APNIC 35 CONFERENCE

SINGAPORE
25 February - 1 March 2013

APNIC RPKI Report

George Michaelson

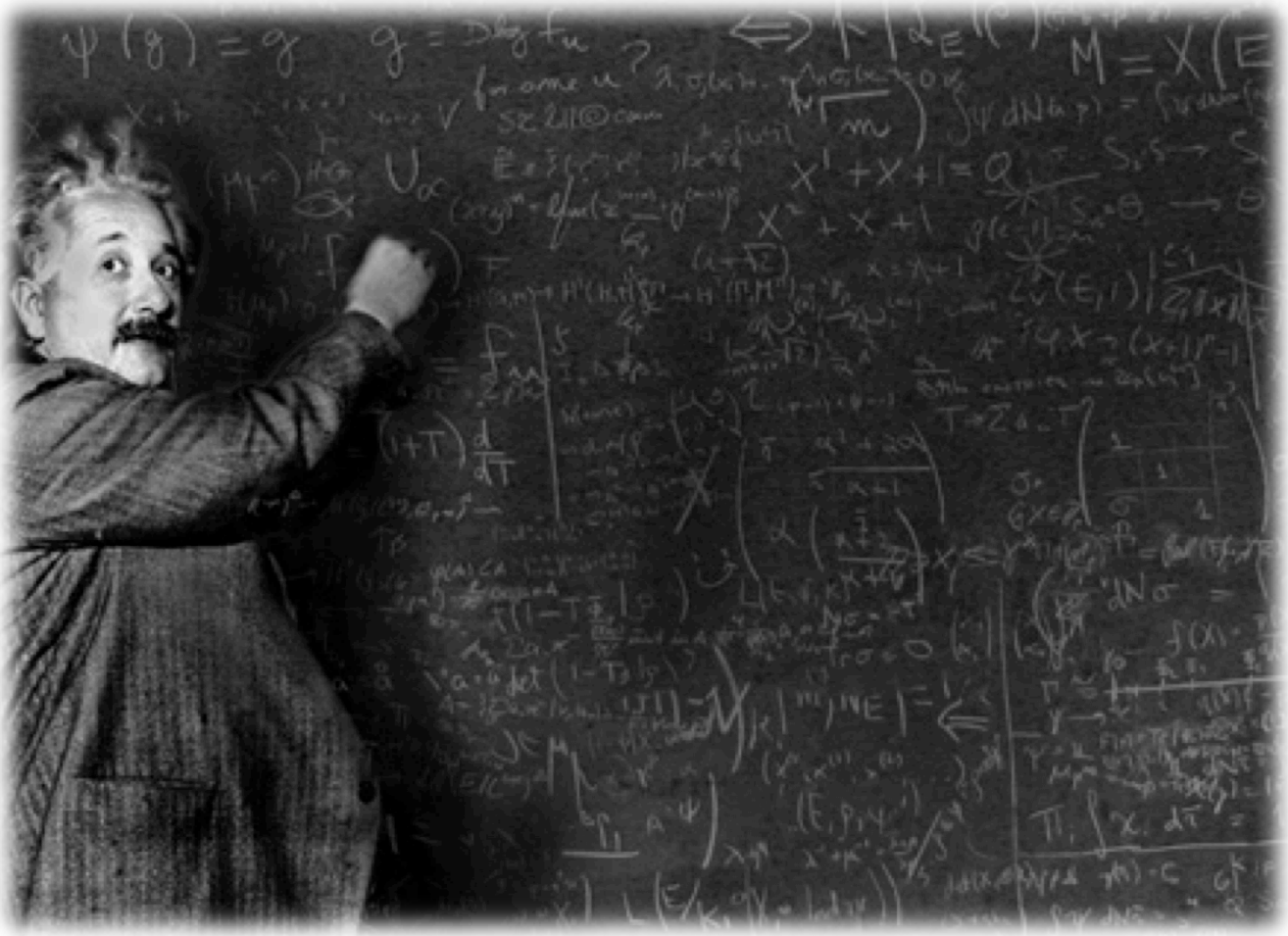
APNIC RPKI – Current Activities

- Splitting the TAL
- Standards Compliance
- Provisioning Protocol Services
- RPKI UI in MyAPNIC re-design
- General sign

Splitting the TAL

- A Quick Primer on Certificates and Validation
- The RPKI TA Framework
- APNIC's TA Changes

A Quick Primer on Certificates and Validation



A Quick Primer on Certificates and Validation

- Public/private key cryptography relies on public algorithms, public data (public key value), and a carefully guarded secret (private key value)
  - Encrypt using the private key
  - Decrypt using the public key

- But which public key should be used?
  - X.509 public key certificates bind an entity's identity to a given public key value
  - If you trust the identity checks performed by the X.509 certificate issuer then you can trust the association of identity with public key value

A Quick Primer on Certificates and Validation

- “Resource Certificates” are subtly different:
  - They bind a set of IP addresses with a given public key
  - The certificate issuer is certifying that the addresses listed in the certificate are currently held by the entity who has the key pair where the public key part is also listed in the certificate
  - The grounds for issuing the certificate is that the certificate’s issuer also was the entity who allocated or assigned the addresses to the current address holder
- The collection of resource certificates mirror the address allocation hierarchy
- Digitally signed attestations about addresses can be made by an address holder, signing with their private key
- These attestations can be validated by testing the integrity of the digital signature (good signature) and that integrity of the address block (good addresses)

A Quick Primer on Certificates and Validation

- RPKI is a framework that has been defined to use this method to specify PKI outcomes relating to IP addresses.
  - Combines the IP address registration hierarchy with a Certification hierarchy,

- RPKI provides a strong, testable basis for supporting digital signatures in statements made about IP addresses.
  - A secure basis for attestations about IP addresses
  - anyone can validate and verify for themselves.

A Quick Primer on Certificates and Validation

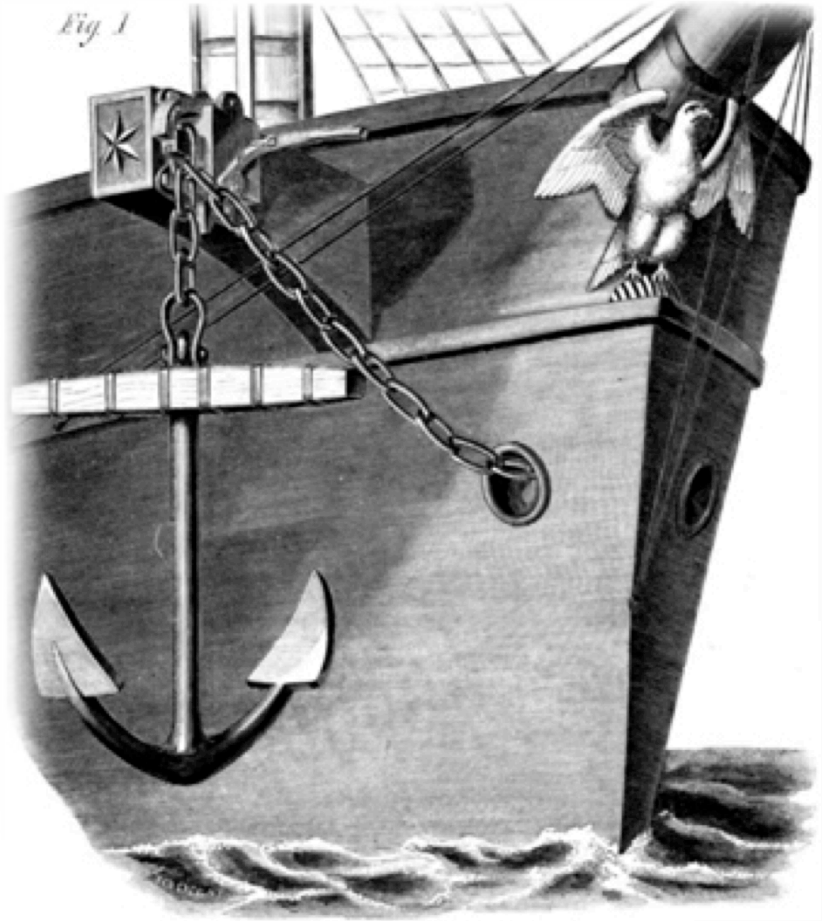
- Certificate based Public Key Cryptography (PKI) uses the concept of a "**trust anchor**" or **TA**
  - the cryptographic public key that a relying party (the ones who perform validation) is prepared to trust **innately**.

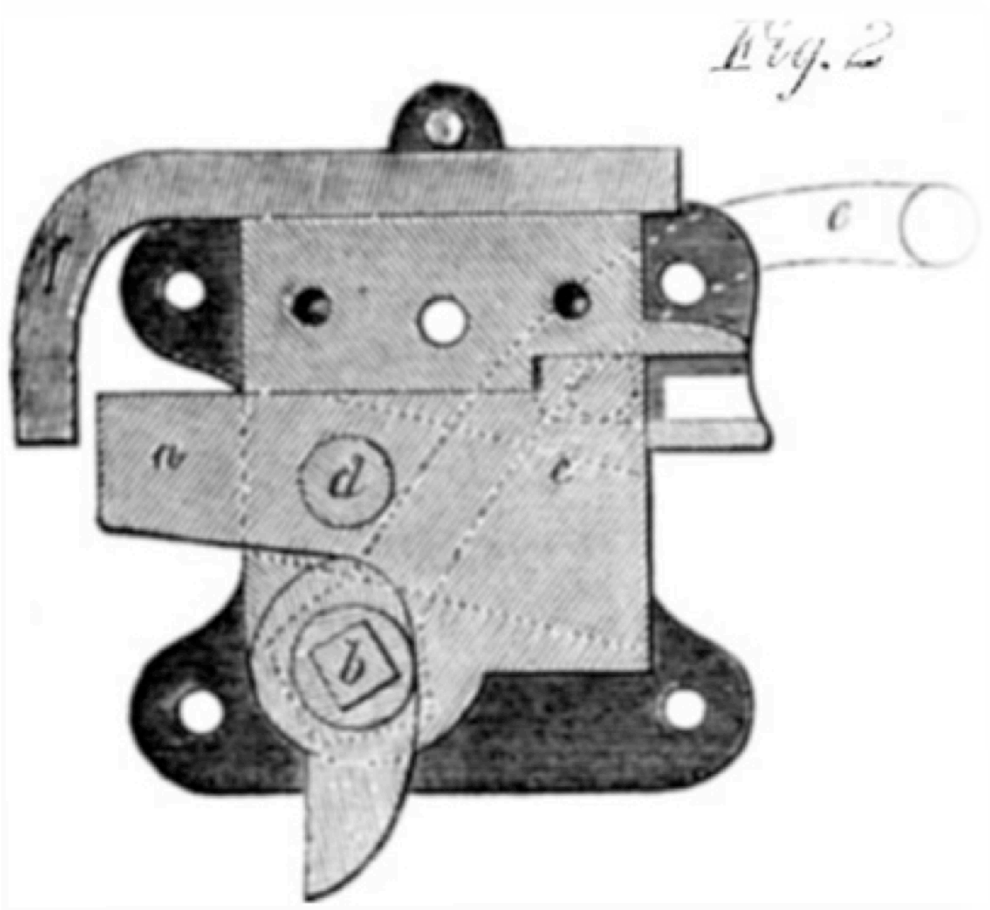
- Validating a certificate requires finding the "chain of trust"
  - between the Certification Authority (CA) whom the relying party trusts, namely the **Trust Anchor**, and the issuer of the certificate being validated.

A Quick Primer on Certificates and Validation

- Conventionally, these trust anchors (TA) are obtained ‘out of band’ from any specific certificate chain being validated.
  - For example, You may receive a large number of TAs embedded in browsers
  - operating systems often use pre-loaded TAs to support the integrity of code distribution through signed code releases, such as iOS, OSX or Windows.
- The integrity of the checking process for a digital signature depends on the integrity of the TA.

The RPKI TA Framework





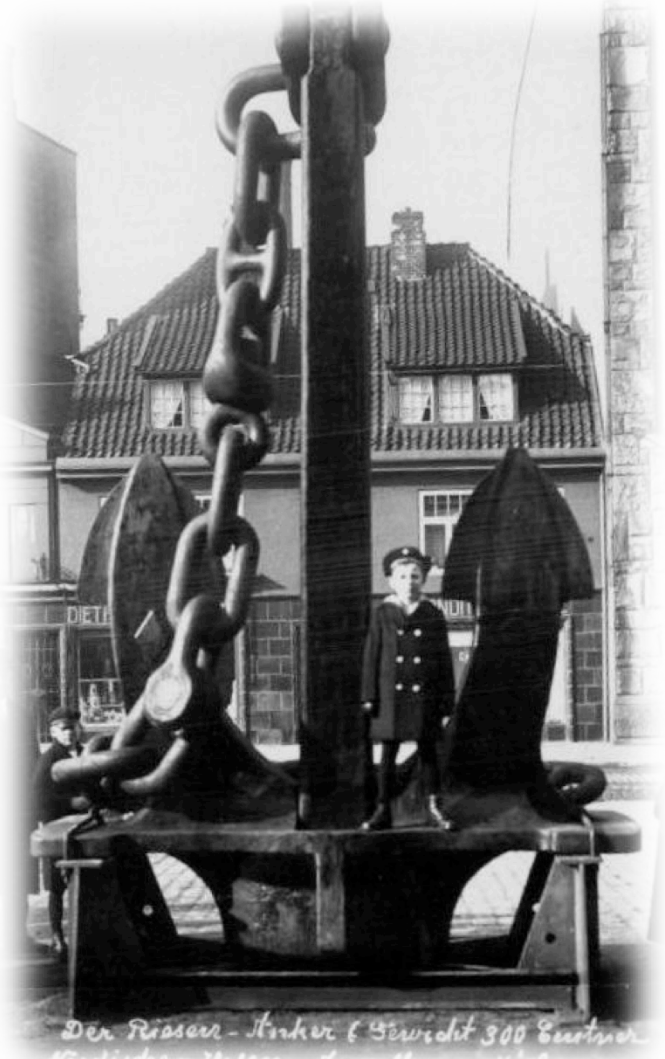
The RPKI TA Framework

- Managing TAs is an issue of concern in the RPKI because the integrity of the assertions will be ‘tested’ by relying parties against the TAs they hold.
- At present there is no single TA covering the entire span of the IP address space.
  - Today we use a collection of TAs, where each TA encompasses a subset of the address space under separate registry management.
- Each Regional Internet Registry publishes its own public key as a ‘putative’ TA for relying parties to use.

The RPKI TA Framework

- TA management is not directly defined by the RPKI standards, except in respect of the TA Locator or ‘TAL’
  - Mechanism to fetch public key of TA, and URL to fetch it.
  - Relying parties can obtain the root RPKI certificate, and then anchor validation chains of RPKI certificates.
- A relying party can use multiple TAs, and these can encompass overlapping ranges of Internet Number Resources,
  - because the validation process is defined as finding **any** TA which can validate the resources in the PKI
  - not a **specific** TA.

APNIC's TA Changes



APNIC's TA Changes

- When APNIC started deploying RPKI, it adopted a simple model of anchoring its resources in a single TA.

APNIC Trust Anchor Certificate
1/8, 14/8, 36/8,...

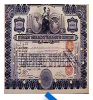
APNIC-Issued Certificates for resource-holding members

APNIC's TA Changes

- When APNIC started deploying RPKI, it adopted a simple model of anchoring its resources in a single TA.
  - This was easy to deploy
  - reflected our understanding at the time
    - internet number resources we had administrative management authority over within APNIC's registry,
    - as distinct from the other RIR registries that provide number resource management.

APNIC's TA Changes

- As the RPKI project has progressed, other RIR are now publishing their own TA, and these TAs include resources that are contained in the APNIC registry.



ARIN Trust Anchor Certificate
... 128/8, ...

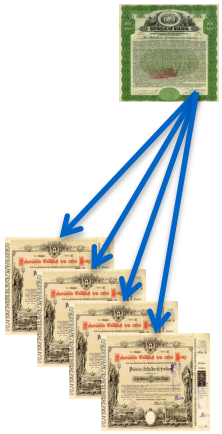
?

APNIC-Registry: ...128.134/16 ...

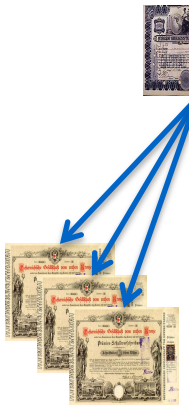
APNIC's TA Changes

- Re-align our issued certificates to accurately reflect the "provenance " of the resources that are held in our registry.
  - E.G. if a resource in APNIC's registry is a fragment of a larger block that is held in the RIPE NCC's registry, then we would like to use a certificate structure that reflects this.
- Structure APNIC's RPKI certificate collection, and the associated TA material
  - Reflect the hierarchy of registry responsibility for internet number resource management.

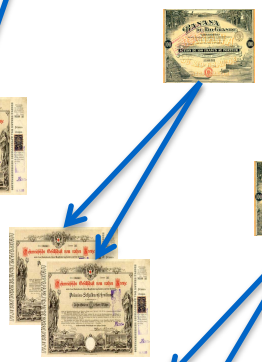
APNIC's TA Changes



APNIC-from-IANA Trust Anchor Certificate
1/8, 14/8, 36/8,...



APNIC-from-ARIN Trust Anchor Certificate
128.134/16,...



APNIC-from-RIPE NCC Trust Anchor Certificate

APNIC-from-LACNIC Trust Anchor Certificate

APNIC-from-AFRINIC Trust Anchor Certificate

APNIC's TA Changes

- APNIC's TA are 5 discrete components, reflecting the different 'inheritance' paths
  - Resources for which IANA has assigned responsibility to APNIC.
    - Number blocks described in the IANA number registries as being assigned to APNIC, such as 42.0.0.0/8 and 2400::/12
  - Resources managed by APNIC, transferred as a fragment of a larger number block, that is administered by another RIR.
- This *inter-RIR registry arrangement* is typically the result of a relocation of administrative control from one RIR region to another
  - E.G. when a multinational entity decides to move Internet Number resource management from Europe to its Asian office
  - may arise from an inter-RIR address transfer.
- Split TA maintains a direct relationship between the RPKI certificate structure and the specific path of registry responsibility that APNIC has over those resources through another RIR

APNIC's TA Changes

- By converting to this split TAL model **now**:
  - APNIC avoids any future need to re-issue operating certificates, and the associated resources held by members in future.
  - Given that we have few products published now, but intend promoting RPKI strongly through 2013, we have avoided a future migration for all RPKI certified members.

APNIC's TA Changes

- Other RIRs have taken a different approach and have opted to publish all resources they hold under the hierarchy of a single "root" certificate, which is, in effect, their TA.
- Right now we are not sure if this represents the preferred option for the community of RPKI relying parties.
  - If there is a desire to further simplify the APNIC TA structure it is possible to generate a single encompassing certificate and publish a single APNIC TA.
- We would like to understand the larger story of the overall direction of RPKI trust anchors and the community preference relating to the management of trust anchors across the entire RPKI as a precursor to further changes in this area.

Standards Compliance

Standards Compliance

- We found our system has not kept pace with the changing standards environment.
  - APNIC began offering RPKI services in 2009
    - Elements of our code were built prior to the completion of IETF standards in this area.
  - We had concentrated on a service delivery code development, and not targeted ‘relying party’ tools
    - so we did not have our own RPKI validation tools to check our published RPKI products with, against other implementations

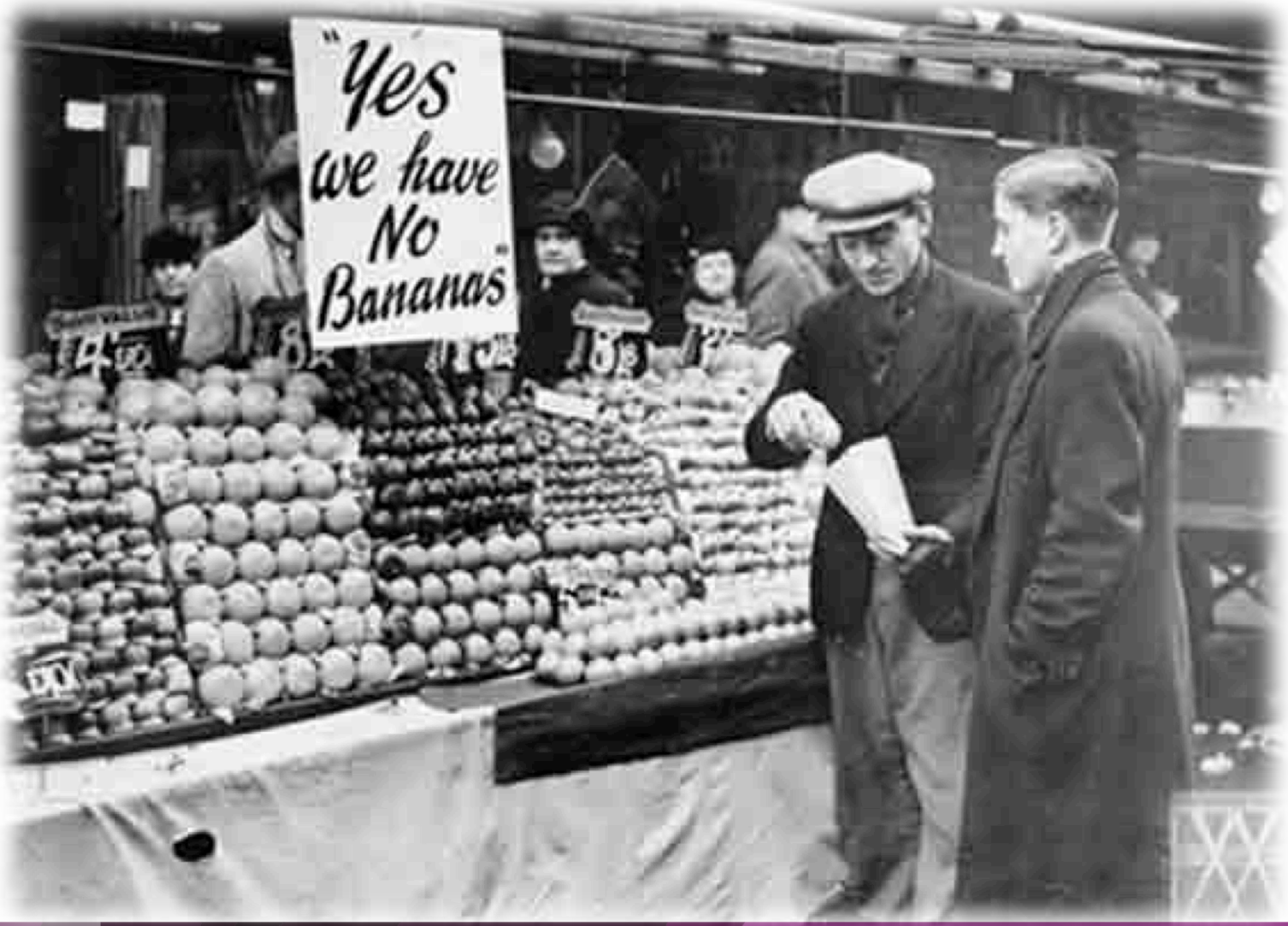
Standards Compliance

- RPKI.NET and the RIPE NCC engineers have written fully independent relying-party validation tools
  - APNIC was able to test its products under both.
    - This has identified a small number of incompatibilities which were due to our pre-standardization deployment.
  - We hadn't ensured that issued certificates used the right ASN.1 encoding for textual labels.
    - We've now ensured we use an alphabet which adopts the appropriate ASN.1 encoding for strings all the time.
  - Some mandatory elements were missing, and others wrongly encoded.

Standards Compliance

- As of the time of writing, APNIC's published RPKI products show "all green" on the status boards for both web relying-party repository tools.
  - We continue to monitor as the relying party codebase is upgraded.
- We are now checking this aspect of our RPKI systems much more closely
  - software processes to keep our encodings and products in line with community expectations as expressed in the commonly used relying party tool sets.

Provisioning Protocol Services



Provisioning Protocol Services

- APNIC has been running a provisioning protocol (the “up/down” protocol) since the inception of our web portal service.
  - The MyAPNIC portal uses provisioning protocol to talk to the APNIC RPKI engine
  - to ensure strict separation between the RPKI products we make, as a registry, and the RPKI products that our members direct us to make.
- However, we hadn’t provided a publicly visible port of this RPKI certificate management protocol to the wider community
  - we didn’t have any mechanism to exchange business PKI information, which is necessary since the messages which flow over provisioning protocol are signed CMS.

Provisioning Protocol Services

- We're in the process of writing an Interface on the MyAPNIC Portal to permit members to upload their business PKI (bPKI)
  - using the RPKI.NET defined XML which encodes the trust chain, behind the certificate which will be used 'on the wire' to sign the CMS.
- By incorporating this key material into the APNIC trust set, we can validate
  - that the CMS part of the subsequent protocol exchange is well signed,
  - that the certificate chain over it reflects the currently known authority provided by that member.

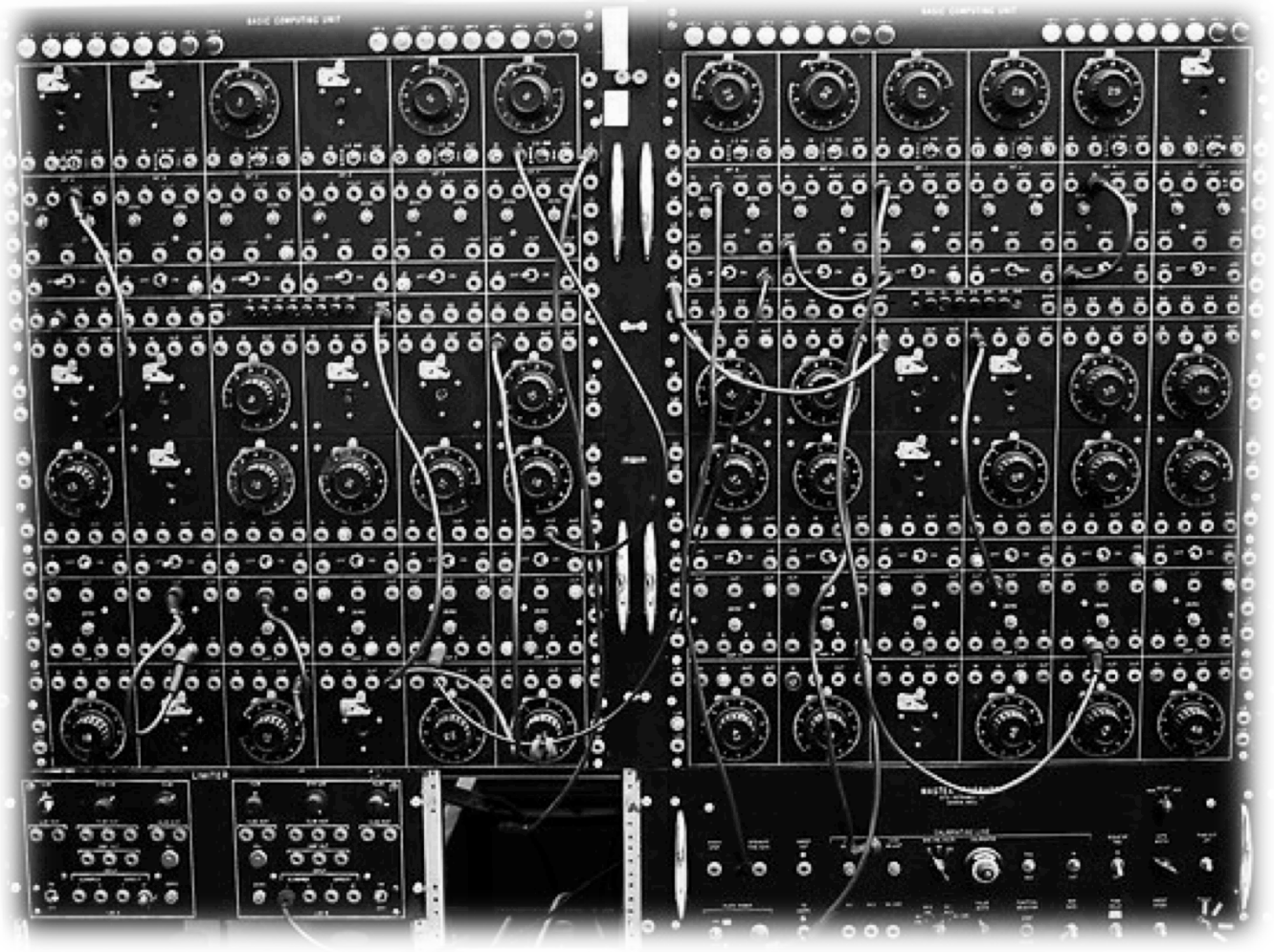
Provisioning Protocol Services

- We believe this is a good reflection of community expectations, although its details are not currently defined by any standards or draft-standard.
  - Rob Austein, the developer, has informed us that the XML may well change in 2013 to reflect changes in his model of provisioning new bPKI relationships
  - we intend working to adopt his new model as it is defined.

Provisioning Protocol Services

- APNIC has also identified process complexities in migrating from an existing hosted solution (using MyAPNIC to create RPKI outcomes) to an external (self-hosted) system.
  - Obvious risks where there is both a "live" RPKI space in the MyAPNIC managed service area, and a “live" RPKI space managed entirely by the member.
  - We are designing a User Interface which clearly identifies the transitional stages, and ensures the member is clearly in charge of the transition process at all times.

RPKI User Interface changes to the MyAPNIC Portal



RPKI User Interface changes to the MyAPNIC Portal

- APNIC's original RPKI user interface (UI) was designed over 3 years ago, and reflected our sense of how users wanted to specify signing operations over their resources:
  - We designed a system for making abstract named collections of resources, modeling the concepts like "my customers" or "my infrastructure"
  - so that members could create signed outcomes which reflected the distinctions of use between different classes of resources held by the member.
- We also made it explicit that Route Origin Attestations (ROA) had specific lifetimes and exposed the exact state of the ROA to the member.

RPKI User Interface changes to the MyAPNIC Portal

- A radically simpler model had been developed by the RIPE NCC:
  - Hides the existence of any specific ROA from the user and concentrate on the more abstract idea of "my certified prefixes"
  - The user is presented with a list of what is seen in routing (ie in BGP) and what they have currently defined, each as a list of prefix and origin-AS couplets.
  - As long as you specify you want the given prefixes to be originated by the given origin-AS, the system ensures that exactly the right ROAs are published to achieve this, and that they are subsequently kept up to date.
- .

RPKI User Interface changes to the MyAPNIC Portal

- We liked this system a lot.
- We liked it so much, that we asked the RIPE NCC if we could take their design and re-implement it into our MyAPNIC portal, and a redesign is now underway, due for release early in 2013.

RPKI User Interface changes to the MyAPNIC Portal

- We see benefits in this adoption of a common UI which should help with RPKI deployment for everyone:
  - Training and Promotional materials are now much more likely to be similar in both the APNIC and the RIPE NCC regions.
  - Members who maintain resources in both regions will have a more consistent UI experience managing their resources in each portal.
  - Reporting tools under development by the RIPE NCC are much more likely to deliver outcomes useful to members who maintain their RPKI in the APNIC portal.
- Early version of the new UI released here at the APRICOT meeting.
  - This initial UI will then be further developed and brought into alignment with the RIPE NCC portal as it develops in turn.

Home

Welcome to MyAPNIC

What can I do?

- View and update your resource information for IPv4, IPv6, AS numbers and Whois updates
- Manage your resource certificates
- View your Member details and Contact details.
- Use the Training section to view training and events history
- Use the APNIC looking glass or generate a prefix report

News

- More news...

Hello Robert!

My Profile

Membership details

Account: **ACE-JP**

Expiry: **2013-12-31** Renew

Tier: **medium**

APNIC Digital Certificate

Get your certificate now.

Error: certificate enrolment is not supported for your browser.

Useful links

MyAPNIC features

IRT object guide

How do I create a Route object?

IP address calculator

Reverse DNS troubleshooting

Training

Annual membership fees calculator

Welcome to MyAPNIC

What can I do?

- View and update your resource information for IPv4, IPv6, AS numbers and Whois updates
- Manage your resource certificates
- View your Member details and Contact details.
- Use the Training section to view training and events history
- Use the APNIC looking glass or generate a prefix report

News

- More news...

Hello Robert!

My Profile

Membership details

Account: **ACE-JP**

Expiry: **2013-12-31** Renew

Tier: **medium**

APNIC Digital Certificate

Get your certificate now.

Error: certificate enrolment is not supported for your browser.

Useful links

MyAPNIC features

IRT object guide

How do I create a Route object?

IP address calculator

Reverse DNS troubleshooting

Training

Annual membership fees calculator

RPKI

Enable Resource Certification

Currently, you have not enabled resource certification for your registry.

- (•) I want to operate in the MyAPNIC RPKI portal.
- ( ) I want to host my own certification authority and run an RPKI engine myself.

Next

RPKI

Enable Hosted Resource Certification

Currently, you have not enabled resource certification for your registry.

Terms and Conditions of APNIC Certification Authority

Introduction

APNIC publishes all Certificates, Certificate Revocation Lists (CRLs), and RPKI-signed objects in the Certification Repository ("**Repository**"). The Repository is available to anyone under these Terms and Conditions.

Article 1 - Definitions

In the Terms and Conditions, unless the context requires otherwise, the following terms have the meanings assigned to them below:

APNIC – APNIC Pty Ltd ACN 081 528 010 (a company incorporated under the laws of Australia), the

I accept. Create my Certification Authority

RPKI

Activating engine, please wait...

RPKI

ROA Configuration

Origin ASN | Prefix | Max Length | Add | Add & clone | Clear

All | Changes | Items per page 10 | Search by AS or IP...

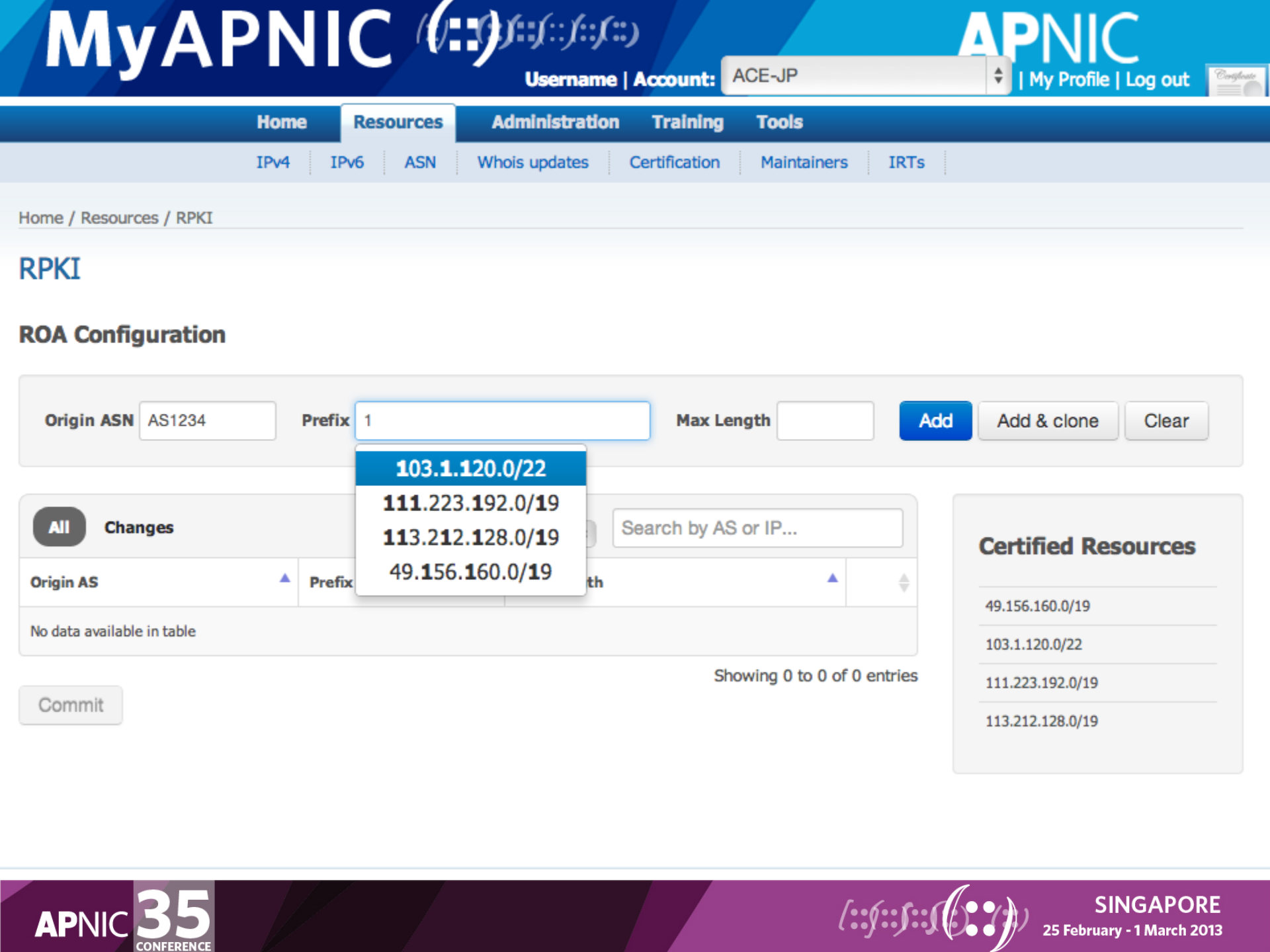
Origin AS	Prefix	Max Length	
No data available in table			

Showing 0 to 0 of 0 entries

Commit

Certified Resources

- 49.156.160.0/19
- 103.1.120.0/22
- 111.223.192.0/19
- 113.212.128.0/19


MyAPNIC
APNIC
Username | Account: ACE-JP | My Profile | Log out
Home
Resources
Administration
Training
Tools
IPv4
IPv6
ASN
Whois updates
Certification
Maintainers
IRTs
Home / Resources / RPKI
RPKI
ROA Configuration
Origin ASN AS1234
Prefix 1
Max Length
Add
Add & clone
Clear
103.1.120.0/22
111.223.192.0/19
113.212.128.0/19
49.156.160.0/19
All
Changes
Search by AS or IP...
Origin AS
Prefix
No data available in table
Showing 0 to 0 of 0 entries
Commit
Certified Resources
49.156.160.0/19
103.1.120.0/22
111.223.192.0/19
113.212.128.0/19
APNIC 35 CONFERENCE
SINGAPORE
25 February - 1 March 2013

RPKI

ROA Configuration

Origin ASN AS1234 Prefix 111.223.192.0/19 Max Length 19 Add | Add & clone | Clear

All | Changes | Items per page 10 | Search by AS or IP...

Origin AS	Prefix	Max Length	
No data available in table			

Showing 0 to 0 of 0 entries

Commit

Certified Resources

- 49.156.160.0/19
- 103.1.120.0/22
- 111.223.192.0/19
- 113.212.128.0/19

RPKI

ROA successfully marked for addition (AS1234, 111.223.192.0/19, 19). Remember to commit you changes. ×

ROA Configuration

Origin ASN | Prefix | Max Length | Add | Add & clone | Clear

All | Changes | Items per page 10 | Search by AS or IP...

Origin AS	Prefix	Max Length	
AS1234	*111.223.192.0/19*	*19*	🗑

Showing 1 to 1 of 1 entries

< 1 of 1 >

Commit

Certified Resources

- 49.156.160.0/19
- 103.1.120.0/22
- 111.223.192.0/19
- 113.212.128.0/19

RPKI

ROA successfully marked for addition (AS1, 103.1.120.0/22, 32). Remember to commit you changes.

ROA Configuration

Origin ASN | Prefix | Max Length | Add | Add & clone | Clear

All | Changes | Items per page 10 | Search by AS or IP...

Origin AS	Prefix	Max Length	
AS1	*103.1.120.0/22*	*32*	
AS1234	*111.223.192.0/19*	*19*	

Showing 1 to 2 of 2 entries

< 1 of 1 >

Commit

Certified Resources

- 49.156.160.0/19
- 103.1.120.0/22
- 111.223.192.0/19
- 113.212.128.0/19

RPKI

Done!

ROA Configuration

Origin ASN | Prefix | Max Length | Add | Add & clone | Clear

All | Changes | Items per page 10 | Search by AS or IP...

Origin AS	Prefix	Max Length	
1	103.1.120.0/22	32	
1234	111.223.192.0/19	19	

Showing 1 to 2 of 2 entries

< 1 of 1 >

Commit

Certified Resources

- 49.156.160.0/19
- 103.1.120.0/22
- 111.223.192.0/19
- 113.212.128.0/19

RPKI

Enable Resource Certification

Currently, you have not enabled resource certification for your registry.

- ○ I want to operate in the MyAPNIC RPKI portal.
- ◉ I want to host my own certification authority and run an RPKI engine myself.

Next

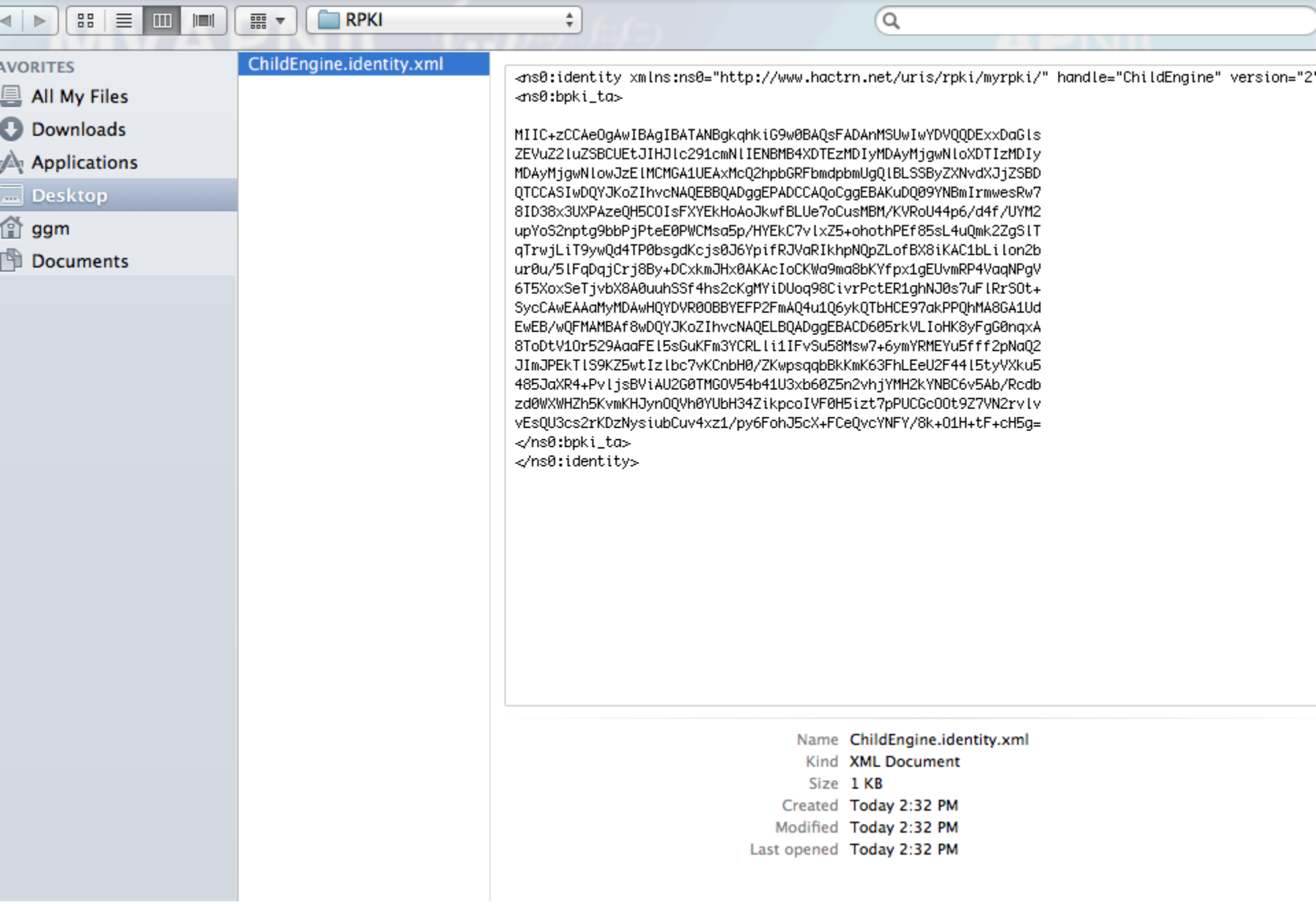
RPKI

Create new Engine

Upload XML... Submit

Certified Resources

You have no certified resources!


RPKI
AVORITES
All My Files
Downloads
Applications
Desktop
ggm
Documents
ChildEngine.identity.xml
<ns0:identity xmlns:ns0="http://www.hactrn.net/uris/rpki/myrpki/" handle="ChildEngine" version="2"
<ns0:bpki_ta>
MIIC+zCCAeOgAwIBAgIBATANBgkqhkiG9w0BAQsFADAnMSUwIwYDVQQDExxDaGls
ZEVuZ2luZSBCUEtJIHJlc291cmNlIENBMB4XDTEzMDIyMDAyMjgwNloXDTIzMDIy
MDAyMjgwNlowJzElMCMGA1UEAxMcQ2hpbGRFbmdpbmUgQlBLSSByZXNvdXJjZSBD
QTCCASIwDQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBAKuDQ09YNBmIrmwesRw7
8ID38x3UXPAzeQH5COIsFXYEkHoAoJkwfBLUe7oCusMBM/KVRoU44p6/d4f/UYM2
upYoS2nptg9bbPjPteE0PWCMsa5p/HYEkC7vlxZ5+ohothPEf85sL4uQmk2ZgSlT
qTrwjLiT9ywQd4TP0bsgdKcjs0J6YpifRJVaRIkhpNQpZLofBX8iKAC1bLilon2b
ur0u/5lFqDqjCrj8By+DCxkmJHx0AKAcIoCKWa9ma8bKYfpx1gEUvmRP4VaqNPgV
6T5XoxSeTjvbX8A0uuhSSf4hs2cKgMYiDUoq98CivrPctER1ghNJ0s7uFlRrSOt+
SycCAwEAAaMyMDAwHQYDVR0OBBYEFP2FmAQ4u1Q6ykQTbHCE97akPPQhMA8GA1Ud
EwEB/wQFMAMBAf8wDQYJKoZIhvcNAQELBQADggEBACD605rkVLIoHK8yFgG0nqxA
8ToDtV1Or529AaaFEl5sGuKFm3YCRLli1IFvSu58Msw7+6ymYRMEYu5fff2pNaQ2
JImJPEkTlS9KZ5wtIzlbc7vKCnbH0/ZKwpsqqbBkKmK63FhLEeU2F44l5tyVXku5
485JaXR4+PvljsBViAU2G0TMGOV54b41U3xb60Z5n2vhjYMH2kYNBC6v5Ab/Rcdb
zd0WXWHZh5KvmKHJynOQVh0YUbH34ZikpcoIVF0H5izt7pPUCGcOOt9Z7VN2rvlv
vEsQU3cs2rKDzNysiubCuv4xz1/py6FohJ5cX+FCeQvcYNFY/8k+O1H+tF+cH5g=
</ns0:bpki_ta>
</ns0:identity>
Name ChildEngine.identity.xml
Kind XML Document
Size 1 KB
Created Today 2:32 PM
Modified Today 2:32 PM
Last opened Today 2:32 PM

RPKI

Selected file: ChildEngine.identity.xml (text/xml, 1185 bytes)

Create new Engine

Upload XML... Submit

Certified Resources

You have no certified resources!

RPKI

Uploading XML file... please wait...

Create new Engine

Upload XML... Submit

Certified Resources

You have no certified resources!

RPKI

Uploading XML file... please wait...

Create new Engine

Upload XML... Submit

Certified Resources

You have no certified resources!

RPKI

My Engine

Description	Actions
A91DC5BE0000	Upload new XML... Download parent XML

Certified Resources

- 180.149.224.0/20
- 202.12.28.0/23
- 202.12.31.0/24
- 203.119.0.0/24
- 203.119.42.0/23
- 203.119.76.0/23
- 203.119.86.0/24
- 203.119.92.0/23
- 203.119.95.0/24
- 203.119.96.0/20

RPKI

My Engine

Description	Actions
A91DC5BE0000	Upload new XML... Download parent XML

Certified Resources

- 180.149.224.0/20
- 202.12.28.0/23
- 202.12.31.0/24
- 203.119.0.0/24
- 203.119.42.0/23
- 203.119.76.0/23
- 203.119.86.0/24
- 203.119.92.0/23
- 203.119.95.0/24

APNIC-AP/rest/rpki/children/7/identity.xml

our computer. Do you
xml anyway?
Discard Keep

bash

```
tity_APNIC-AP_7.xml
ion="1.0"?>
t xmlns:oob="http://www.hactrn.net/uris/rpki/myrpki/" version="2" service_uri="http://rpki1.tst.apnic.net/cgi-bin/up-dow
C-AP/" parent_handle="APNIC-AP" child_handle="A91DC5BE0000"><oob:bpki_resource_ta>MIICADCCAWmgAwIBAgIBATANBgkqhkiG9w0BAQ
GAYDVQQDExFUZXN0
9vdCBDQTAeFw0xMzAyMjAwMjAzNDFaFw0yMzAyMTgwMjAzNDFaMB4x
MTE1Rlc3QgQlBLSSBTZXJ2ZXIgQ0EwgZ8wDQYJKoZIhvcNAQEBBQAD
GBALX01NOngjx4P6PzJaUlJmoBZpzDeoPKk5hdcc6bdtJBG78MqFDf
AiePiSl8jAEbhcYG7Vnft58Sh7s4hvTcaeKo4SbMSljT//PReb9dLC
6QgUI0Y0iKqElZYENBoAT/yF76+/+CaIZgZohYit7GY+YJAgMBAAGj
UdEwQFMAMBAf8wHQYDVR0OBBYEFA/HmnYXxhq+l635tljHulWdoCK6
QYMBaAFFTxD+8MnOdW/hwbrUoKkwI6gFcoMA0GCSqGSIb3DQEBCwUA
4/q52dTVc7sF+4dx7b44exeFoMRcxFmmPVgHB2OlgRTHS2rkUUE61L
XJ8qf2lA9YLbKsx4x1P0os8vnu43qfEz5qSQosd/JdiOgI3r82oJNM
LAljfr+1EGD7hyULchiIs44weScHrRjD4b1U6P

_resource_ta><oob:bpki_child_ta>MIIC+zCCAeOgAwIBAgIBATANBgkqhkiG9w0BAQsFADAnMSUwIwYDVQQDExxDaGls
BCUEtJIHJlc291cmNlIENBMB4XDTEzMDIyMDAyMjgwNloXDTIzMDIy
owJzElMCMGA1UEAxMcQ2hpbGRFbmdpbmUgQlBLSSByZXNvdXJjZSBD
YJKoZIhvcNAQEBBQADggEPADCCAQoCggEBAKuDQ09YNBmIrmwesRw7
AzeQH5COIsFXYEkHoAoJkwfBLUe7oCusMBM/KVRoU44p6/d4f/UYM2
9bbPjPteE0PWCMsa5p/HYEkC7vlxZ5+ohothPEf85sL4uQmk2ZgSlT
wQd4TP0bsgdKcjs0J6YpifRJVaRIkhpNQpZLofBX8iKAC1bLilon2b
qjCrj8By+DCxkmJHx0AKAcIoCKWa9ma8bKYfpx1gEUvmRP4VaqNPgV
vbX8A0uuhSSf4hs2cKgMYiDUoq98CivrPctER1ghNJ0s7uFlRrSOt+
MyMDAwHQYDVR0OBBYEFP2FmAQ4u1Q6ykQTbHCE97akPPQhMA8GA1Ud
MBAf8wDQYJKoZIhvcNAQELBQADggEBACD605rkVLIoHK8yFgG0nqxA
29AaaFEl5sGuKFm3YCRLli1IFvSu58Msw7+6ymYRMEYu5fff2pNaQ2
9KZ5wtIzlbc7vKCnbH0/ZKwpsqqbBkKmK63FhLEeU2F44l5tyVXku5
vljsBViAU2G0TMGOV54b41U3xb60Z5n2vhjYMH2kYNBC6v5Ab/Rcdb
KvmKHJynOQVh0YUbH34ZikpcoIVF0H5izt7pPUCGcOOt9Z7VN2rvlv
KDzNysiubCuv4xz1/py6FohJ5cX+FCeQvcYNFY/8k+O1H+tF+cH5g=

_child_ta><oob:repository type="none"/></oob:parent>
```

General sign and non-BGP uses of RPKI

General sign and non-BGP uses of RPKI

- APNIC has been interested for some time in the ways that RPKI could be used outside of secure BGP, to improve the trust in Internet Number Resource management.
  - The ways which resource holders currently request origination of their prefix by a provider is a very ad-hoc process:
    - Some members use WHOIS data to provide an out-of-band check on permission to originate.
    - Some use WHOIS data in the form of RPSL Internet Routing Registries to construct filters, and manage their view of prefix origination.
    - Others rely on the APNIC hostmasters to facilitate a process between different parties.
- We think we can use digital signatures and the RPKI to improve aspects of this situation.

General sign and non-BGP uses of RPKI

- APNIC has designed a general-signing model, which permits RPKI certificates to be used to sign more arbitrary attestations with RFC3779 certificates.
- The mechanism uses a structured signing which permits multiple signatures, and clarification of which resources are being signed against,
  - so that everyone involved can know the certificates reflect what they consciously wanted signed over, as well as performing a formal RFC5280 PKI validation of the signed products including the RFC3779 part.

General sign and non-BGP uses of RPKI

- We envisage use cases such as:
  - *"Please can you originate this prefix for me, behind your origin AS. I have created a ROA to authorize this, but I want you now to add my prefix to your BGP configuration and provide transit, signed (**prefix holder**)"*
  - *"I am interested in transferring the following resources to you for a consideration. To demonstrate I have functional control and authority over these resources, I have signed this statement with my RPKI certificate and you can compare the list of resources in this proposal with the certificate to ensure I have correctly identified the rights to transfer, signed (**prefix holder**)"*

General sign and non-BGP uses of RPKI

- This allows signed attestations to be made by resource holders that can be independently validated.
- This work is still under development, as we refine the documentation around how to encode the signed outcomes,
- We are interested in community feedback as to what would be useful here in supporting existing and new business processes relating to the use of IP addresses.

What do you think?

- We're committed to continue improving our RPKI services, and we'd love to know what people think of these changes and the proposed activity in 2013.
- If you'd like to get in touch with us, please use the MyAPNIC system to contact helpdesk or hostmaster, or get in touch with us at research@apnic.net.