
98.128.1.0/24	3130	VALID

GUI



実験環境



DynaMIPS(C7200VXR)エミュレータ) on MacMini

10.0.0.0/8

RPKI-Rtr
Protocol

AS65000

AS65001

202.214.86.148
Global
Internet

RPKI
Cache

98.128.0.0/16
98.128.0.0/24
98.128.1.0/24
...
98.128.31.0/24

AS3130

Seattle

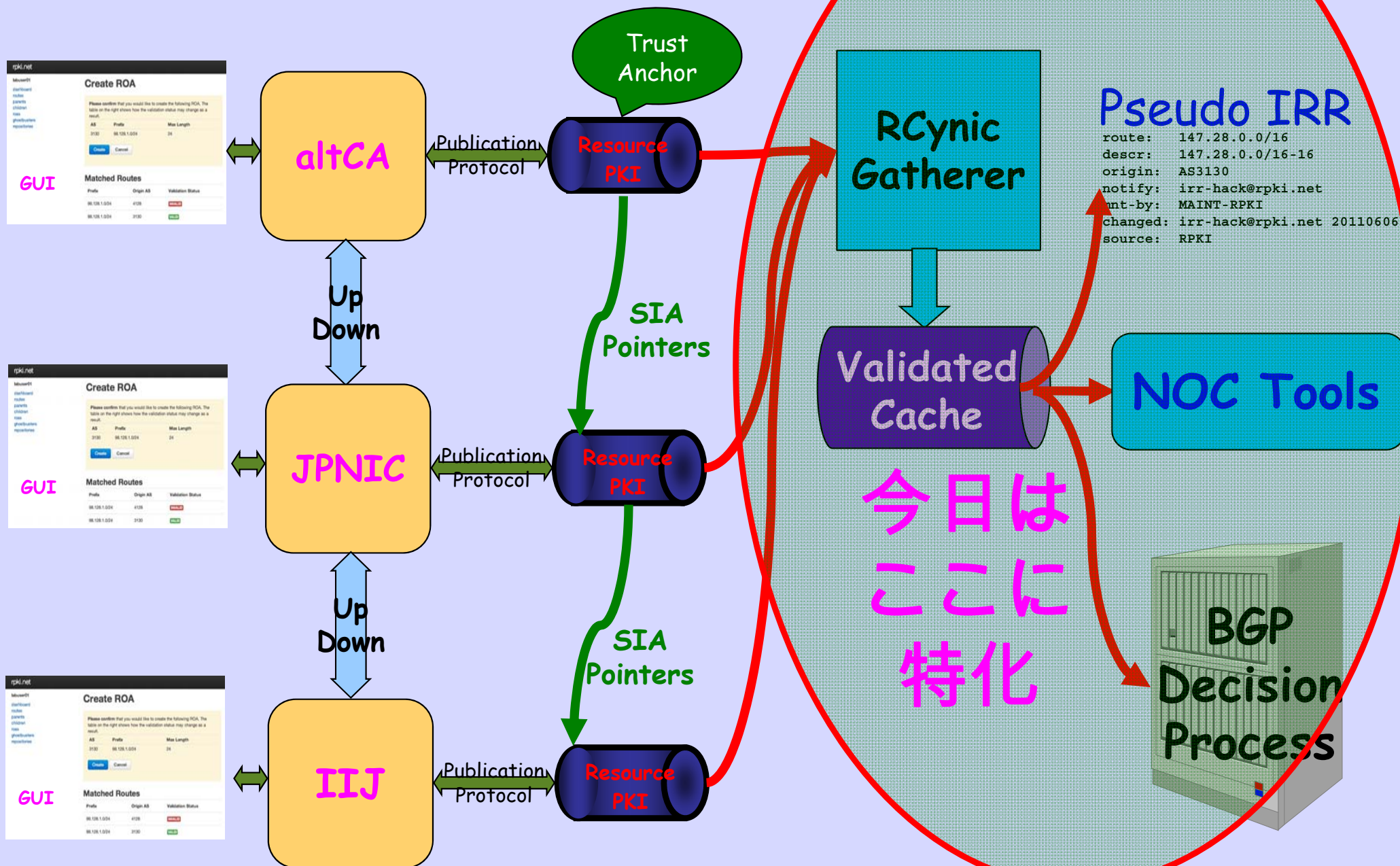
98.128.0.0/16
98.128.0.0/24
98.128.1.0/24
...
98.128.31.0/24

AS4128

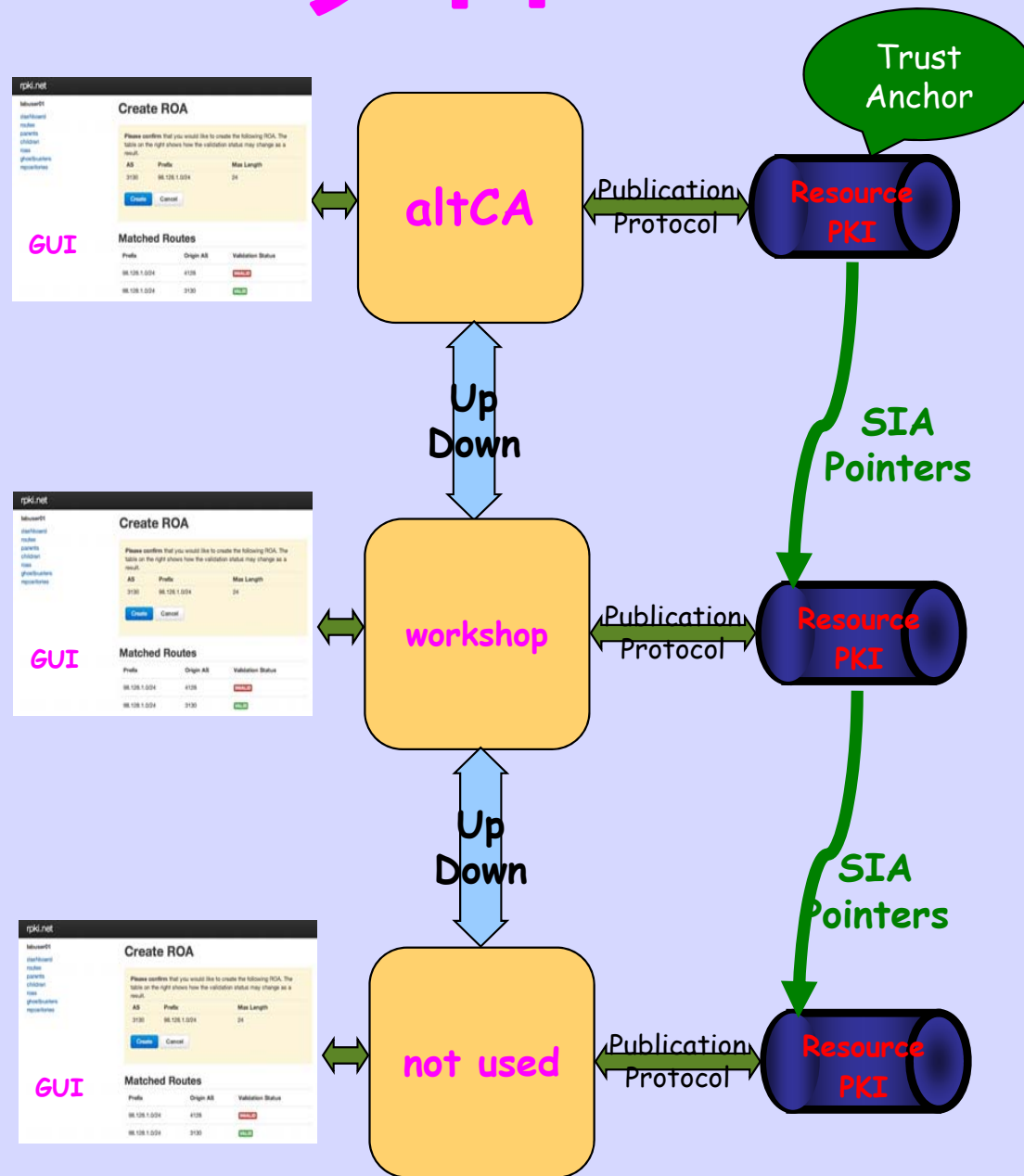
Dallas

Issuing Parties

Relying Parties



今日



IP Address 割り振り

98.128.0.0/16 ARIN Experimental Allocation

98.128.0.0/24 Instructors Play

98.128.1.0/24 labuser01 (参加者 1)

98.128.2.0/24 labuser02 (参加者 2)

...

98.128.32.0/24 labuser32 (参加者 3 2)

GUI Accounts

<https://ca0.vmini.rpki.net/>

UserID

Password

labuser01

fnord

labuser02

fnord

labuser03

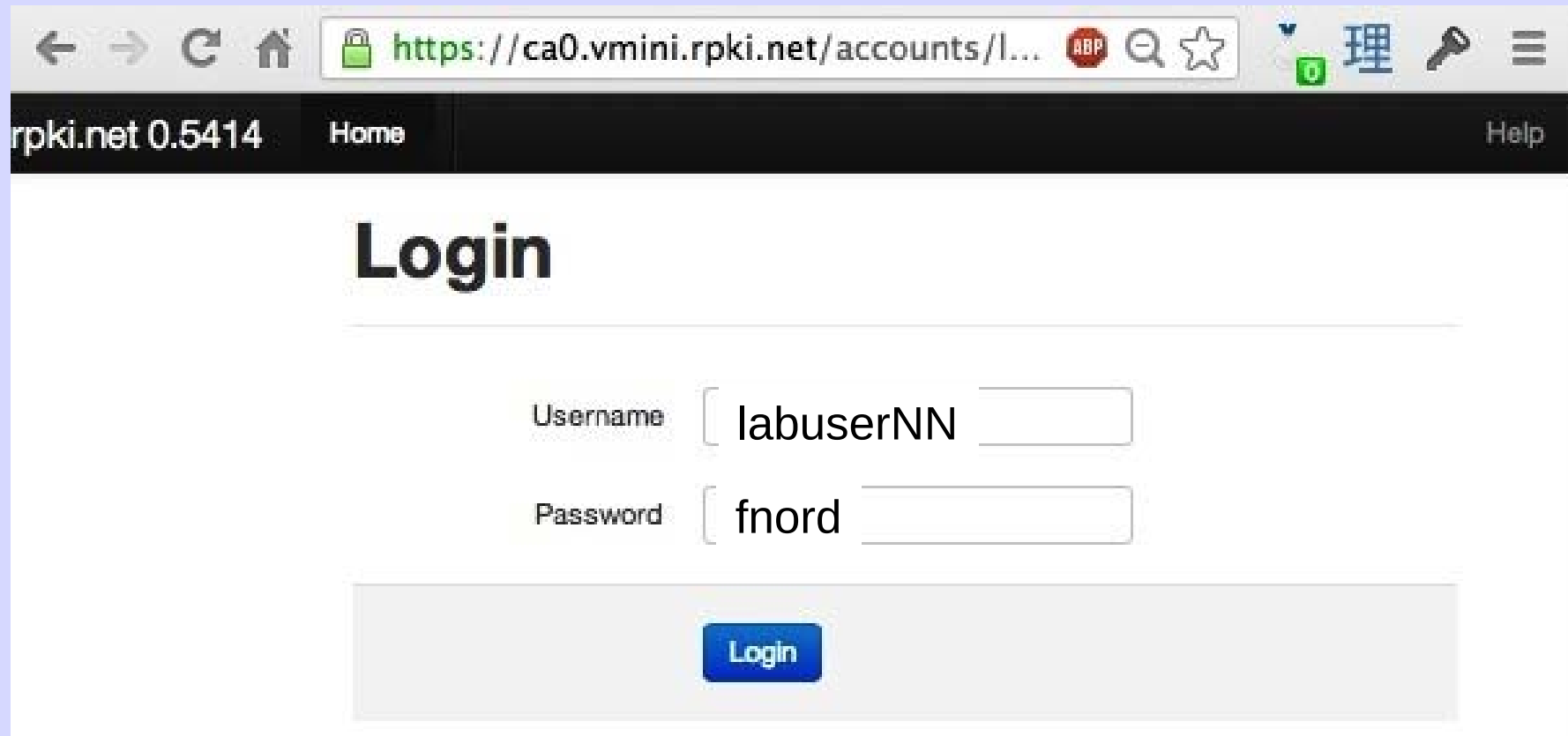
fnord

...

labuser16

fnord (えふのるど)

https://ca0.vmini.rpki.net/



The screenshot shows a web browser window with the address bar displaying `https://ca0.vmini.rpki.net/accounts/l...`. The page has a dark header bar with the text "rpki.net 0.5414" on the left, "Home" in the center, and "Help" on the right. Below the header, the main content area is white and features a large "Login" heading. Underneath the heading, there are two input fields: "Username" with the value "labuserNN" and "Password" with the value "fnord". A blue "Login" button is positioned below these fields.

rpki.net 0.5414 Home Help

Login

Username

Password

Login

The Dashboard

rpki.net 0.5414 Home Logged in as labuser01 Log Out

labuser01

[dashboard](#)

[routes](#)

[alerts](#) 9

[select identity](#)

[export identity](#)

Resources

Resource	Valid Until	Parent
98.128.1.0/24	June 21, 2014, 1:38 p.m.	workshop

[refresh](#)

ROAs

Prefix	Max Length	AS
Create Import Export		

Children

Handle
Child ASNs Prefixes
ASNs Prefixes

Repositories

Handle
workshop Import

Unallocated Resources

The following resources have not been allocated to a child, nor appear in a ROA.

IPv4

Prefix	Action
98.128.1.0/24	ROA

Ghostbusters

Full Name	Organization	Email	Telephone
Create			

Parents

Handle
workshop Import



ROAの生成

rpki.net 0.5414 Home Logged in as labuser01 Log Out

labuser01 Create ROAs

dashboard
routes
alerts 0
select identity

98.128.1.0/24 Max len 4128 Delete

Preview Cancel



なにが起きる？

rpki.net 0.5414 Home Logged in as labuser01 Log Out Help

labuser01

[dashboard](#)

[routes](#)

[alerts](#) 0

[select identity](#)

Confirm ROA Requests

Please confirm that you would like to create the following ROA(s). The accompanying table indicates how the validation status may change as a result.

Prefix	Max Length	AS
98.128.1.0/24	24	4128

Create

Cancel



Matched Routes

Prefix	Origin AS	Validation Status
98.128.1.0/24	4128	valid
98.128.1.0/24	3130	invalid

Routers

- Use Your Own! (in production images from C&J)
- 16 DynaMIPS 7200s in Lab
- 7200s in Live Internet

ご注意!

- いくつかの公開キャッシュには大量のROAがあります。
- RIPEからROAキャッシュをとると大量なのでDynamips環境には適用しないで
- Dynamipsを壊したければ、198.180.152.11にはフル経路のROAがあるよ、、、

7200sの実環境

```
$ ssh demo@r0.sea.rg.net
```

```
Password: demo
```

or

```
$ ssh demo@r1.iad.rg.net
```

```
Password: demo
```

Sorry, enableは無しで



実験環境のRouter

Accounts

```
% telnet vmini.rpki.net 20NN
```

```
user: isplab
```

```
password: lab-PW
```

```
enable: lab-PW
```

RouterのNN番号は後で割り当てます

Ciscoを覗こう

r0.sea#show ip bgp rpki ?

servers Display RPKI cache server information

table Display RPKI table entries

RPKIキャッシュの状態

r0.sea#**show ip bgp rpki servers**

BGP SOVC neighbor is 192.168.179.3/43779 connected to port 43779

Flags 0, Refresh time is 600, Serial number is 1304239609

InQ has 0 messages, OutQ has 0 messages, formatted msg 345

Session IO flags 3, Session flags 4008

Neighbor Statistics:

Nets Processed 624

Connection state is ESTAB, I/O status: 1, unread input bytes: 0

Connection is ECN Disabled

Mininum incoming TTL 0, Outgoing TTL 255

Local host: 199.238.113.10, Local port: 57932

Foreign host: 192.168.179.3, Foreign port: 43779

Connection tableid (VRF): 0

Look at Table

router1#show ip bgp rpki table

76 BGP sovc network entries using 6688 bytes of memory

78 BGP sovc record entries using 1560 bytes of memory

Network	Maxlen	Origin-AS	Source	Neighbor
98.128.0.0/24	24	3130	0	192.168.179.3/43779
98.128.0.0/16	16	3130	0	192.168.179.3/43779
98.128.6.0/24	24	4128	0	192.168.179.3/43779
98.128.9.0/24	24	3130	0	192.168.179.3/43779
98.128.30.0/24	24	1234	0	192.168.179.3/43779
128.224.1.0/24	24	3130	0	192.168.179.3/43779
129.6.0.0/17	17	49	0	192.168.179.3/43779
129.6.112.0/24	24	10866	0	192.168.179.3/43779
129.6.128.0/17	17	49	0	192.168.179.3/43779
147.28.0.0/16	16	3130	0	192.168.179.3/43779

Look at BGP Table

```
r0.sea#sh ip bgp
```

	Network	Next Hop	Metric	LocPrf	Weight	Path
* i	I 198.180.150.0	144.232.9.61	100	0	1239	3927 i
*>	I	199.238.113.9	0	2914	3927	i
*	I	129.250.11.41	0	2914	3927	i
*>	V 198.180.152.0	199.238.113.9	0	2914	4128	i
*	V	129.250.11.41	0	2914	4128	i
*>	N 198.180.155.0	199.238.113.9	0	2914	22773	i
*	N	129.250.11.41	0	2914	22773	i
*>	N 198.180.160.0	199.238.113.9	0	2914	23308 13408	5752 i
*	N	129.250.11.41	0	2914	23308 13408	5752 i

Mis-Originationの検出

R3#**sh ip bgp 98.128.0.0/24**

BGP routing table entry for 98.128.0.0/24, version 94

Paths: (2 available, best #2, table default)

Advertised to update-groups:

1

Refresh Epoch 1

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**

Refresh Epoch 1

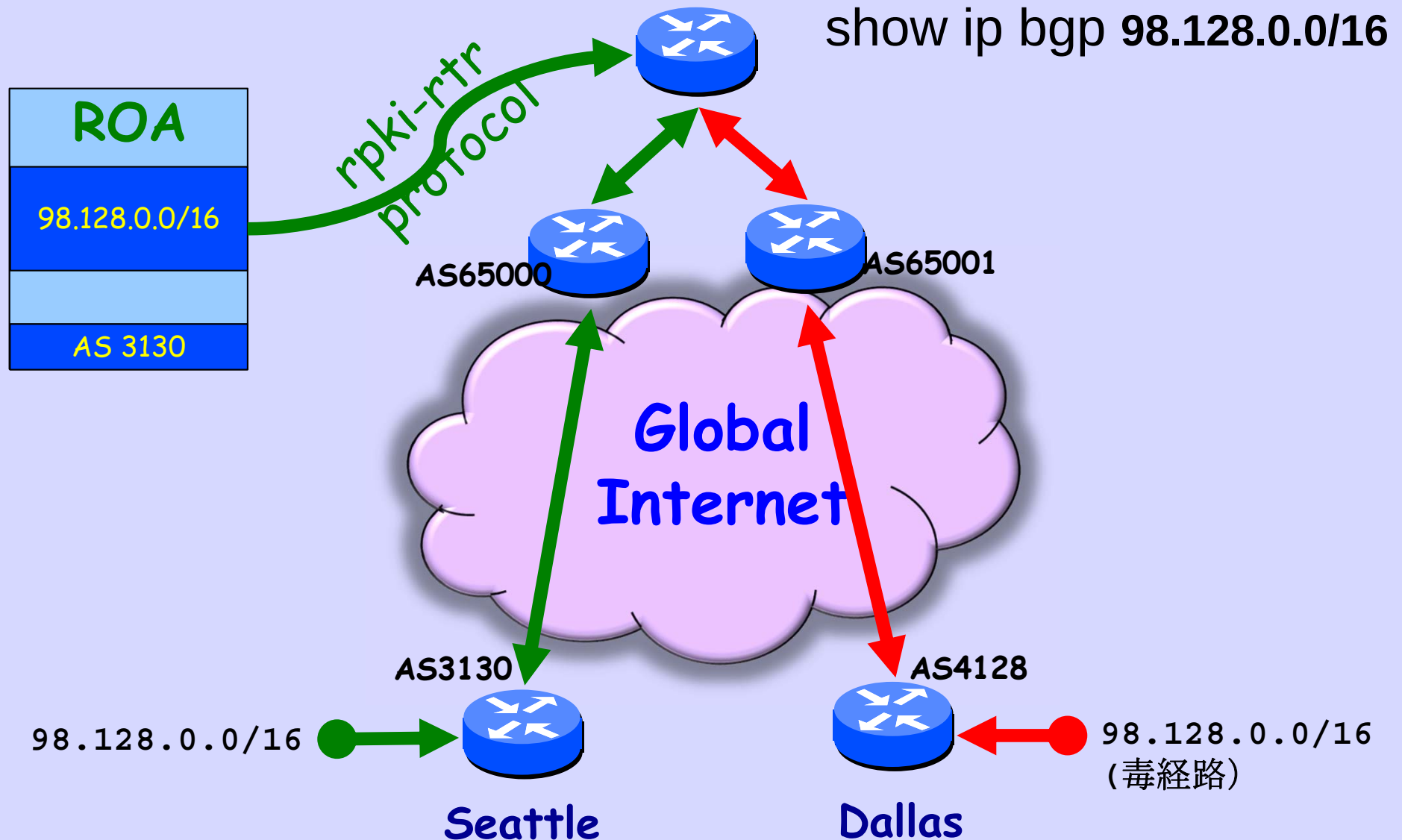
65001 4128

10.0.1.1 from 10.0.1.1 (65.38.193.13)

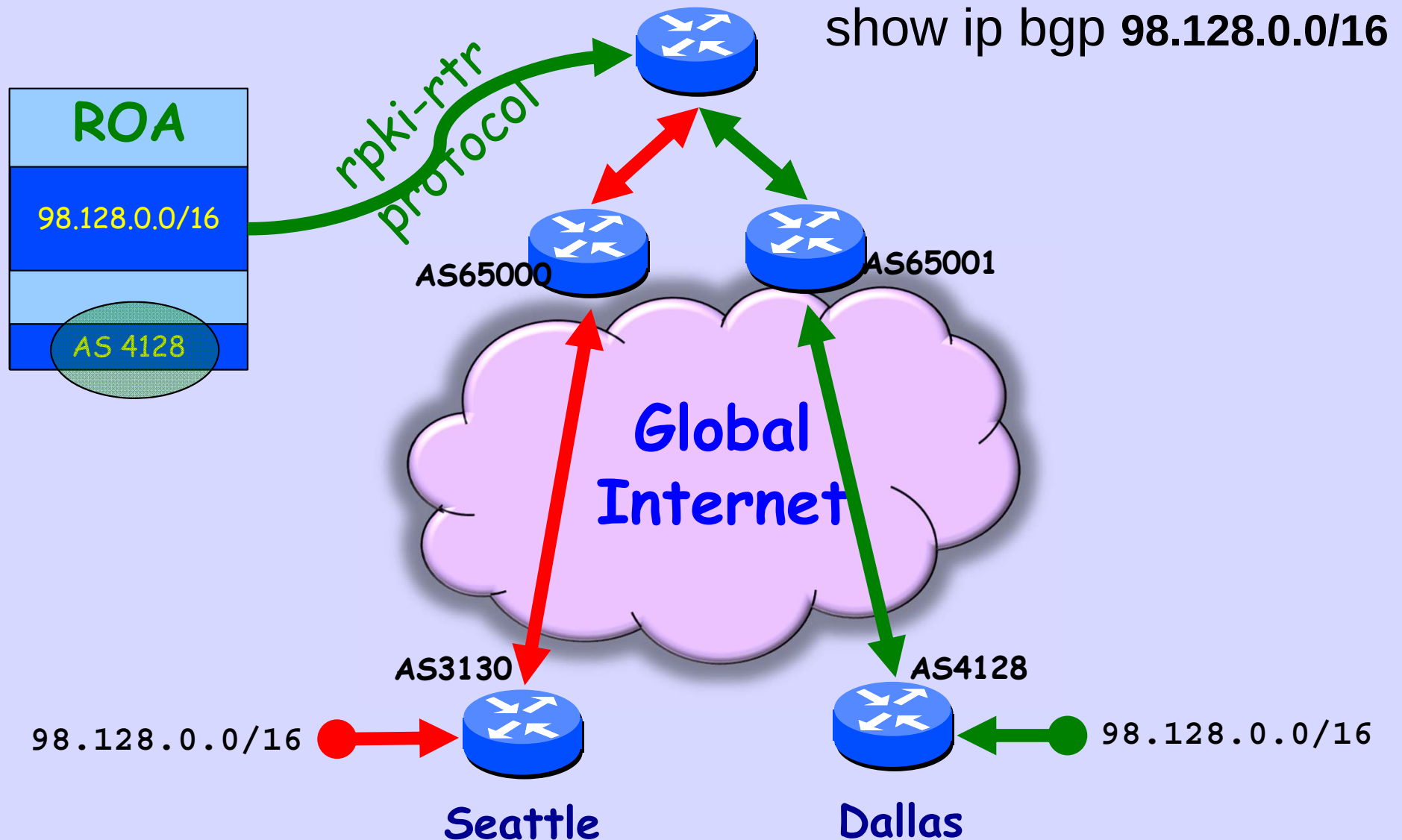
Origin IGP, localpref 100, valid, external, best

path 6802D7C8 **RPKI State valid**

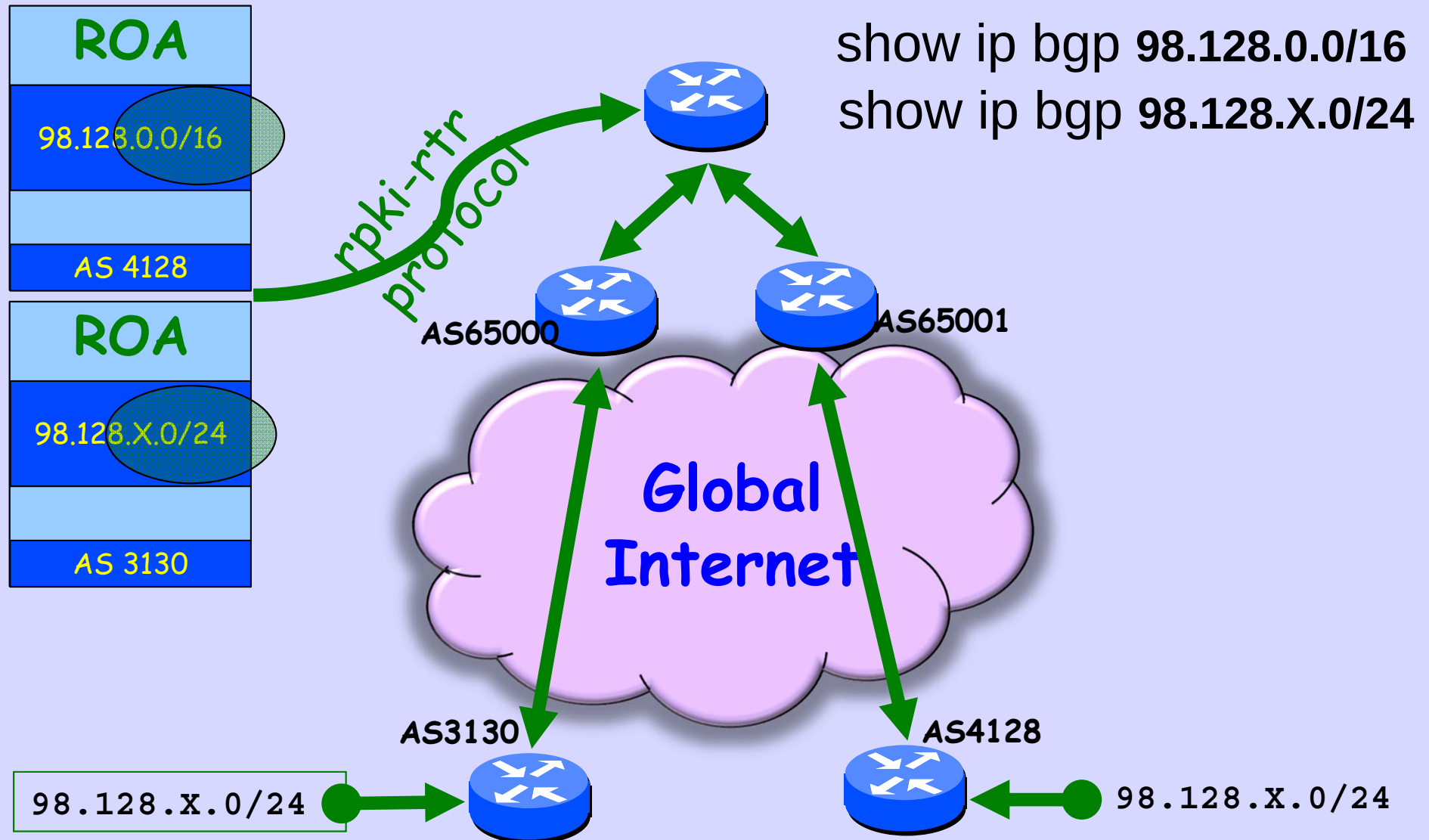
タイプミスの検知



ROAは正当性を担保



/24で試してみて



Install RP Cache SW

On Your Laptop

(FreeBSD, Ubuntu, ...)

or

Remote (Virtual) Ubuntu Server

VMの貸与

- Servers in Ashburn, Virginia US
- Ubuntu 12.04.2 LTS Server
- ssh labuserNN@ubuNN.rpki.net
- Password is Vattood1
- You are in sudoers
- Do not worry, machines are snapshotted

Installing RP Package

Debian/Ubuntu

Copy and Paste from

<https://trac.rpki.net/wiki/doc/RPKI/Installation/UbuntuPackages>

```
$ wget -q -O - http://download.rpki.net/APT/apt-gpg-key.asc | sudo apt-key add -
```

```
$ sudo wget -q -O /etc/apt/sources.list.d/rpki.list  
http://download.rpki.net/APT/rpki.ubuntu.list
```

```
$ sudo apt-get update
```

```
$ sudo apt-get install rpki-rp
```

Upgrading RP Package

```
$ sudo apt-get update
```

```
$ sudo apt-get install rpki-rp
```

トラストアンカーを指定

- 今日はDynaMIPS上のエミュレートされたルータを使う。そのためメモリが限られる
- なので、インターネット全体のROAをルータへ投入することはできません
- こう書いてください
 - Edit /etc/rcynic.conf

trust-anchor-directory = ¥

/etc/rpki/trust-anchor/**altca.tal**

急ぐために

- ROAの伝播をまっていられない
- ROA収集コマンドのrcynicを短期間で動かしましょう
- **\$ sudo crontab -e -u rcynic**

0/2 * * * * * exec /usr/bin/rcynic-cron

RPKI-Rtr(キャッシュデーモン) の動作確認?

\$ rtr-origin --client tcp localhost 43779

2013-03-09 23:10:19 rtr-origin/client[17089]: [Startup]

**2013-03-09 23:10:19 rtr-origin/client[17089]: [Starting raw TCP
connection to localhost:43779]**

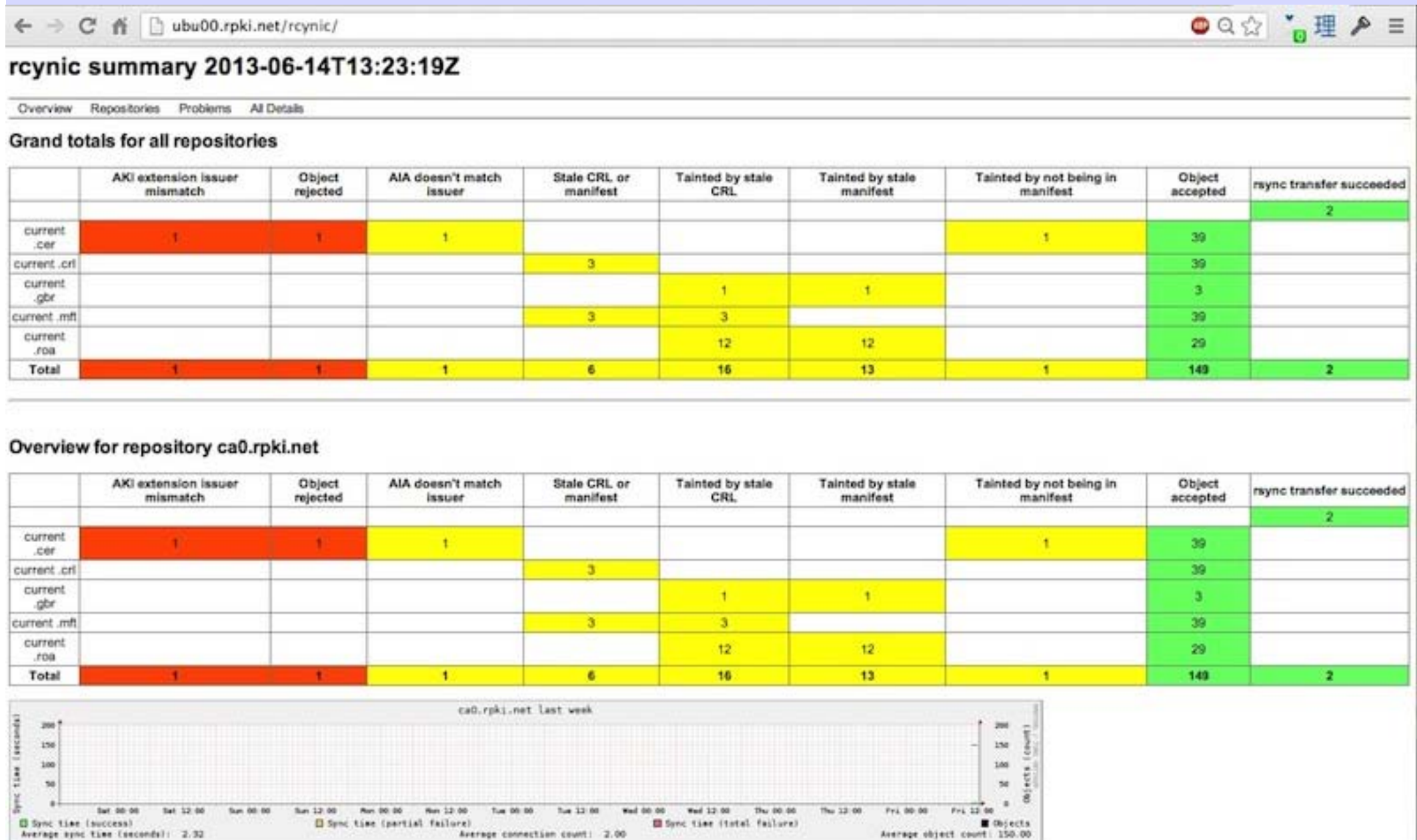
2013-03-09 23:10:19 rtr-origin/client[17089]: [reset_query]

**2013-03-09 23:10:19 rtr-origin/client[17089]: [cache_response,
nonce 37394]**

**2013-03-09 23:10:19 rtr-origin/client[17089]: + 12322
78.192.0.0/10-10
00:04:00:00:00:00:00:14:01:0A:0A:00:4E:C0:00:00:00:00:30:22**

**2013-03-09 23:10:19 rtr-origin/client[17089]: + 3320
79.192.0.0/10-10
00:04:00:00:00:00:00:14:01:0A:0A:00:4F:C0:00:00:00:00:0C:F8**

CacheはWeb機能もあり



Check Server

r0.sea#show ip bgp rpki servers

BGP SOVC neighbor is 192.168.179.3/43779 connected to port 43779

Flags 0, Refresh time is 600, Serial number is 1304239609

InQ has 0 messages, OutQ has 0 messages, formatted msg 345

Session IO flags 3, Session flags 4008

Neighbor Statistics:

Nets Processed 624

Connection state is ESTAB, I/O status: 1, unread input bytes: 0

Connection is ECN Disabled

Mininum incoming TTL 0, Outgoing TTL 255

Local host: 199.238.113.10, Local port: 57932

Foreign host: 192.168.179.3, Foreign port: 43779

Connection tableid (VRF): 0

Look at ROA/VRF Table

router1#**show ip bgp rpki table**

76 BGP sovc network entries using 6688 bytes of memory

78 BGP sovc record entries using 1560 bytes of memory

Network	Maxlen	Origin-AS	Neighbor
98.128.0.0/24	24	3130	192.168.179.3/43779
98.128.0.0/16	16	3130	192.168.179.3/43779
98.128.6.0/24	24	4128	192.168.179.3/43779
98.128.9.0/24	24	3130	192.168.179.3/43779
98.128.30.0/24	24	1234	192.168.179.3/43779
128.224.1.0/24	24	3130	192.168.179.3/43779
129.6.0.0/17	17	49	192.168.179.3/43779
129.6.112.0/24	24	10866	192.168.179.3/43779
129.6.128.0/17	17	49	192.168.179.3/43779
147.28.0.0/16	16	3130	192.168.179.3/43779

Look at BGP Table

r0.sea#sh ip bgp

	Network	Next Hop	Metric	LocPrf	Weight	Path
* i	I198.180.150.0	144.232.9.61	100	0	1239	3927 i
*>	I	199.238.113.9	0	2914	3927	i
*	I	129.250.11.41	0	2914	3927	i
*>	V198.180.152.0	199.238.113.9	0	2914	4128	i
*	V	129.250.11.41	0	2914	4128	i
*>	N198.180.155.0	199.238.113.9	0	2914	22773	i
*	N	129.250.11.41	0	2914	22773	i
*>	N198.180.160.0	199.238.113.9	0	2914	23308 13408	5752 i
*	N	129.250.11.41	0	2914	23308 13408	5752 i

Look at a Prefix

R3#show ip bgp 98.128.0.0/24

BGP routing table entry for 98.128.0.0/24, version 360

Paths: (2 available, best #1, table default)

65000 3130

10.0.0.1 from 10.0.0.1 (193.0.24.64)

**Origin IGP, localpref 100, valid, external, best
path 680D859C RPKI State valid**

65001 4128

10.0.1.1 from 10.0.1.1 (193.0.24.65)

**Origin IGP, localpref 100, valid, external
path 680D914C RPKI State invalid**

試してほしいこと

- Look at your neighbors' prefixes
- Use the GUI to change the ROA for your prefix, and wait for it to propagate
- Attack your neighbor's prefix by configuring your bgp to announce it
router bgp 651nn
network 98.128.<neighbor>.0 255 255 255.0

注意：そのままでは、、、

```
router bgp 651nn
```

```
network 98.128.<neighbor>.0 255 255 255.0
```

```
show ip bgp 98.128.<neighbor>.0
```

- 上記はあなたのルータであなたが作った実験用の悪い経路にInvalidをつけます。そのため、悪いPrefixを外にアナウンスできません。そこで、おまじないを、、
- router bgp 651nn
no bgp bestpath prefix-validate local
- これで、外に悪い経路を広報し、観察してもらうことができます。

あなたはすでに、Youtube
事件の対処法を知っている

家に帰っても
試してみてね