# APNIC Resource Certification Service Project

Routing SIG
7 Sep 2005
APNIC20, Hanoi, Vietnam

George Michaelson

# Overview

- Motivation
- Objectives
- RFC3779 summary
- Certificate format
- Project phases
- Deliverables
- Q & A

# Motivation

- Routing security has become critical in the operation of the Internet
  - Vital need for (automatic) AS/route validity checks
- RFC3779 has been created to address this problem
  - Defines extension to the X.509 certificate format for IP addresses & AS number
- The RFC specifies that the certification authority hierarchy should follow the IP address and AS delegation hierarchy
  - Follows IANA -> RIR ->LIR
    - And all their downstream delegations

# Objectives

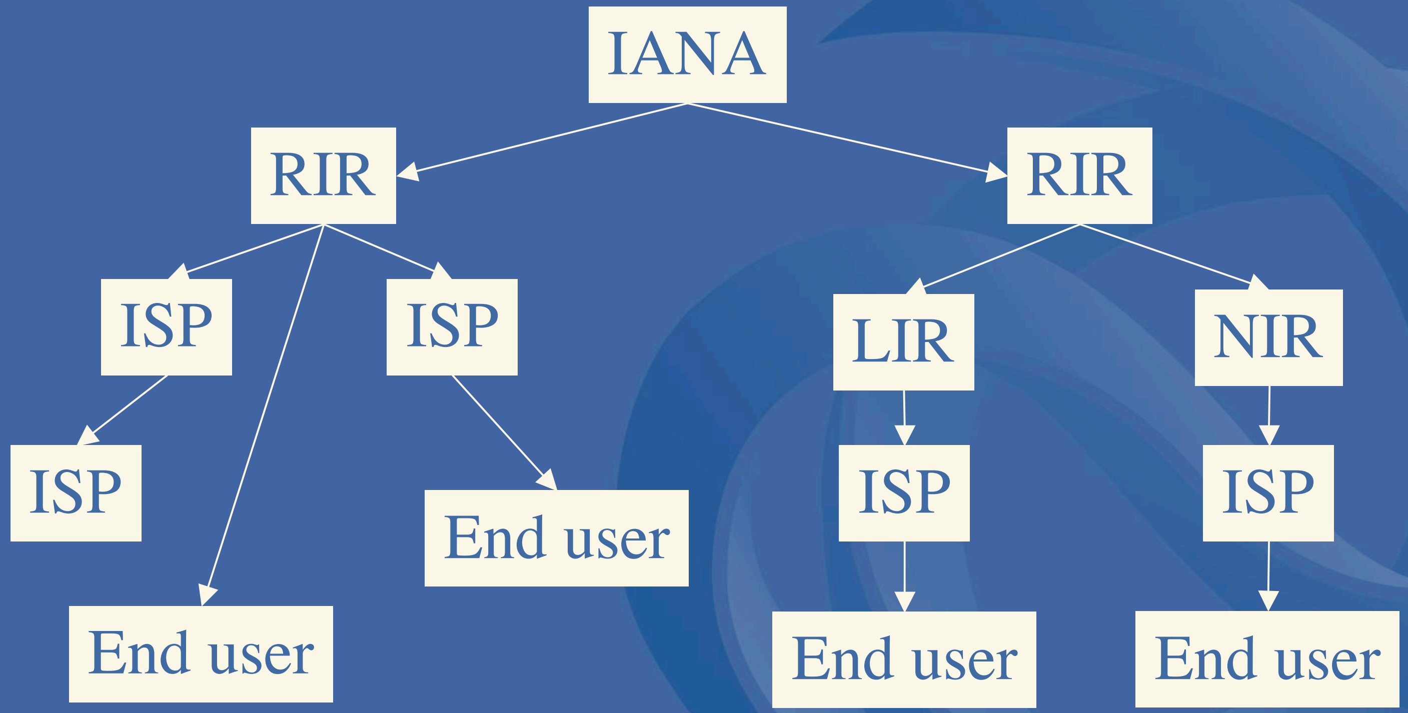
- This project establishes a new APNIC service to provide
  - Issuance of RFC3779 compliant certificates to APNIC members
  - Policy and technical infrastructure necessary to deploy and use the certificates by the routing community and general public
    - CPS (Certification practice statement)
    - Certificate repository
    - CRL (Certificate revocation list)
  - Tools and examples (open source) for downstream certification by NIR, LIR and ISP

# RFC3779 summary

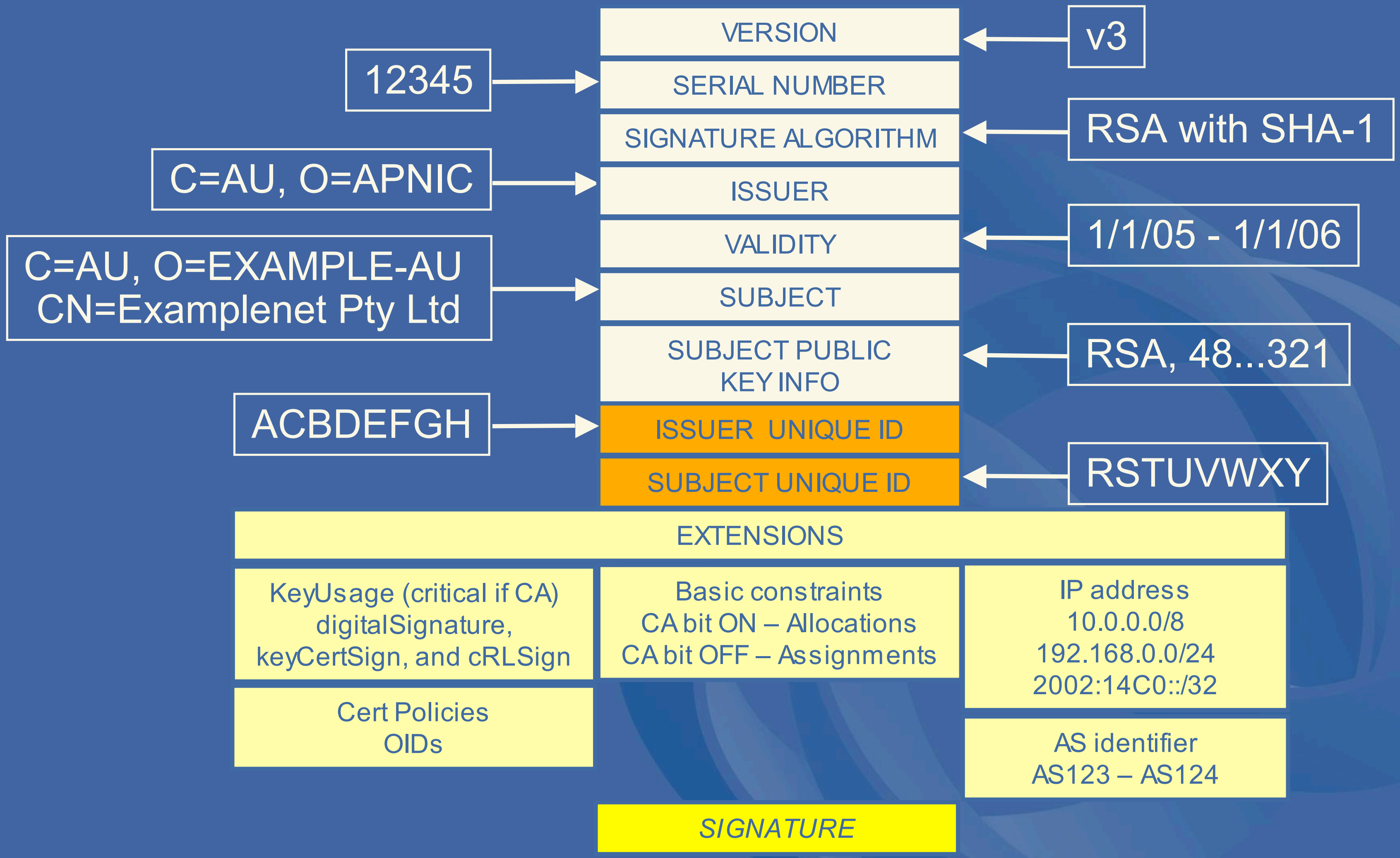
- Abstract
  - This document defines two X.509 v3 certificate extensions
    - The first binds a list of IP address blocks, or prefixes, to the subject of a certificate
    - The second binds a list of autonomous system identifiers to the subject of a certificate
  - These extensions may be used to convey the authorization of the subject to use the IP addresses and autonomous system identifiers contained in the extensions

# RFC3779 summary

- The certificate chain will reflect the delegation hierarchy, from IANA down to the end users



# Certificate format



VERSION ← v3

12345 → SERIAL NUMBER

SIGNATURE ALGORITHM ← RSA with SHA-1

C=AU, O=APNIC → ISSUER

VALIDITY ← 1/1/05 - 1/1/06

C=AU, O=EXAMPLE-AU CN=Examplenet Pty Ltd → SUBJECT

SUBJECT PUBLIC KEY INFO ← RSA, 48...321

ACBDEFGH → ISSUER UNIQUE ID

SUBJECT UNIQUE ID ← RSTUVWXY

EXTENSIONS

KeyUsage (critical if CA)
digitalSignature,
keyCertSign, and cRLSign

Basic constraints
CA bit ON – Allocations
CA bit OFF – Assignments

IP address
10.0.0.0/8
192.168.0.0/24
2002:14C0::/32

Cert Policies
OIDs

AS identifier
AS123 – AS124

*SIGNATURE*

# Project phases

- Trial – 4Q 2005
  - Early adopters, s/w developers, router designers
  - Major requirement changes allowed
    - Certificate formats may change
- Pilot – 1Q 2006
  - Input from trial used to test service
  - Wider deployment
  - Minor requirement changes allowed
    - Certificate format should be stable
- Full service – 2Q 2006
  - General service availability
  - Full policy and procedures in place

# Deliverables

- Phase 1 – trial
  - RFC3779 compliant certificates issued to selected members
  - Tools and utilities (open source)
    - Requesting certificates
    - Issuing downstream certificates
    - Certificate validation tools
      - Both online and offline
  - Experiences/Outcomes to be presented at next AMM in Routing SIG
  - May lead to policy proposals

# Q & A

- FAQ
  - Router community participation?
    - Discussed with Cisco, Juniper, actively seeking participation of other BGP coders in tests
  - Certificate lifetimes?
    - Have to be tied to membership/relationship. Considering options for longer lifetimes subject to suitable agreements
  - APNIC certify LIR sub-delegations?
    - NO. Only warrant relationship with LIR, existance of resource allocation to that LIR from APNIC

# Questions?

Thank you!