Intro to RPKI

Contact: training@apnic.net

Overview

- What is RPKI?
- Background of RPKI
- Right to Resources
- X.509 Certificates
- Route Origin Authorizations (ROA)
- What is Resource Certification?
- Creating ROA records

SIDR Working Group

- Secure Inter-Domain Routing (SIDR)
- Its purpose is to “reduce vulnerabilities to the inter-domain routing system”
- Addresses two vulnerabilities:
  - Is an Autonomous System authorized to originate an IP prefix?
  - Is the AS-Path represented in the route the same as the path through which the NLRI traveled?
- RPKI is in the process of standardization through the Secure Inter-Domain Routing (SIDR) working group

http://datatracker.ietf.org/wg/sidr/charter/

What is RPKI?

- Resource Public Key Infrastructure (RPKI)
- A robust security framework for verifying the association between resource holder and their Internet resources
- Created to address the issues in RFC 4593
- Uses X.509 v3 certificates
  - With RFC3779 extensions
- Helps to secure Internet routing by validating routes
  - Proof that prefix announcements are coming from the legitimate holder of the resource
- A system to manage the creation and storage of digital certificates and the associated Route Origin Authorization documents

RFCs on RPKI

- **RFC 6810** – The Resource Public Key Infrastructure (RPKI) to Router Protocol (January 2013) - *Standard*
- **RFC 6480** – An Infrastructure to Support Secure Internet Routing (Feb 2012) - *informational*
- **RFC 6481** – A Profile for Resource Certificate Repository Structure (Feb 2012) - *standard*
- **RFC 6491** – RPKI Objects Issued by IANA
- **RFC 6493** – The RPKI Ghostbusters Record
- **RFC 6487** – A Profile for X.509 PKIX Resource Certificate

Resource Certification Benefits

- Routing information corresponds to properly delegated address resources
- Resource Certification gives resource holders proof that they hold certain resources
- Resource holders can attest to those resources when distributing them

Benefits (Cont.)

- Resource users can 'sign' information with a digital signature, which essentially 'freezes' that information
  - Any effort to alter that information results in the signature being invalidated
  - Only resource holders with a properly delegated 'right of use' can generate a signature
- Routing advertisements are made with the explicit agreement of the current 'right of use' holder of the addresses being advertised.
- Prevents “Route Hijacking”
  - when an entity participating in Internet routing announces a prefix without authorization
  - Reason: malicious attack or operational mistake

“Right” to Resources

- ISP gets their resources from the RIR
- ISP notifies its upstream of the prefixes to be announce
- Upstream _must_ check the Whois database if resource has been delegated to customer ISP.

X.509 Certificate

- Resource certificates are based on the X.509 certificate format - RFC 5280
- Extended by RFC 3779 – this extension binds a list of resources (IP, ASN) to the subject of the certificate

X.509 Certificate with 3779 Extension

- SIA – Subject Information Access; contains a URI that references the directory

Two Components

- Certificate Authority (CA)
  - Internet Registries (RIR, NIR, Large LIR)
  - Issue certificates for customers
  - Allow customers to use the CA's GUI to issue ROAs for their prefixes
- Relying Party (RP)
  - Software which gathers data from CAs

Route Origin Attestations (ROA)

- Certificate holder uses its private key to sign an ROA
- Verifies that an AS has been given permission by an address block holder to advertise routes to one or more fpxies without a blog.

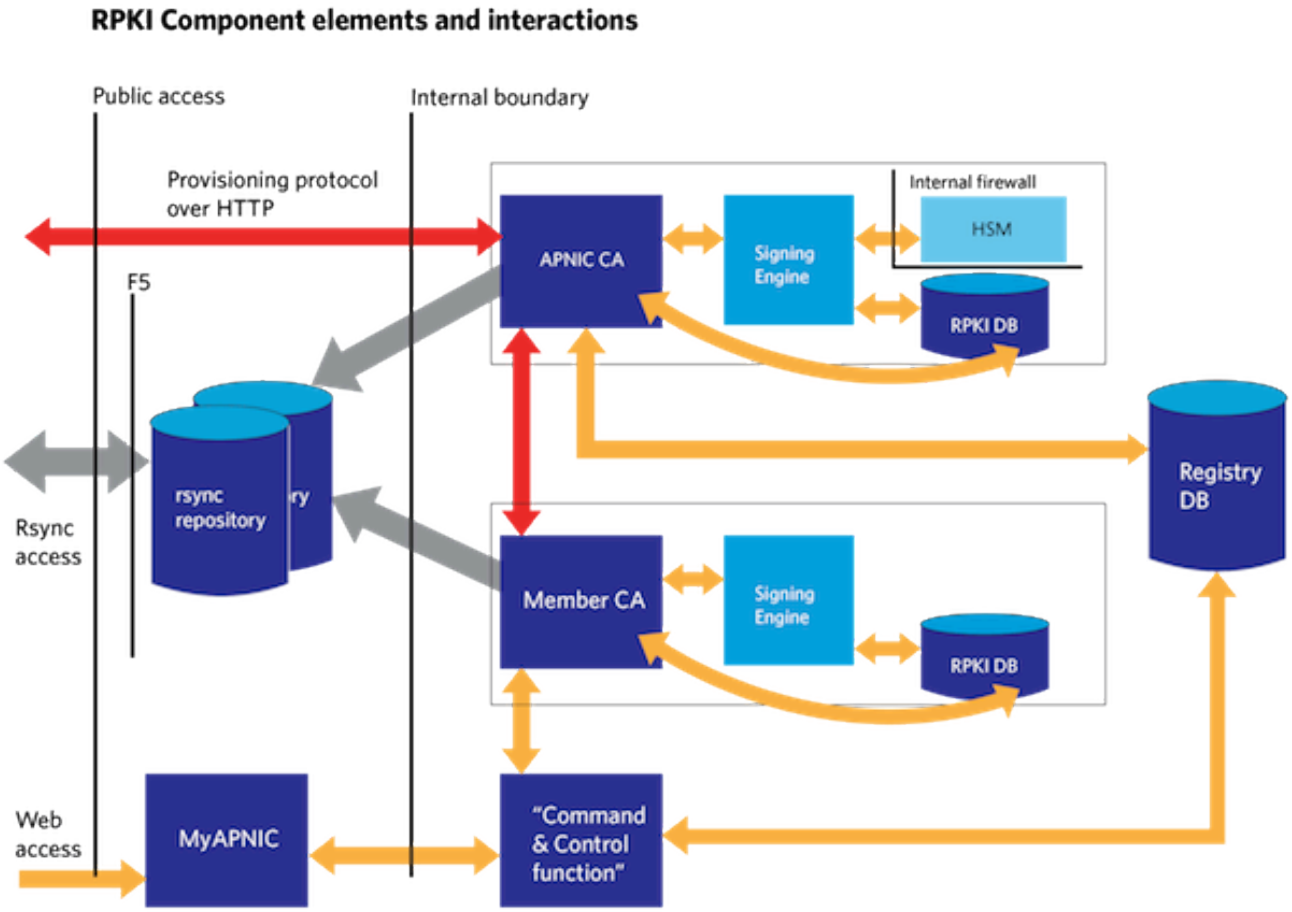
RPKI in the RIRs

- APNIC implemented RPKI Resource Certification

APNIC Resource Certification

- A robust security framework for verifying the association between resource holders and their Internet resources.
- Initiative from APNIC aimed at
  - improving the security of inter-domain routing, and
  - augmenting the information published in the Whois database
- Verifies a holder's current "right-of-use" over an Internet resource

How it Works

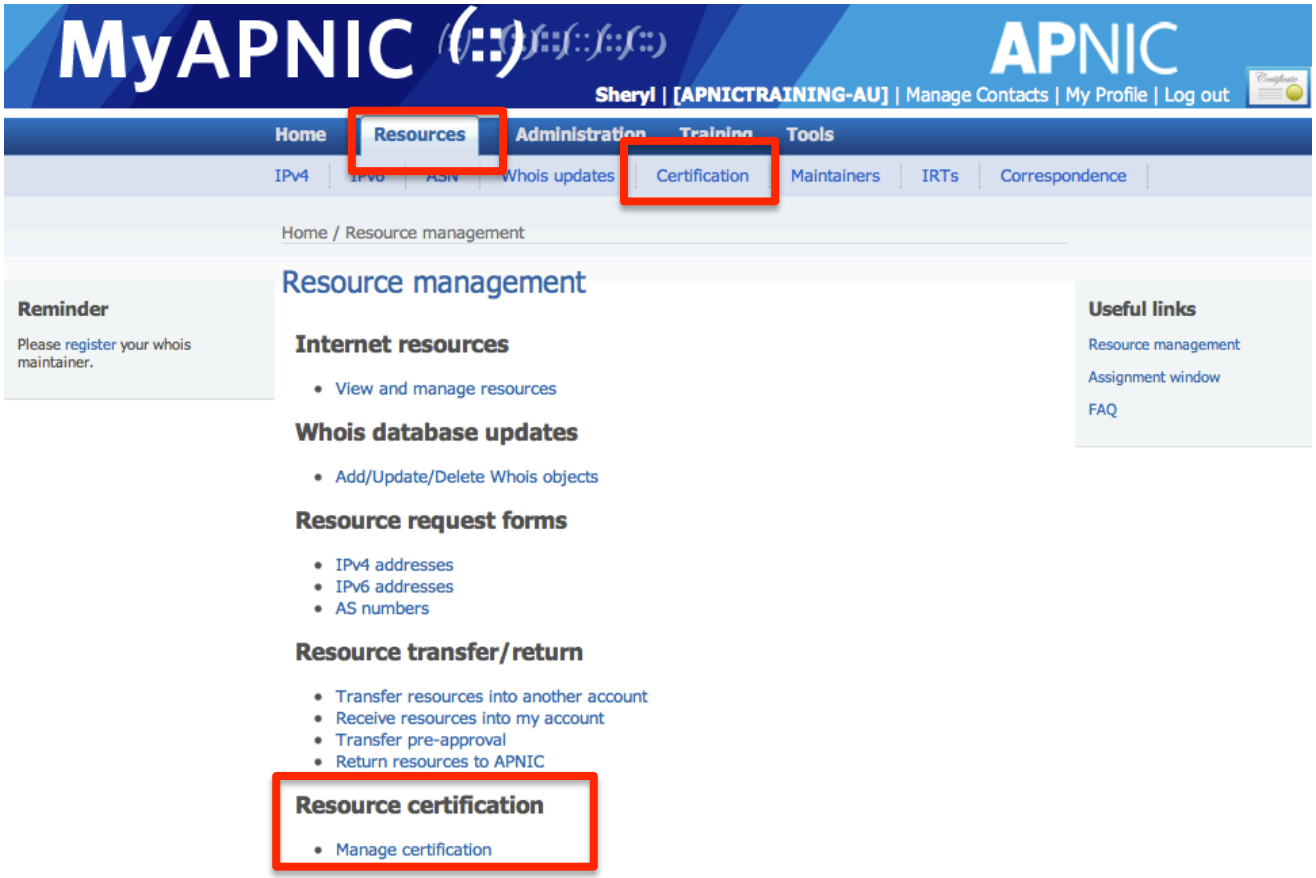

RPKI Component elements and interactions
Public access
Internal boundary
Provisioning protocol over HTTP
Internal firewall
APNIC CA
Signing Engine
HSM
RPKI DB
F5
rsync repository
Rsync access
Registry DB
Member CA
Signing Engine
RPKI DB
Web access
MyAPNIC
"Command & Control function"

Resource Certification (APNIC)

- Verify signed data using the signer's public key
- Verify public key through a chain of interlocking certificates that connect a Trust Anchor to the signer's public key certificate.
  - This is what we refer to as RPKI
- Why it's important:
  - Routing advertisements is now verifiable

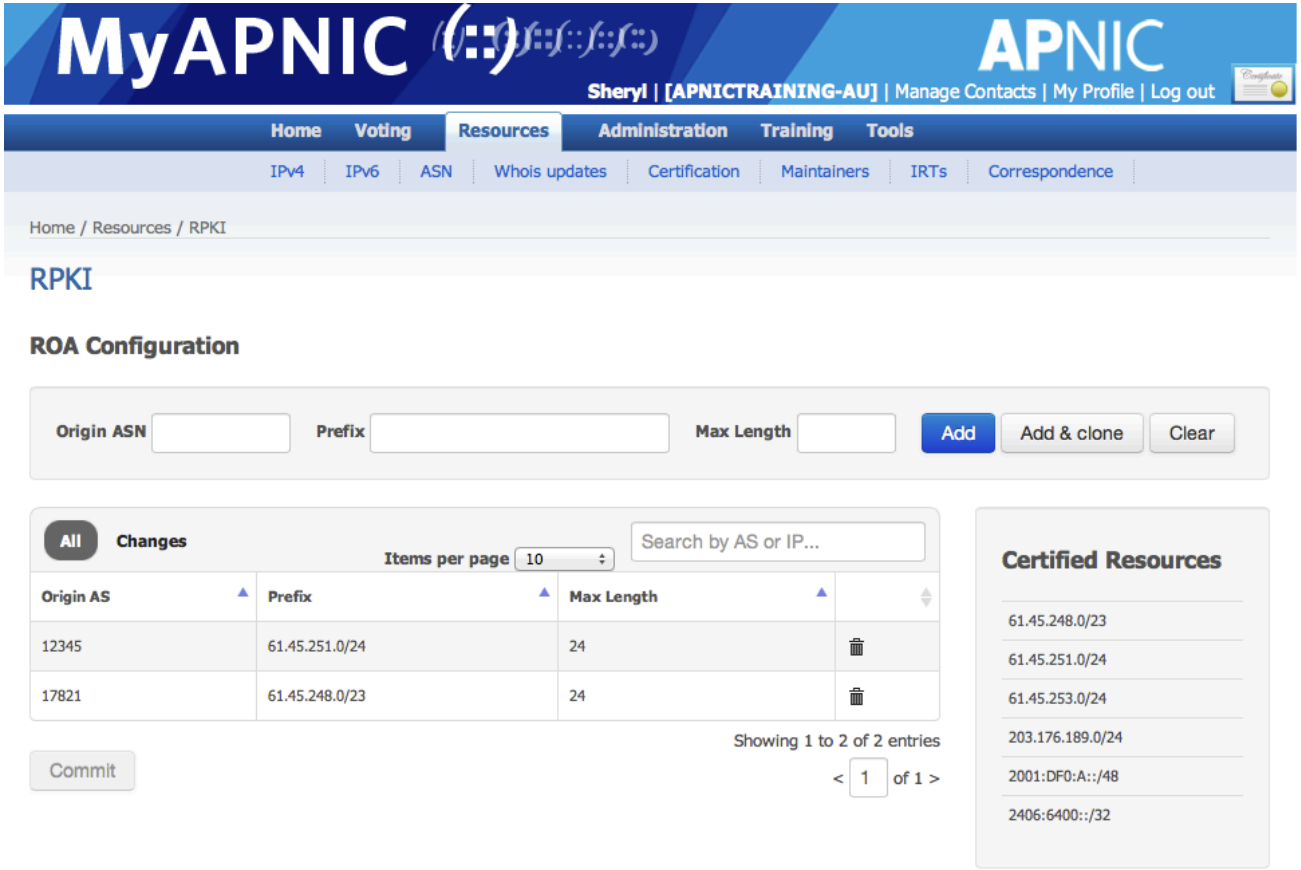
Creating ROA Records

- Login to MyAPNIC, then **Resources** -> **Certification**

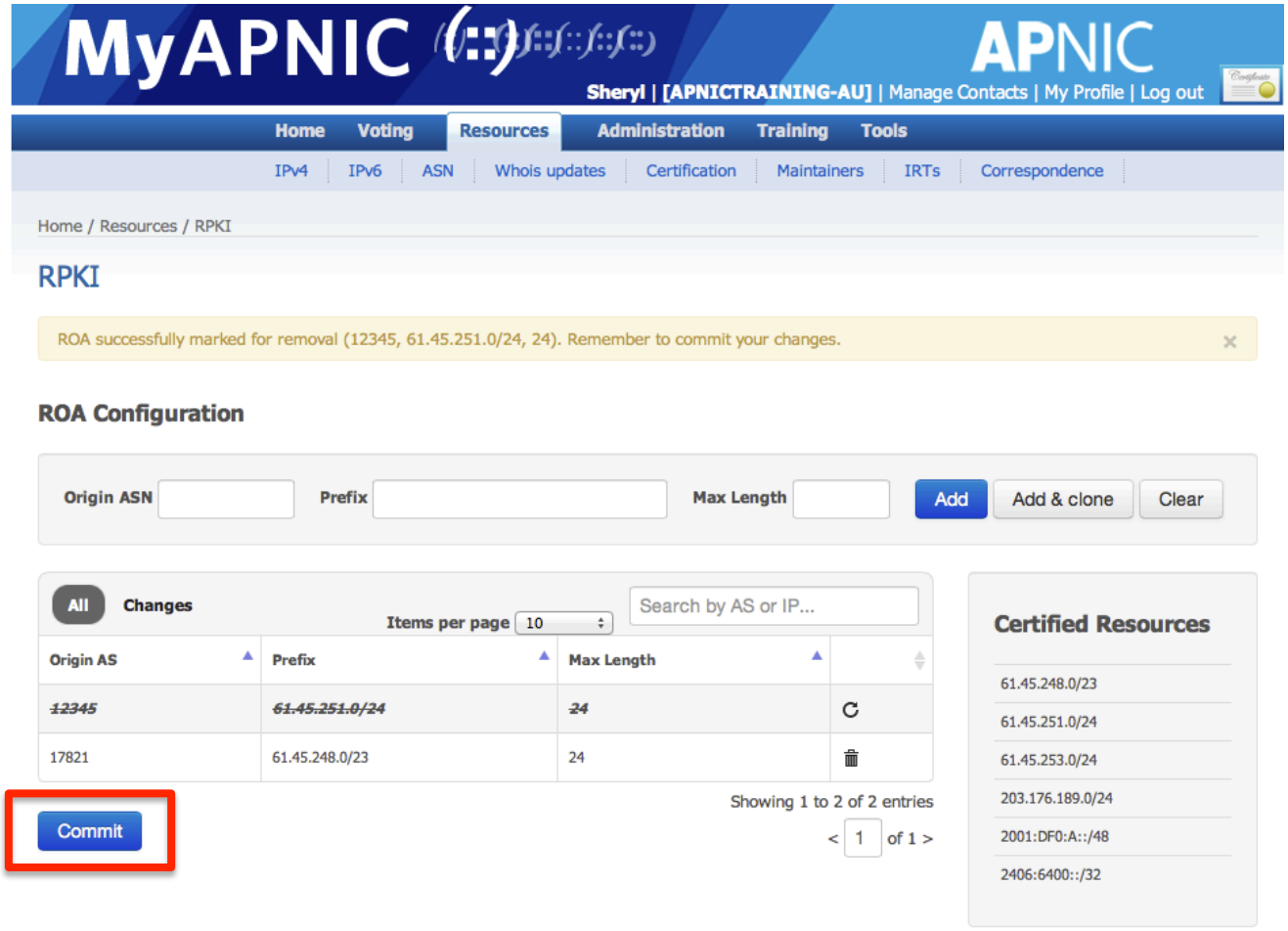


Adding ROA Records

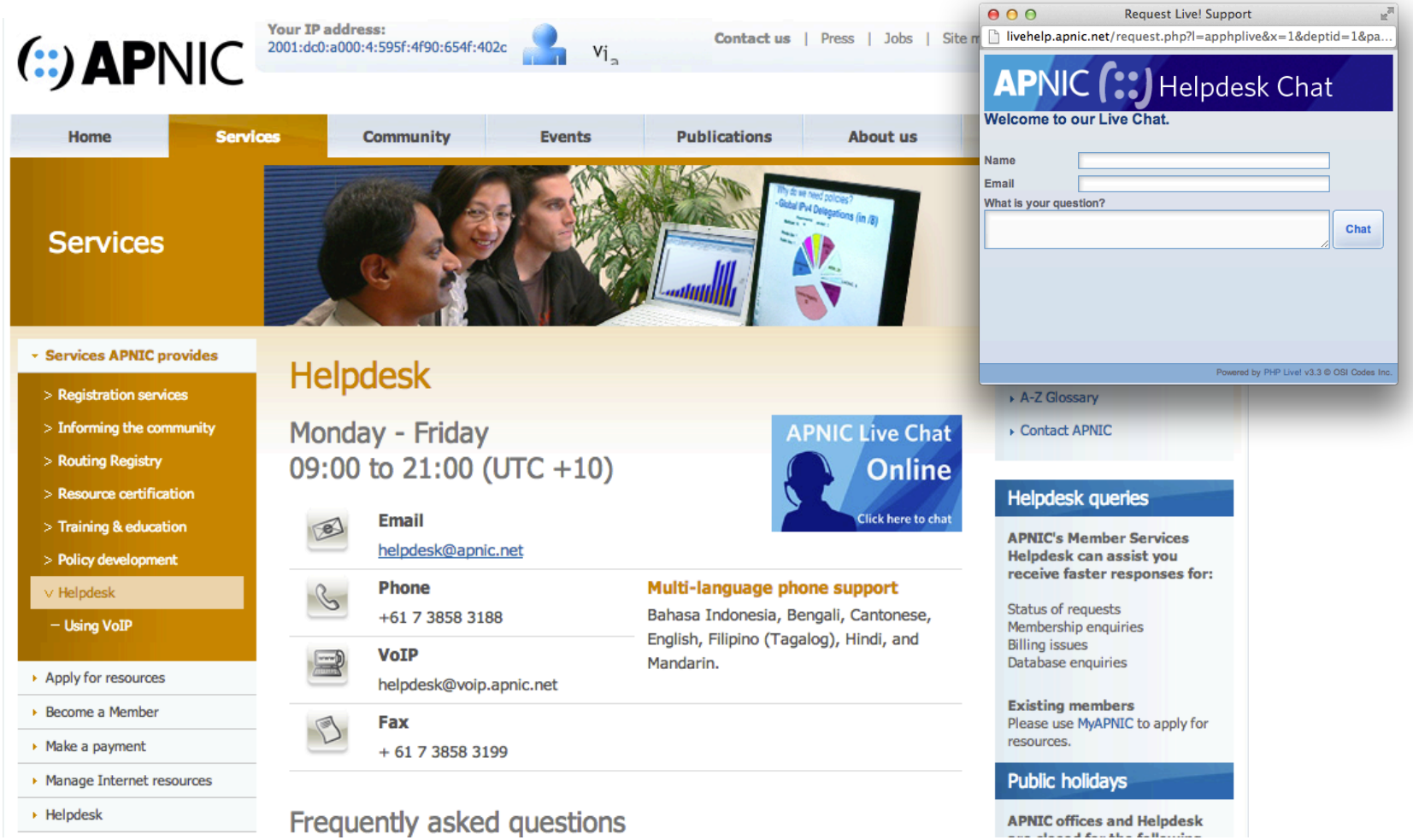
- Simple view and add using the form



Deleting ROA Records



APNIC Helpdesk Chat



Thank You!

End of Session

APNIC