An Introduction to Routing Security (and RPKI Tools)

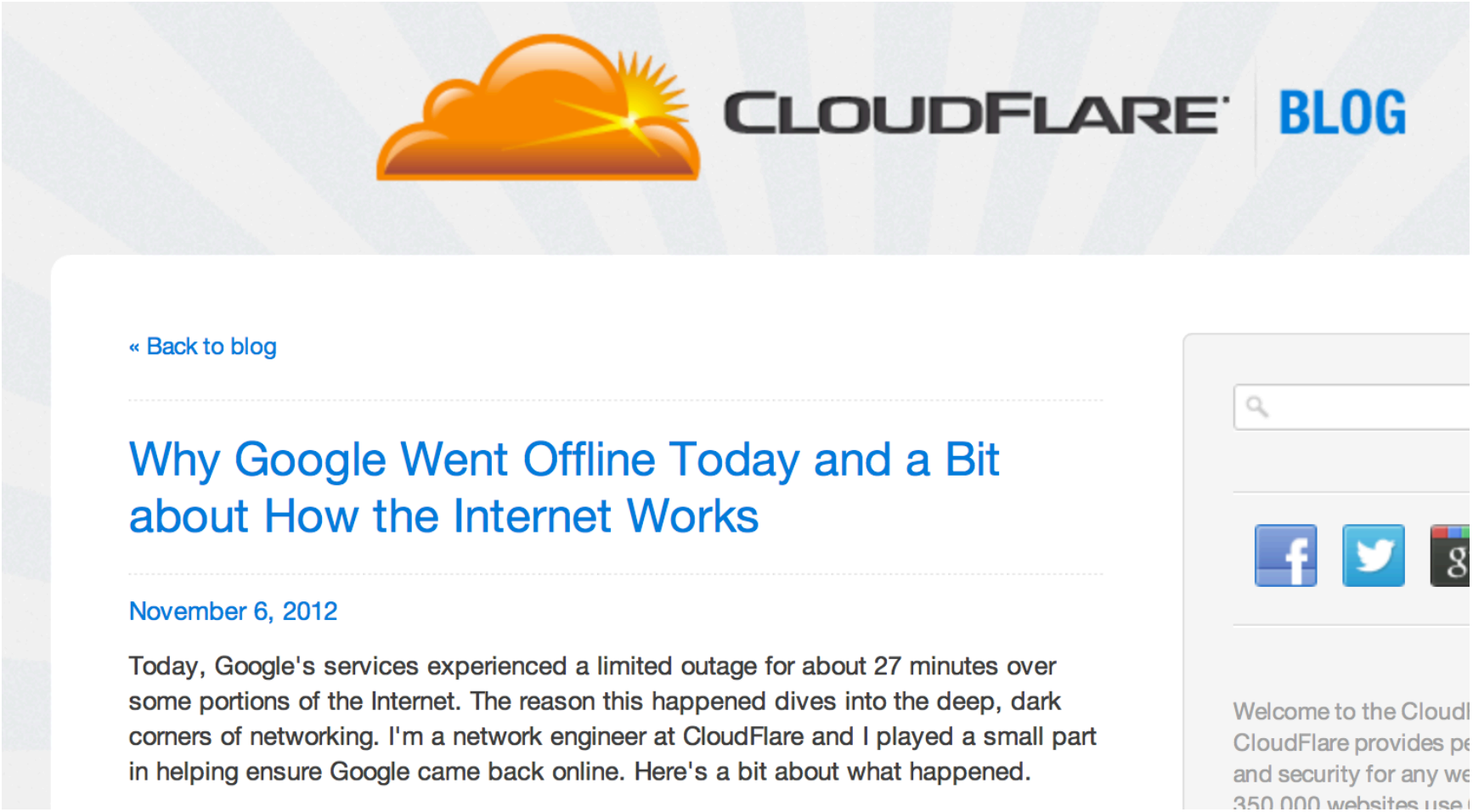
Geoff Huston

May 2013

Today's Routing Environment is Insecure

- Routing is built on mutual trust models
- Routing auditing requires assembling a large volume of authoritative data about addresses and routing policies
  - And this data does not readily exist
- We have grown used to a routing system that has some "vagueness" at the edges
  - Working out who has the authority to advertise what information into the routing system can be a difficult question to answer
- And sometimes that "vagueness" bites us…

Back in November last year...



Telling “Good Routing” from “Bad Routing”

- “BAD” routing does not proclaim itself as evil
  - So how can we identify a routing update that contains false information?
- The only robust tool we have is to be able to generate a “digital signature” that covers an object
  - The signature can tell if the digital payload has been tampered with in any way
  - And if you can validate the key used to generate the signature then you also can derive authenticity and non-repudiation
- All we can do is label “GOOD” routing, and then use the *absence* of the “good label” to infer badness

Telling “Good” from “Bad”

Therefore…

- To identify what’s “bad,” we need to clearly label everything that we’d label as “good”

And if we can do that, then…

- Can we set up a mechanism to allow an automated system to validate that the use of an address in the context of a routing protocol update has been duly authorized by the holder of that address, and that the reachability information in the routing update accurately reflects the current state of the forwarding subsystem?

Routing Registries

- We've already tried this with the Routing Registry (IRR) approach:
  - ISPs publish a list of the prefixes they intend to advertise and their route policies
  - You can use this information to automate the construction of input route filters
  - Route updates are accepted only if they pass through the filter: i.e. only if they match the constraints as specified in the route policy statements
  - Limits the extent of propagation of unregistered routes

- But routing registries have some downsides:

  High maintenance overhead, very complex policy specification, poor security model, limited uptake by AS operators, conflicting registries

BGP + Security

- Is is possible to wrap integrity credentials inside the inter-domain routing protocol?
  - Receivers of a routing update could then use the credentials attached to the update to check if the update is genuine, and has been duly authorised
- This is the foundation of BGPsec:
  - a set of additions to BGP that add attributes to BGP updates that include digital signatures over certain contents of the update

BGPsec

- Developed by the IETF)over the period 2003 to the present)
  - Strong foundation in earlier sBGP work from BBN
  - Includes additional attributes to a BGP update that hold digital signatures that sign over:
    - The origination of the route
      - Prefix holder signing over the originating AS number to convey authorization
    - Each “AS pair” in the AS path
      - AS holder signs over the next AS in the path to indicate where the update was passed
  - A BGPsec speaker uses additional information to validate that the keys used to generate these signatures are valid and trustable

Validating Credentials

This is a conventional application of public/private key cryptography, with "authority to use" conveyed by a digital signature from the authority grantor who signs across the authority subject

- Using a private key to digitally sign the authority, and the public key to validate the authority

We use a conventional X.509 Public Key certificate infrastructure to support public key validation at the scale of the Internet

- But how can we inject trustable authority into this framework?

Trustable Credentials

How can we inject trustable authority into this framework?

- Use the existing address allocation hierarchy
  - IANA to the RIRs
  - RIRs to the NIRs & LIRs,
  - NIRs and LIRs to the End holders
- Describe this address allocation structure using X.509 public key certificates
  - If A allocated a resource to B then A can issue a certificate with a subject of B, and a certificate content of the resources that A has allocated to B
  - These certificates do not introduce additional data into the registry system – they are a representation of registry information in a particular digital format

Resource Certificates

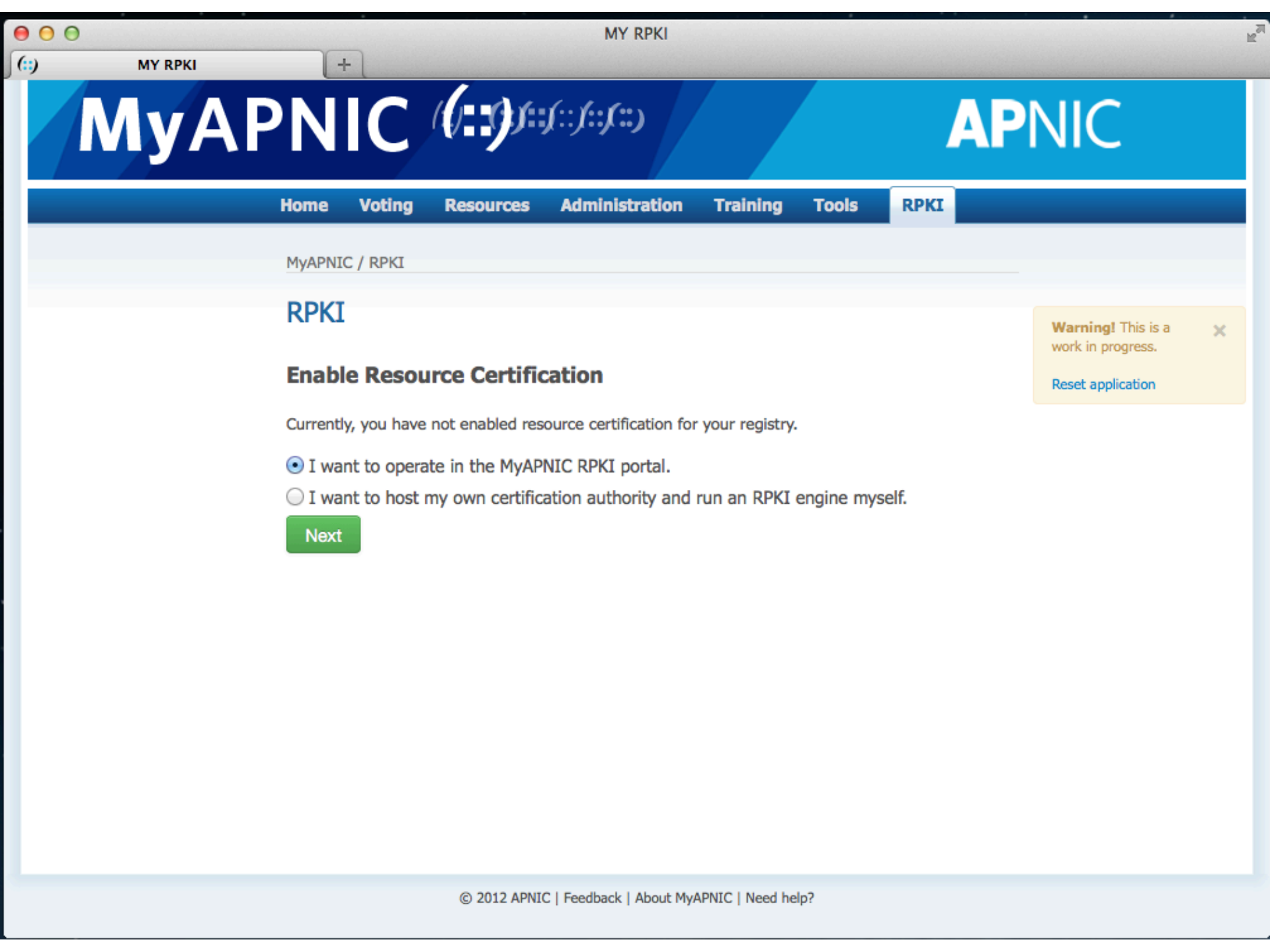
- A resource certificate is a digital document that binds together an IP address block with the IP address holder's public key, signed by the certification authority's private key
- The certificate set can be used to validate that the holder of a particular private key is held by the current legitimate holder of a particular number resource – or not!

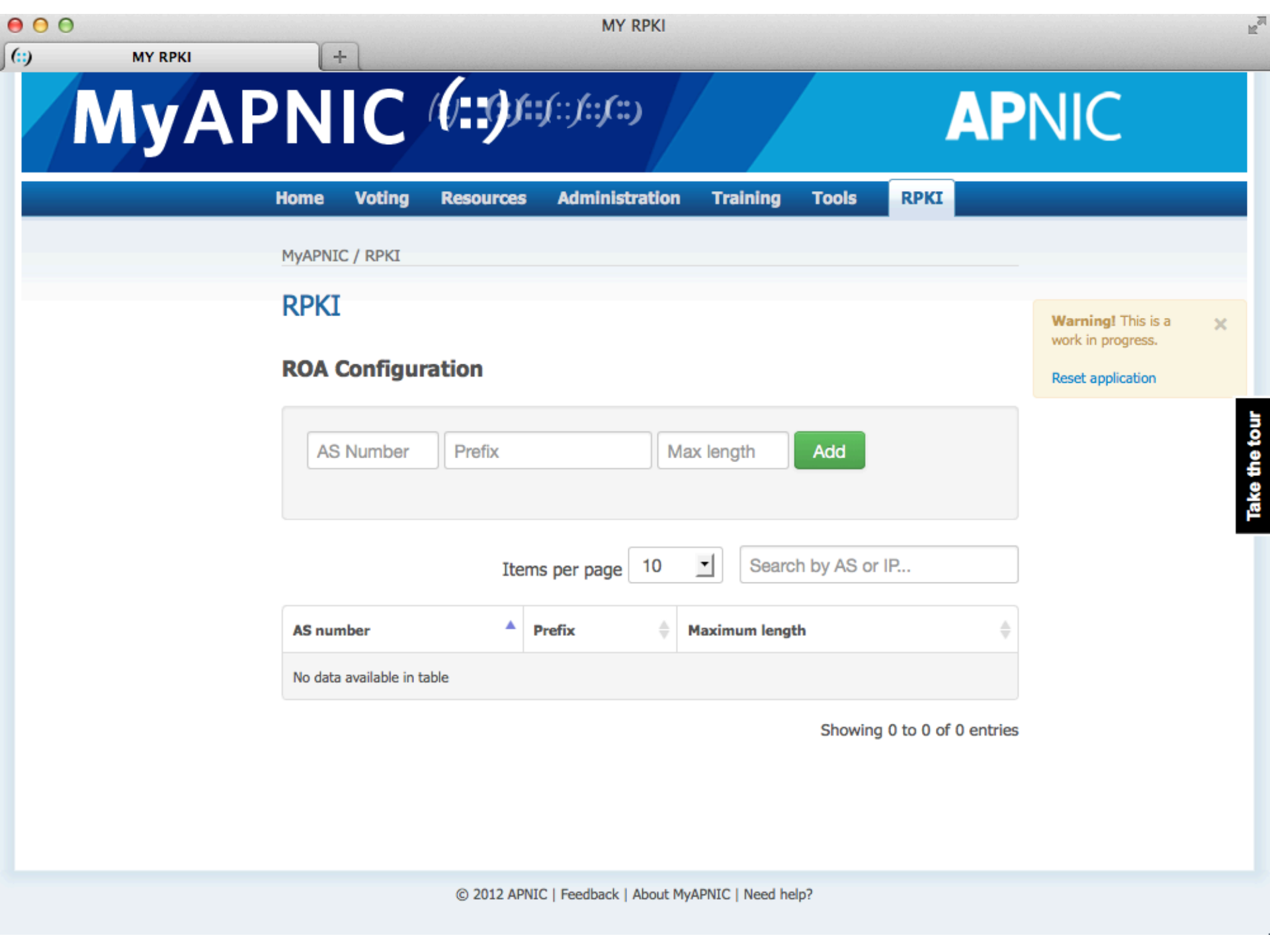
The RPKI Certificate Service

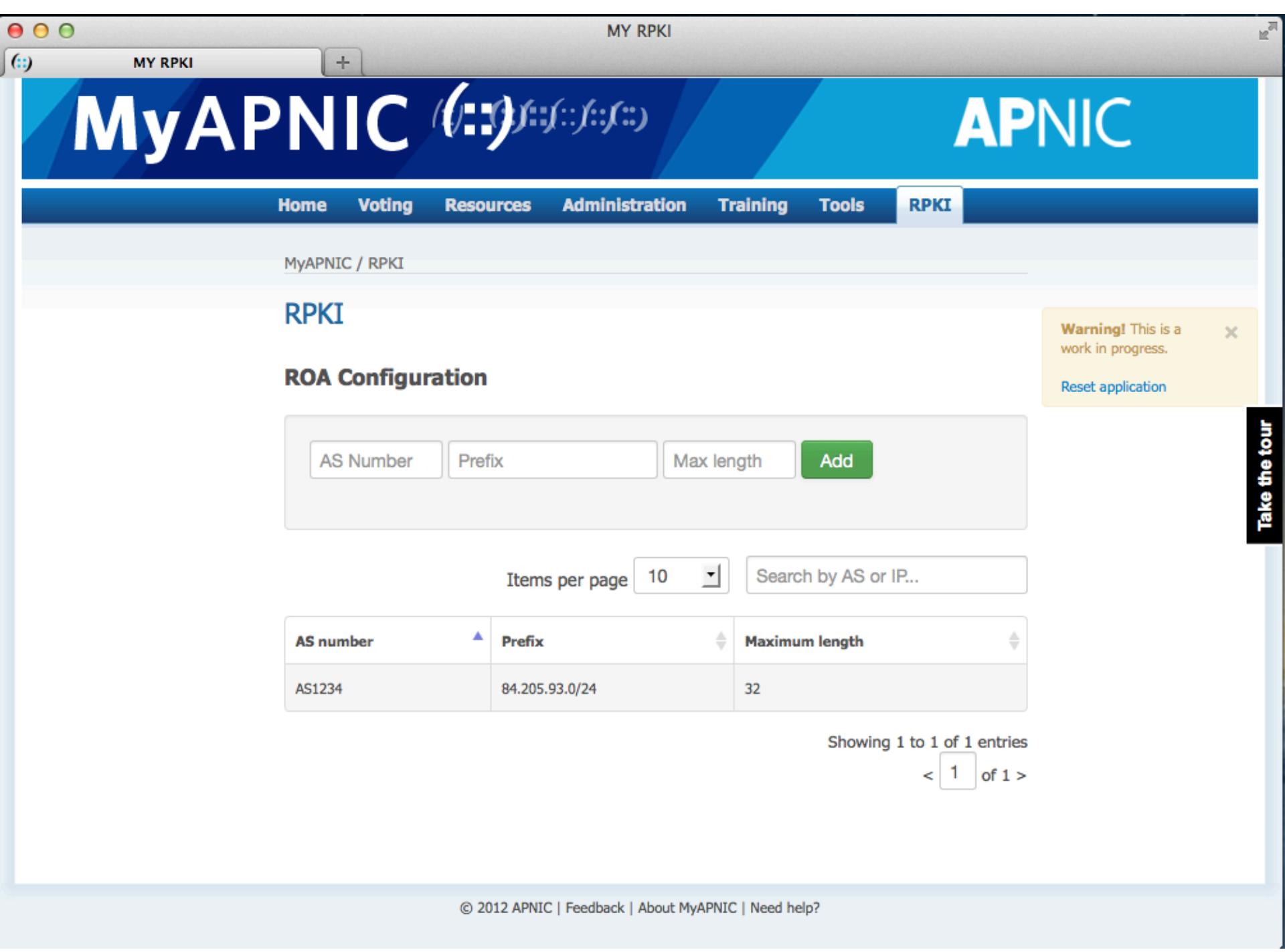
- Enhancement to the RIR Registry
  - Offers verifiable proof of number holdings
- Resource Certification is an opt-in service
  - Number Holders choose to request a certificate and provide their public key to be certified
    - Derived from registration data

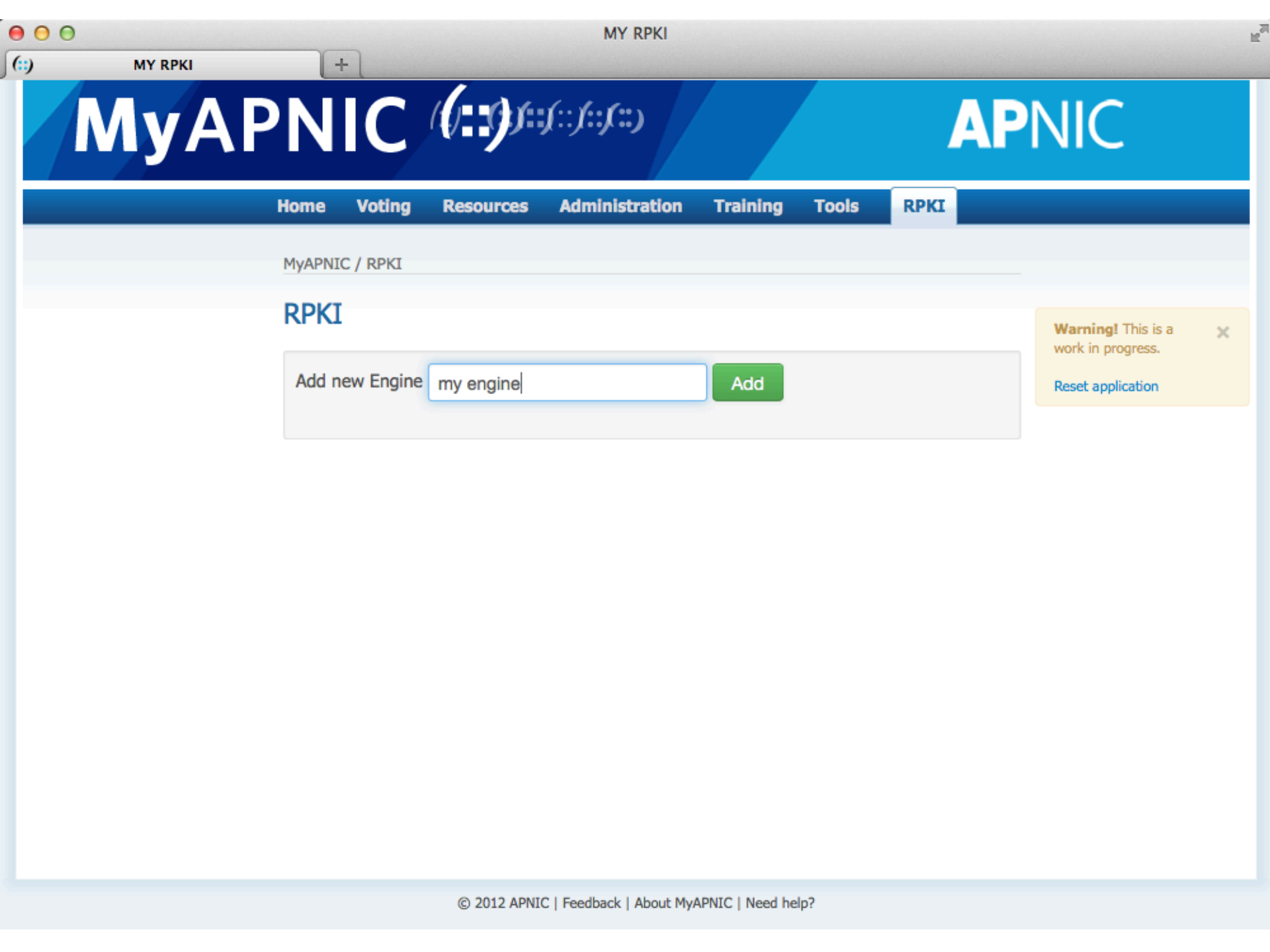
APNIC's RPKI System

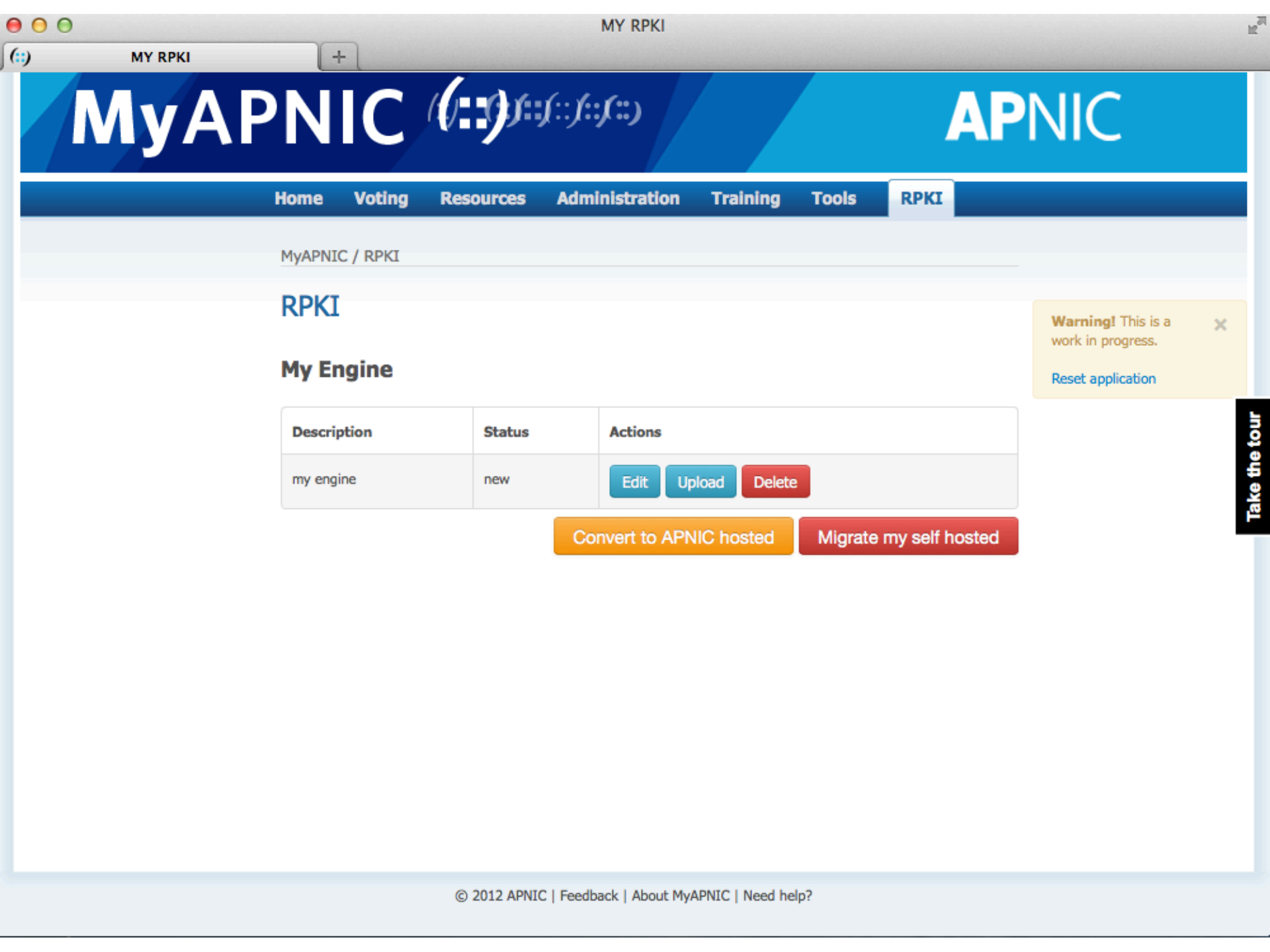
- APNIC has integrated RPKi management services into its MyAPNIC Portal for APNIC member use
- The following are some screenshots of this system


MY RPKI
MY RPKI
MyAPNIC
APNIC
Home
Voting
Resources
Administration
Training
Tools
RPKI
MyAPNIC / RPKI
RPKI
Warning! This is a work in progress.
Reset application
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
© 2012 APNIC | Feedback | About MyAPNIC | Need help?


MY RPKI
MY RPKI
MyAPNIC
APNIC
Home
Voting
Resources
Administration
Training
Tools
RPKI
MyAPNIC / RPKI
RPKI
Warning! This is a work in progress.
Reset application
ROA Configuration
AS Number
Prefix
Max length
Add
Take the tour
Items per page
10
Search by AS or IP...
AS number
Prefix
Maximum length
No data available in table
Showing 0 to 0 of 0 entries
© 2012 APNIC | Feedback | About MyAPNIC | Need help?


MY RPKI
MY RPKI
MyAPNIC
APNIC
Home
Voting
Resources
Administration
Training
Tools
RPKI
MyAPNIC / RPKI
RPKI
Warning! This is a work in progress.
Reset application
ROA Configuration
AS Number
Prefix
Max length
Add
Items per page
10
Search by AS or IP...
AS number
Prefix
Maximum length
AS1234
84.205.93.0/24
32
Showing 1 to 1 of 1 entries
< 1 of 1 >
Take the tour
© 2012 APNIC | Feedback | About MyAPNIC | Need help?


MY RPKI
MY RPKI
MyAPNIC
APNIC
Home
Voting
Resources
Administration
Training
Tools
RPKI
MyAPNIC / RPKI
RPKI
Add new Engine
my engine
Add
Warning! This is a work in progress.
Reset application
© 2012 APNIC | Feedback | About MyAPNIC | Need help?


MY RPKI
MY RPKI
MyAPNIC
APNIC
Home
Voting
Resources
Administration
Training
Tools
RPKI
MyAPNIC / RPKI
RPKI
Warning! This is a work in progress.
Reset application
My Engine
Description
Status
Actions
my engine
new
Edit
Upload
Delete
Convert to APNIC hosted
Migrate my self hosted
Take the tour
© 2012 APNIC | Feedback | About MyAPNIC | Need help?

APNIC's Current Activities

- UI developments
  - Integration of live BGP information into ROA generation (based on RIPE UI)
- Testbed Interface for RPKI-RPKI interface
  - Allows NIRs/LIRs to deploy a local RPKI engine

RIRs' Issues

- Trust Anchors for the RPKI
  - RIR Trust Anchor structure varies:
    - ARIN covers /8s + ERX in their TAL
    - RIPE NCC covers only IANA-assigned /8s in their self-signed TA (no ASNs)
    - LACNIC covers /8s + ERX in their TAL
    - AFRINIC covers only IANA-assigned /8s
    - APNIC use a split 5 self signed certs (IANA /8s, ERX from ARIN, RIPE NCC, …)
  - How many Trust Anchors?
  - What's IANA's role here?
- How to certify ERX'd resources?
- How to manage transfers in RPKI space
- Use of the RPKI provisioning protocol (RFC6492) varies

Current Activities

- Certificate Infrastructure
  - Integration of Certificate Issuance Systems into production services
  - Signing and validation service modules as plugin modules for other apps
  - Tools for the distribution and synchronization of the certificate store
- Secure Routing Systems (IETF)
  - Specification of AS Path signing extensions to BGP

Thank You