

APNIC **34**
CONFERENCE

PHNOM PENH
CAMBODIA

21 - 31 August 2012

APNIC RPKI Report

George Michaelson

ggm@apnic.net



Current Status

- In service since Jan 2009
- Two level service accessed via myAPNIC
 - APNIC certifies members holdings
 - Members can certify their allocations through hosted service interface

Current APNIC RPKI Service

- Generate CA Certificates covering allocated resources
- Manage resource pools and datasets
- Generate Routing Authority Attestations (ROA)

Current Activity

1. Trust Anchor management
2. ROA management
3. General Signer
4. Public Up-Down Protocol interface

1. Trust Anchor Management

- Split single APNIC TA to multi-component TA
 - Reflect IANA and ERX resource origin
 - Compatible with ongoing work on Global TA
- Disruption to existing deployed service will be minimal due to sparse ERX holdings in APNIC region
- TA transition in place by Q4

2. ROA Management

- User defined MaxLength parameter for ROA
 - Previously fixed-length in UI
 - No back-end changes

3. General Signer

- “Resource Tagged Attestations”
 - Ability to sign files with RPKI digital signatures
 - Useful for Resource Transfers, Customer Provisioning, general attestations about addresses
 - CMS based objects
 - multiple key signing supported
 - Validity dates

General Signer Motivation

- RFC3779 encodes Internet Number Resources as critical extensions into public-key certificates
 - This is a (cryptographically) strong mechanism
- We now have a mechanism to make strong, testable attestations about Internet Number Resources.

Examples

“please can you add a static route for 192.0.200.0/24 to my service,

signed, owner of 192.0.200.0/24”

- ISP can now verify request comes from delegate for the prefix

“Dear broker, as the current holder of 192.0.200.0/24 please list this block as available for transfer,

signed, the soon-to-be ex-owner of 192.0.200.0/24”

- Broker can now validate this listing request



Home / Resources / Certification

Resource Certification

Resource Certificate Download

Download the [current issued certificate](#) covering your owned resource set.

General Signing Tool

Upload a [file](#) for general purpose signing and verification.

Sign Route Origin Authorization

Create a [signed ROA document](#), certifying your authorization for an Autonomous System to originate routes for your resources.

Recent Signed Products

You have no recently signed products

Advanced Management

For [more advanced management](#) of your resource collections, [Route Origin Authorization](#) details and [general purpose signed objects](#). You can also view the [activity log](#).

General Signing Tool

Step 1: Select file to upload or enter text

Content from: Upload file Enter text [Help](#)

File: [Browse...](#) [Help](#)

Step 2: Choose a collection you would like to use to sign the uploaded file

Collection: [Help](#)

- asn
- ipv4
- ipv6

[Manage Collections](#)

Step 3: Set validity period for the digital certificate

Valid from: [Help](#)

Valid to: [Help](#)

Step 4: Sign and receive the package

The package will contain:

- uploaded file
- digital signature
- digital certificate to verify the signature

How do you want to receive the package: Download Email

[Sign Package](#)

General Signing Tool

Step 1: Select file to upload or enter text

Content from: Upload file Enter text [Help](#)

Text: [Help](#)
This is a file containing a brief amount of text that could possibly indicate an offer of availability for various resources under nominal control of the sender.

Step 2: Choose a collection you would like to use to sign the uploaded file

Collection: [Help](#)
asn
ipv4
ipv6
one /24
[Manage Collections](#)

Step 3: Set validity period for the digital certificate

Valid from: [Help](#)
Valid to: [Help](#)

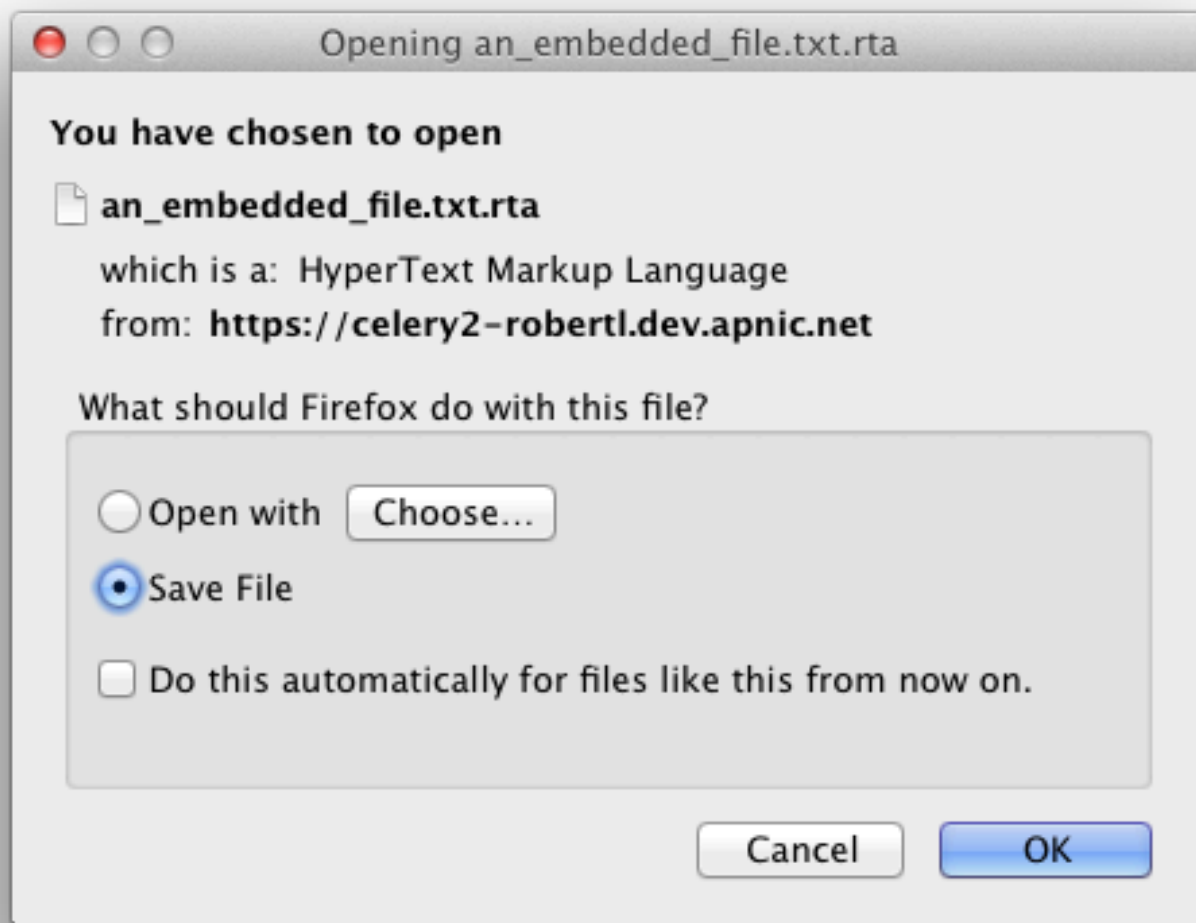
Step 4: Sign and receive the package

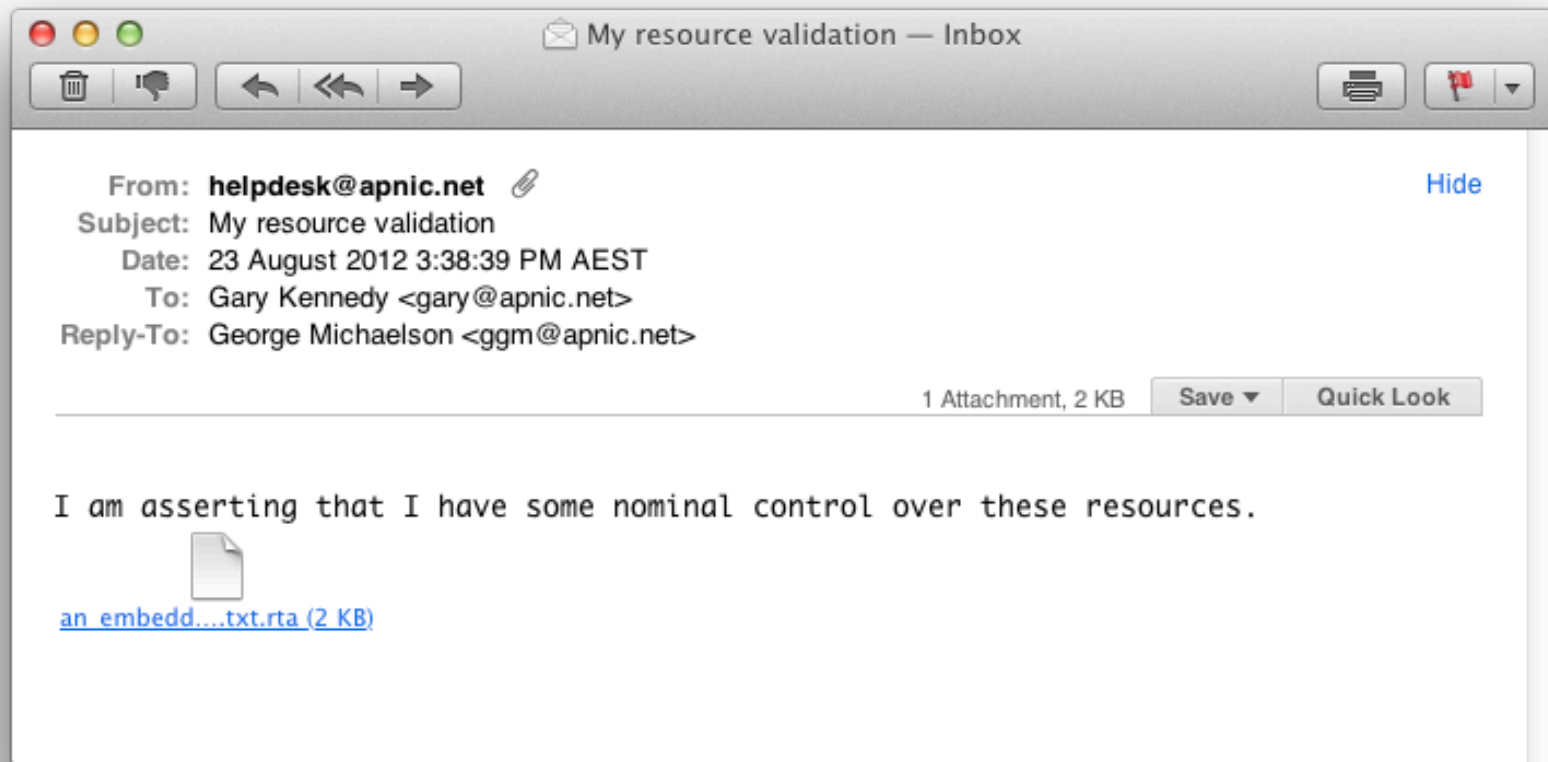
The package will contain:

- uploaded file
- digital signature
- digital certificate to verify the signature

How do you want to receive the package: Download Email

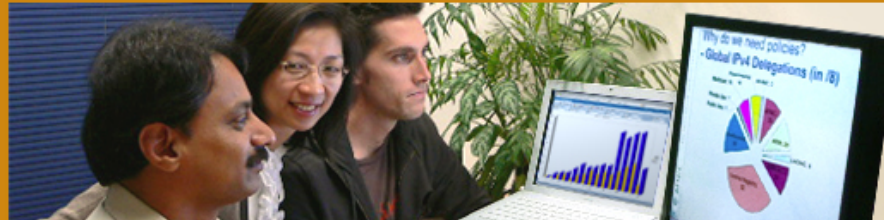
[Sign Package](#)








Services



Print this page 

Services APNIC provides

- > Registration services
- > Informing the community
- > Routing Registry
- ▼ Resource certification
 - RPK Infrastructure
 - Certification Authorities
 - **Signature verification tool**
 - What's new
- > Training & education
- > Policy development
- > Helpdesk

▶ Apply for resources

▶ Become a member

▶ Make a payment

▶ Manage Internet resources

▶ Helpdesk

Signature verification tool

Upload the signed package

File:

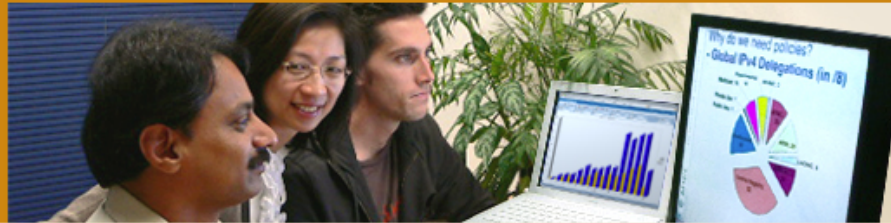
Related links

▶ [Certificates for MyAPNIC](#)

Features & benefits

- Routing information corresponds to properly delegated address resources.
- Resource Certification gives resource holders proof that they hold certain resources.
- Resources holders can attest to those resources when distributing them.
- Allows anyone to make assertions about their right to use an IP address and allows anyone else to validate such a claim in a secure and reliable fashion.
- Resource users can 'sign' information with a digital signature which essentially 'freezes' that information. Therefore, 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

Services



Print this page

Related links

▸ Certificates for MyAPNIC

Features & benefits

- Routing information corresponds to properly delegated address resources.
- Resource Certification gives resource holders proof that they hold certain resources.
- Resources holders can attest to those resources when distributing them.
- Allows anyone to make assertions about their right to use an IP address and allows anyone else to validate such a claim in a secure and reliable fashion.
- Resource users can 'sign' information with a digital signature which essentially 'freezes' that information. Therefore, any effort to alter that information results in the signature being invalidated.
- Only resource holders with a properly delegated 'right of use' can

▼ Services APNIC provides

- > Registration services
 - > Informing the community
 - > Routing Registry
 - ▼ Resource certification
 - RPK Infrastructure
 - Certification Authorities
 - **Signature verification tool**
 - What's new
 - > Training & education
 - > Policy development
 - > Helpdesk
-
- Apply for resources
 - Become a member
 - Make a payment

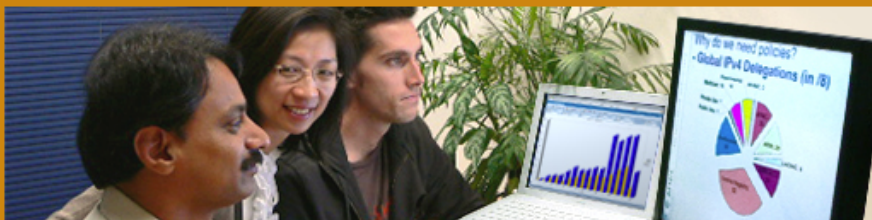
Signature verification tool


Upload the signed package

File:



Services



Print this page 

Related links

▶ Certificates for MyAPNIC

Features & benefits

- Routing information corresponds to properly delegated address resources.
- Resource Certification gives resource holders proof that they hold certain resources.
- Resources holders can attest to those resources when distributing them.
- Allows anyone to make assertions about their right to use an IP address and allows anyone else to validate such a claim in a secure and reliable fashion.
- Resource users can 'sign' information with a digital signature which essentially 'freezes' that information. Therefore, any effort to alter that information results in the signature being invalidated.
- Only resource holders with a

Services APNIC provides

- > Registration services
 - > Informing the community
 - > Routing Registry
 - ▼ Resource certification
 - RPK Infrastructure
 - Certification Authorities
 - **Signature verification tool**
 - What's new
 - > Training & education
 - > Policy development
 - > Helpdesk
-
- ▶ Apply for resources
 - ▶ Become a member
 - ▶ Make a payment

Signature verification tool

Verification Failed

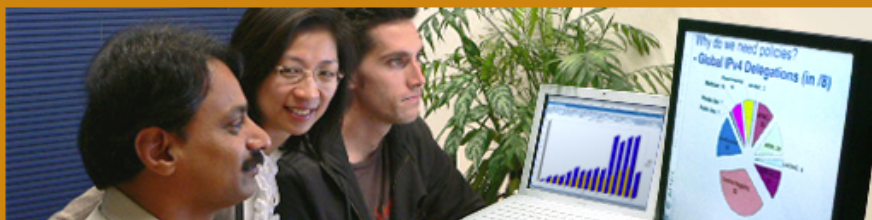
Verification of your signature package failed with the response:


- Not a valid RTA package

Clear & Start Again



Services



Print this page 

Related links

▶ Certificates for MyAPNIC

Features & 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.
- Allows anyone to make assertions about their right to use an IP address and allows anyone else to validate such a claim in a secure and reliable fashion.
- Resource users can 'sign' information with a digital signature which essentially 'freezes' that information. Therefore, 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

Services APNIC provides

- > Registration services
 - > Informing the community
 - > Routing Registry
 - ▼ Resource certification
 - RPK Infrastructure
 - Certification Authorities
 - **Signature verification tool**
 - What's new
 - > Training & education
 - > Policy development
 - > Helpdesk
-
- ▶ Apply for resources
 - ▶ Become a member
 - ▶ Make a payment
 - ▶ Manage Internet resources
 - ▶ Helpdesk

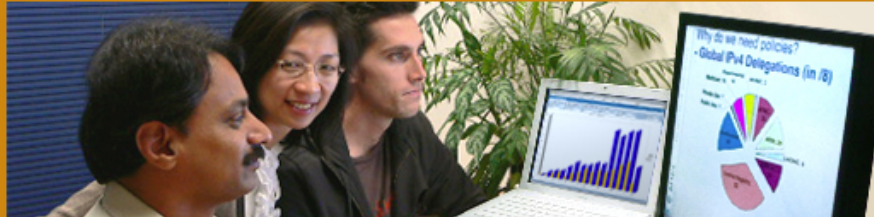
Signature verification tool


Upload the signed package

File:



Services



Print this page 

Services APNIC provides

- > Registration services
- > Informing the community
- > Routing Registry
- ▼ Resource certification
 - RPK Infrastructure
 - Certification Authorities
 - **Signature verification tool**
 - What's new
- > Training & education
- > Policy development
- > Helpdesk
- ▶ Apply for resources
- ▶ Become a member
- ▶ Make a payment

Signature verification tool

Verification Failed

Verification of your signature package failed with the response:

- Signing certificates don't contain resources 7345, 14.64.21.0/24

Clear & Start Again

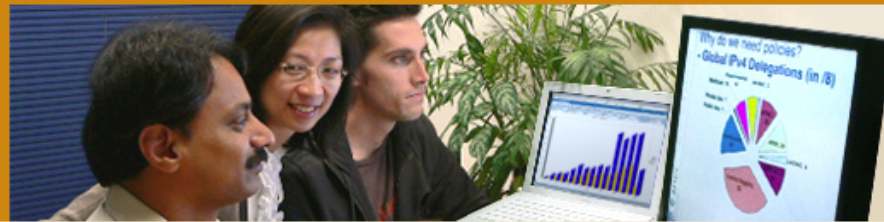
Related links


- ▶ Certificates for MyAPNIC

Features & benefits

- Routing information corresponds to properly delegated address resources.
- Resource Certification gives resource holders proof that they hold certain resources.
- Resources holders can attest to those resources when distributing them.
- Allows anyone to make assertions about their right to use an IP address and allows anyone else to validate such a claim in a secure and reliable fashion.
- Resource users can 'sign' information with a digital signature which essentially 'freezes' that information. Therefore, any effort to alter that information results in the signature being invalidated.
- Only resource holders with a properly delegated 'right of use' can

Services



Print this page 

Related links

▶ Certificates for MyAPNIC

Features & benefits

- Routing information corresponds to properly delegated address resources.
- Resource Certification gives resource holders proof that they hold certain resources.
- Resources holders can attest to those resources when distributing them.
- Allows anyone to make assertions about their right to use an IP address and allows anyone else to validate such a claim in a secure and reliable fashion.
- Resource users can 'sign' information with a digital signature which essentially 'freezes' that information. Therefore, any effort to alter that information results in the signature being invalidated.
- Only resource holders with a

Services APNIC provides

> Registration services

> Informing the community

> Routing Registry

▼ Resource certification

– RPK Infrastructure

– Certification Authorities

– **Signature verification tool**

– What's new

> Training & education

> Policy development

> Helpdesk

▶ Apply for resources

▶ Become a member

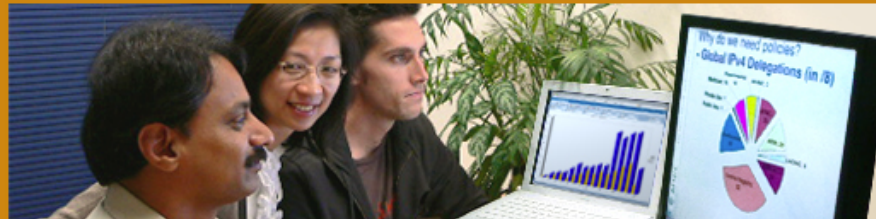
▶ Make a payment

Signature verification tool

Upload the signed package

File:

Services



Print this page

Services APNIC provides

- > Registration services
- > Informing the community
- > Routing Registry
- ▼ Resource certification
 - RPK Infrastructure
 - Certification Authorities
 - **Signature verification tool**
 - What's new
- > Training & education
- > Policy development
- > Helpdesk

- > Apply for resources
- > Become a member
- > Make a payment

Signature verification tool

Verification Successful

The signature in the package has been successfully verified with the certificate having the following resource coverage:

- 70.21.150.0/24
- AS30330

The signature package does not contain any content itself, but rather the hash of another file.

Content hash:

cda1211a928bf2eebed3de1a24d32689b7c95988f967f0f96b7808e6169a3057

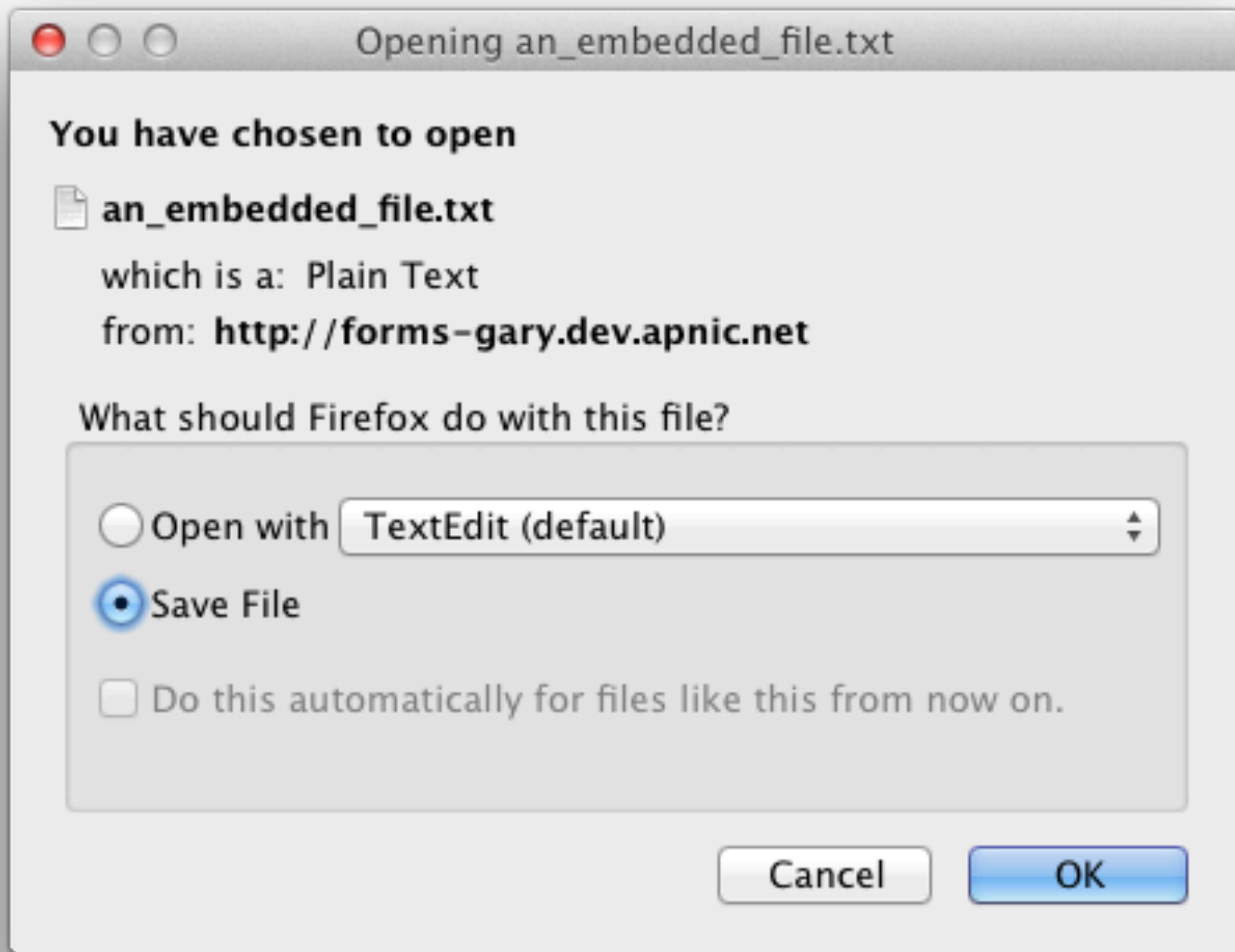
Clear & Start Again

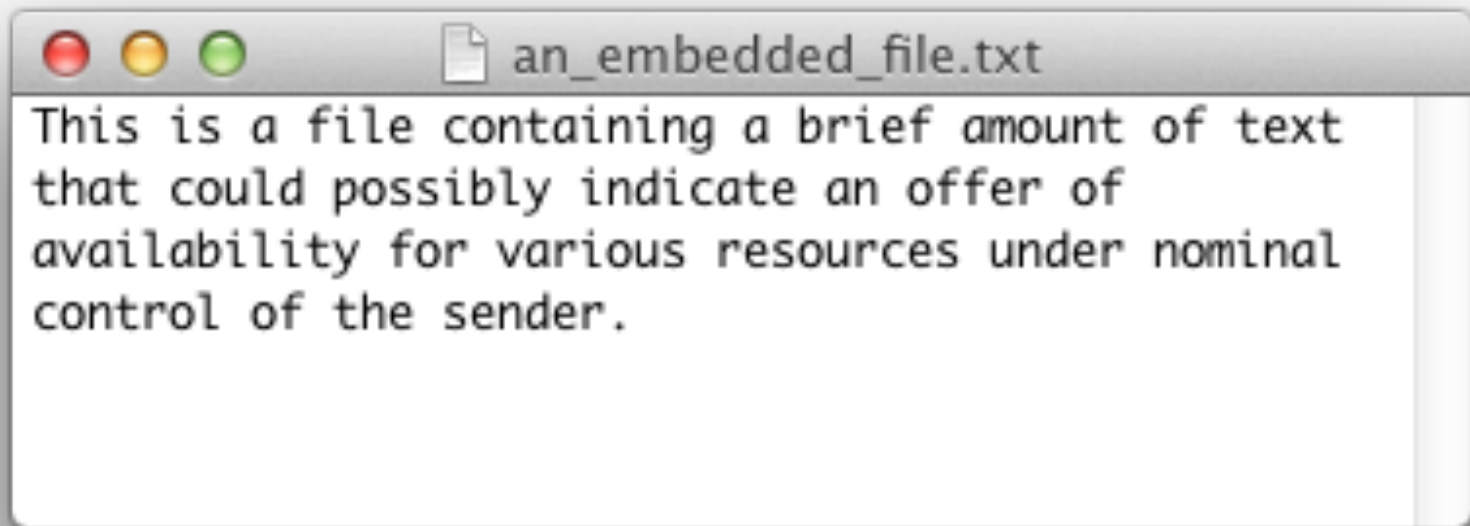
Related links

- > Certificates for MyAPNIC

Features & benefits

- Routing information corresponds to properly delegated address resources.
- Resource Certification gives resource holders proof that they hold certain resources.
- Resources holders can attest to those resources when distributing them.
- Allows anyone to make assertions about their right to use an IP address and allows anyone else to validate such a claim in a secure and reliable fashion.
- Resource users can 'sign' information with a digital signature which essentially 'freezes' that information. Therefore, any effort to alter that information results in the signature being invalidated.
- Only resource holders with a





4. Public Up-Down Protocol interface

- Complements existing myAPNIC hosted services
- Allows for NIR and LIR sub-delegated RPKI services
- Currently designing Up-Down enrollment procedures and credential exchange
- End Q4 deliverable

Interfacing to NIR Resource CA

- RPKI reflects resource allocation hierarchy
 - Support for NIR Resource CA therefore follows allocation hierarchy
- APNIC cannot sign what it doesn't know
 - APNIC RPKI CA signs the state of registry
 - APNIC supplies RPKI services over Up-Down Protocol
- Certification Practice requires APNIC issue RPKI certificates to NIR
 - NIR operates RPKI services reflecting NIR registry state

NIR Operational Model

- NIR operates an RPKI engine instance
- Interface with APNIC via public Up-Down port
- NIR issued RPKI certificates align to NIR resource registry state