

Applications for Resource Certificates

r1.12 – 18 Jan 2008 – 11:45 – [DanielFKarrenberg](#)

Authors: Robert Kisteleki, Daniel Karrenberg

Introduction

The RIPE NCC is currently considering to deploy a system that would issue digital certificates along with the assignment or allocation of Internet number resources. These "resource certificates" will certify that the holder of the certificate has indeed been assigned or allocated the particular resource. Local IRs will be able to issue sub-certificates as they assign parts of the allocations they receive to users. Other RIRs have similar plans to deploy resource certification.

This series of white papers describes a number of the benefits and potential applications for resource certificates. The white papers are intended to help the community understand the costs, benefits and other impacts of resource certification.

About resource certification – A very quick overview

Resource certification mirrors the way in which Internet number resources are distributed. That is, resources are initially handed out by IANA to RIRs, which do further allocations to LIRs (or NIRs), who in turn do the same for their customers. Currently allocations and assignments are recorded at the registry that makes them and in the RIPE database. When we talk about resource certification, this existing process is augmented by a parallel one: the user of a resource can also receive a digital certificate describing the allocation or assignment. These digital certificates are based on public key infrastructure (PKI) principles.

A certificate obtained by a party in the system contains:

- the identification of the issuing Internet Registry (RIR, LIR)
- the identification of the holder of the certificate, or in PKI terms the subject
- the resources that were allocated/assigned by the issuer to the subject (might be just a partial list)
- other data needed for validation

Note that the identifications of both issuer and holder within the certificate are not necessarily human readable or interpretable; resource certificates are not about certifying the identity of either the issuer or the holder.

In general resource certificates enable participating parties to:

- present the certificate to someone as a proof of being entitled to use a particular resource
- sign any kind of data related to the resources described in the resource certificate. In particular:
 - when delegating a subset of the resources used, it can be used to sign certificates about such a delegation
 - when making use of a resource (ie. with routing) sign authorization documents
 - creating special kinds of signatures needed to support the validation and publication of such certificates (like certification revocation lists, publication manifests, etc.)

The current model of resource certificate issuance / revocation assumes the creation of an automated, hierarchical system that requests, issues and revokes such certificates whenever a change happens in the back-end delegation databases of the Internet registries. In this system each participating IR owns/controls a node that is able to:

- communicate with:
 - "upstreams": other IRs that hand out resources to this IR
 - "downstreams": other IRs that receive resources from this IR
 - the IR's resource allocation database
- issue/revoke certificates on demand (certification authority (CA) function)

White Paper Series

In order to make the case for the usefulness of Number Resource Certification and to expose the changes in LIR business processes it would bring about we will describe a number of applications. The form will be a short 2–3 page white paper for each potential application that will describe the motivation for the application, the principle of operation, the LIR business process implications, a description of the costs to the LIR and a summary.

This is very a very rough first brain dump. It will be expanded and spread out into several pages once more meat is there. Currently Robert and Daniel are adding meat.

- [Provisioning of resources](#)
- [Routing tools](#)
- [Resource transfers](#)
- [Failing / disappeared LIR](#) (to be drafted)

Revision: r1.12 – 18 Jan 2008 – 11:45 – [DanielFKarrenberg](#)

[Science](#) > CertWhitePapers