IPv4 Address Trading Using Resource Certificate

Cheol-Soon Park*, Jae-Cheol Ryou** and Yong-Tae Park***

Abstract—The Internet has been growing at unprecedented rates. The problem of an address shortage could act as a barrier on this growth. In principle, a new Internet standard, IPv6 solves the problem of the address shortage because it has a very large address space. But IPv6 is not yet compatible with the IPv4 and during the IPv4-to-IPv6 transition period IPv4 address will continue to be in demand. Thus for quite some time, the problem of IP address shortage will persist. To solve the problem, we propose the mechanism of secure IP address trading. This mechanism is based on the Resource PKI (RPKI). The RPKI is the working item of IETF. This proposed mechanism maximizes the trust of IP address trading using RPKI.

Keywords—IP Address Trading, Resource PKI, Routing Security, IP Address Management

1. INTRODUCTION

The Internet has been growing at unprecedented rates. According to a prediction by the Organization for Economic Cooperation and Development (OECD), it is reported that more than 85% of the available addresses on the Internet have been allocated and the remaining will run out by 2011 [1].

The problem of an address shortage could act as a barrier to the growth of the Internet [1]. Especially Internet business in Africa, Asia and Latin America are just beginning to fulfill their potential level of Internet development [1].

In principle, a new Internet standard, IPv6 solves the problem of address shortage because it has a very large address space (2128 addresses). But IPv6 is not yet compatible with the IPv4 and during the IPv4-to-IPv6 transition period IPv4 addresses will continue to be in demand [1]. Thus for quite some time, the problem of IP address shortage will persist.

Another method to solve this IP address shortage problem is IPv4 address transactions. Address holders who no longer need their IPv4 address could sell or lend their address to someone who wants an IPv4 address. One important benefit of such a transaction is that it provides incentives for existing holders of addresses to release unused address resources. And it might rationalize and make an underground economy in address resources more than transparent [1].

If an IPv4 address transfer market comes to exist, then it is important to consider the method

Manuscript received February 26, 2010; accepted March 4, 2010.
Corresponding Author: Jae-Cheol Ryou
* Korea Communications Commission (KCC), Seoul, Korea (poempark@kcc.go.kr)
** Dept. of Computer Science & Engineering, Chungnam National University, Seoul, Korea (jcryou@home.cnu.ac.kr)
He was supported by the MKE(Ministry of Knowledge Economy), Korea, under the ITRC(Information Technology Research Center) support program supervised by the NIPA(National IT Industry Promotion Agency), (NIPA-2010-(C1090-1031-0005)).
*** Dept. of Industrial Engineering, Seoul National University, Seoul, Korea (parkyt@cybernet.snu.ac.kr)

of IPv4 address protection. If there is no security and confidence concerning the market, few people would feel compelled to participate in the deals. To guarantee secure transactions of IPv4 addresses, we must consider the following:

- Is the seller who wants to sell IP addresses authorized? That is, does the seller have a valid IP address and authorization of the address?
- Am I the only buyer? That is, did the seller sell the same IP address to someone else?
- After the transaction, what is the mechanism that provides the proof of the buyer's purchase?

To answer these questions and provide confidence in the IP address trade market, a security mechanism for the IPv4 address trade process is needed.

Aside from the exhaustion of IP addresses, the security of the IP address resources is still a problem in the routing protocol. Regarding Internet security, we cannot trust information provided by the WHOIS and IRR (Internet Routing Registries). In current Internet (Inter-domain) routing protocol, there are no mechanisms that provide authorization of the holder of IP address resources [4].

One of the candidates for providing confidence in IP address resources is validation based on PKI (Public Key Infrastructure). The PKI is suited to manage IP address resources because the hierarchy of PKI is very similar to the architecture of Internet address resources management.

In this paper, we propose a mechanism of secure IP address trading. This mechanism is based on the Resource PKI (RPKI). RPKI is the working item of IETF sidr (secure inter-domain routing) WG. The rest of the paper is organized as follows: In section 2, we describe IETF resource PKI. And in section 3, we propose an IP address trade mechanism based on RPKI, and in section 4, we evaluate the security of our mechanism. We form our conclusions in section 5.

2. RELATED WORK

2.1 RPKI Overview

Because the holder of a block IP address space is entitled to define the topological destination of the IP datagram whose destinations fall within that block, decisions about inter-domain routing are inherently based on knowledge of the allocation of the IP address space. In current practice, the allocation of IP addresses is hierarchic. The root of the hierarchy is IANA (Internet Assigned Number Authority). Below IANA there are 5 Regional Internet Registries (RIRs), each of which manages an address and AS number allocation within a defined geopolitical region. In some regions, the third tier of the hierarchy includes National Internet Registries (NIRs) as well as Local Internet Registries (LIRs). The term LIR is used in some regions to refer to what other regions define as an ISP [2].

The architecture of IP address management is similar to the hierarchy of Internet PKI. Because of this similarity, IP address allocations can be described naturally by a hierarchic PKI as in Fig. 1. In current IETF sidr WG is working to standardize resource PKI.

The main idea of RPKI is to guarantee authorization to an IP address holder using a signed object. This signed object, called ROA (Route Organization Authorization) includes an IP address block and AS (Autonomous System) number with the digital signature of an IP address holder. The IP address holder's assertion of the IP address is endorsed by the ROA. The ROA is

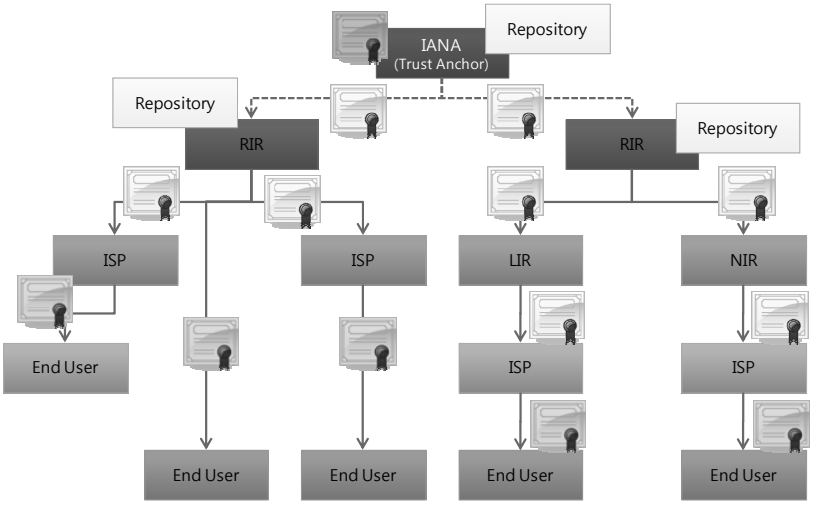

Fig. 1. The architecture of RPKI

then perhaps, validated by the certificate issued by the CA, i.e. the Internet registries.

2.2 Component of resource PKI

2.2.1 ROA

The ROA (Route Organization Authorization) is used to prove authorization of IP address spaces by its holders. Explained further, the organization that digitally signs the ROA asserts its authority of IP address spaces, and this assertion is validated by a certificate that pairs with the private key used to sign the ROA.

If the concerned party for the ROA is successfully validated, that party considers that issuer of the ROA as having the authority to use the specific IP address. The success of validation means the signature attached to the ROA can be verified by the relating certificate, and that the certificate is neither expired nor revoked. The success of ROA validation also entails the following:

- The holder of IP address (ISP, etc.) that claims ROA has authority of ROA
- IP address space in ROA is valid. It means Internet Registries allocate IP address space in ROA to the holder of ROA
- The holder of IP address has authority of IP address in ROA
- The holder of IP address has authority of BGP message that claim AS (Autonomous System) in ROA as the origination of IP address space

Usually the ROA is distributed by the repository system. Repository systems have ROAs, certificates and CRLs (Certificate Revocation Lists). The information which must be included in an ROA is as follows:

- AS Number
- IP address prefixes

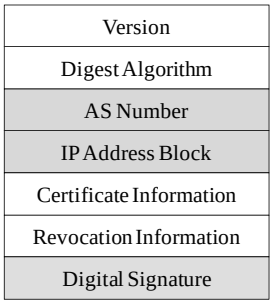

Fig. 2. ROA structure

Fig. 2 describes the structure of an ROA. The 'version' field and 'Digest Algorithm' field denotes both the version of ROA and message digest algorithm used in an ROA. The signature generated by an IP address holder, i.e. the end entity, is attached to the ROA. When an ROA is valid, the corresponding EE certificate is valid; furthermore, the AS number and IP address block in the ROA are identical to the AS number and IP address block in the EE certificate. Therefore, the validation period of the ROA is identical to the validation period of the EE certificate. The 'Certification Information' and 'Revocation Information' usually point to the repository system.

Because each ROA is associated with a single end-entity certificate, the set of IP blocks contained in an ROA must be drawn from an allocation by a single source, i.e., an ROA cannot combine allocations from multiple sources. Address space holders who have allocations from multiple sources, and who wish to authorize an AS to originate routes for these allocations, must issue multiple ROAs to the AS.

2.2.2 CA Certificate

Any resource holder who is authorized to sub-allocate these resources must be able to issue resource certificates to correspond to these sub-allocations [2]. In other words, in resource PKI, Internet registries, for example, APNIC (Asia Pacific Network Information Center), ARIN (American Registry for Internet Numbers), etc) naturally play as CA (Certification Authority)s. To issue ROAs, the holder of an IP address may need CA certificates to be used to validate the signature attached to ROAs

In a typical Internet PKI, the subject name field in a certificate is descriptive. But in a resource PKI the subject name field isn't descriptive. That is, in an Internet PKI, generally the holder of the certificate decides the subject name with specific rules, but in a resource PKI the certificate issuer decides the subject name. This decision is generally part of automatic processing. For example, when the holder of a certificate is APNIC, the subject name field is composed as follows:

- Country: AU
- Organization: Asia Pacific Network Information Center
- Common Name: APNIC Resource Certification Authority

In Internet PKI, the subject name is to identify the holder of the certificate. But in RPK, the

certificate isn't used to identify the holder of the certificate. In order to minimize legal issues and errors when using a non-descriptive subject name field the holder of a resource certificate tries to use the resource certificate for identification purposes. Because Internet Registries issue CA certificates to the organizations that already have a relationship, DB key or ID may be used with a subject name.

RPKI CA certificates include the following fields:

- Serial number: unique serial number per CA
- Signature: signature identifier
- Subject Public Key: public key value
- Subject Key Identifier
- Authority Key Identifier
- CRLDP: CRL (Certificate Revocation List) Distribution Point
- Authority Information Access
- Subject Information Access
- Certificate Policies
- IP Resources
- AS Resources

2.2.3 EE (End Entity) Certificate

The private key that is bound to the public key in an EE certificate isn't used to sign to the other certificates. The main object of an EE certificate is the validation of a signed object related to IP address resources in the ROAs or certificates.

Characteristic of resource PKIs is the one-to-one mapping between EE certificates and signed objects e.g. ROAs. So the private key is used to sign only one object. In other words, each signed object is generated from only one private key. Because of this RPKI feature, there is no need for a certificate revocation mechanism. If the EE certificate is expired, the ROA bound to the expired certificate is automatically regarded as invalid.

This one-to-one correspondence ensures that the private key corresponding to the public key in a certificate is used exactly once in its lifetime, and thus can be destroyed after it has been used to sign its one object. This fact should simplify key management, since there is no requirement to protect these private keys for an extended period of time [2].

Although we describe only two uses for end-entity certificates, additional uses will likely be defined in the future. For example, end-entity certificates could be used as a more general authorization for their subjects to act on behalf of the specified resource holder. This could facilitate authentication of inter-ISP interactions, or authentication of interactions with the repository system. These additional uses for end-entity certificates may require retention of the corresponding private keys, even though this is not required for the private keys associated with end-entity certificates keys used for verification of ROAs and manifests, as described above [2].

2.2.4 Trust Anchors

In any PKI, each relying party (RP) chooses its own set of trust anchors or root CA. This general property of PKIs applies here as well. There is an extant IP address space and AS number allocation hierarchy, and thus IANA and/or the five RIRs are obvious candidates to be default

TAs here.

For example, an RP (e.g., an LIR/ISP) could create a trust anchor to which all address space and/or all AS numbers are assigned, and for which the RP knows the corresponding private key. The RP could then issue certificates under this trust anchor to whatever entities in the PKI it wishes.

It is expected that some parties within the extant IP address space and AS number allocation hierarchy may wish to publish trust anchor material for possible use by relying parties. A standard profile for the publication of trust anchor material for this public key infrastructure can be found in [3].

2.2.5 Repositories

Initially, an LIR/ISP will make use of the resource PKI by acquiring and validating every ROA, to create a table of the prefixes for which each AS is authorized to originate routes. To validate all ROAs, an LIR/ISP needs to acquire all the certificates and CRLs. The primary function of the distributed repository system described here is to store these signed objects and to make them available for download by LIRs/ISPs.

The repository system is the central clearing-house for all signed objects that must be globally accessible to relying parties. When certificates and CRLs are created, they are uploaded to this repository, and then downloaded for use by relying parties (primarily LIRs/ISPs). ROAs and manifests are additional examples of such objects, but other types of signed objects may be added to this architecture in the future. This document briefly describes the way signed objects (certificates, CRLs, ROAs and manifests) are managed in the repository system. As other types of signed objects are added to the repository system, it will be necessary to modify the description, but it is anticipated that most of the design principles will still apply. Although there is a single repository system that is accessed by relying parties, it is comprised of multiple databases. These databases will be distributed among registries (RIRs, NIRs, and LIRs/ISPs).

Repository operators will choose one or more access protocols that relying parties can use to access the repository system. These protocols will be used by numerous participants in the infrastructure (e.g., all registries, ISPs, and multi-homed subscribers) to maintain their respective portions of it. In order to support these activities, certain basic functionality is required of the suite of access protocols, as described below. No single access protocol needs to implement all of these functions (although this may be the case), but each function must be implemented by at least one access protocol.

- Download: Access protocols must support the bulk download of repository contents and subsequent download of changes to the downloaded contents, since this will be the most common way in which relying parties interact with the repository system. Other types of download interactions (e.g., download of a single object) may also be supported.
- Upload/change/delete: Access protocols must also support mechanisms for the issuers of certificates, CRLs, and other signed objects to add them to the repository, and to remove them. Mechanisms for modifying objects in the repository may also be provided. All access protocols that allow modification to the repository (through addition, deletion, or modification of its contents) must support verification of the authorization of the entity performing the modification, so that appropriate access controls can be applied

Current efforts to implement a repository system use RSYNC as the single access protocol. RSYNC, as used in this implementation, provides all of the above functionality. A document specifying the conventions for use of RSYNC in the PKI will be prepared.

3. IPv4 Address Trading Using Resource Certificates

3.1 Scenario

Fig. 3 describes scenario of IP address trading. We consider an on-line trade, but payment method is out of scope.

(1) Seller of IP address requests that the CA issue an EE certificate
(2) CA validates seller's identity
(3) CA issues an EE certificate for seller
(4) Seller sells IP address(es) to the buyer, i.e., seller provides ROA including selling IP address and Resource certificate.
(5) Buyer validates IP addresses using ROA and seller's certificate. After validation the buyer pays.
(6) Payment is processed and a receipt is provided
(7) Buyer requests that the CA issue an EE certificate for buyer's new IP addresses.
(8) CA validate buyer's identity
(9) Finally, CA issues an EE certificate for the buyer

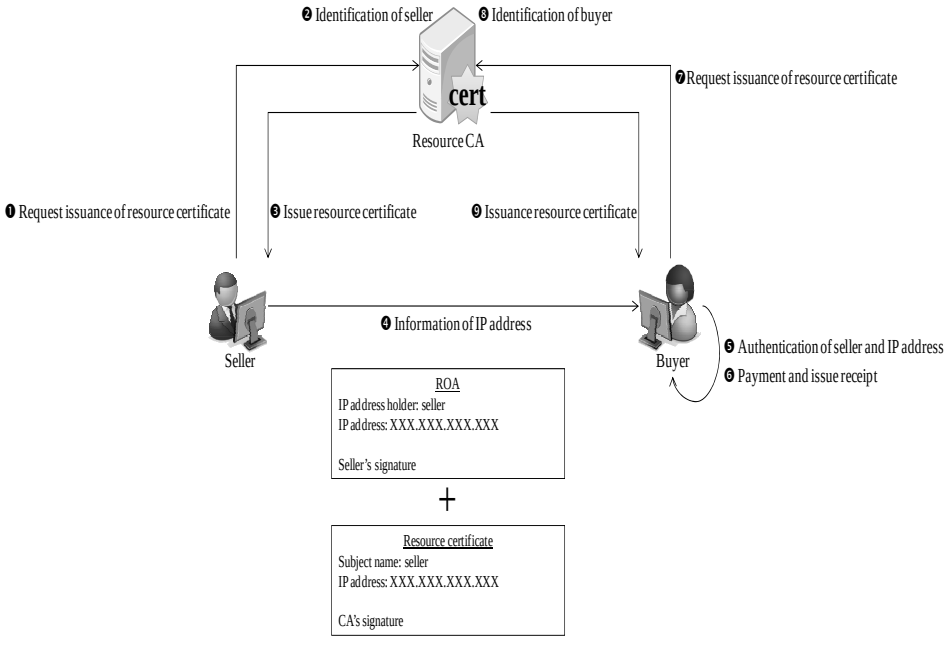

Fig. 3. IP address trading scenario

3.2 Operations

3.2.1 Trading Steps

Steps 1, 2, and 3 are typical certificate issuing steps. But the resource CA doesn't validate the seller's identification. The seller might be assigned IP address blocks and an AS number from the resource CA, but the resource CA simply confirms if the seller is his client or not.

In step 4, the transaction is practically processed. The seller provides his IP address to the buyer and the IP address includes an ROA. Also, the EE certificate and CA certificate(s) are provided together. The ROA and certificates are evidence that prove the seller is authorized to hold an IP address in ROA.

In step 5, the buyer validates the authority of the seller. Explaining this process in further detail, the buyer verifies the signature attached to the ROA, and whether the IP address in ROA is identical to that of the EE certificate. The buyer also verifies the signature attached to the EE certificate, and confirms the expiration date of the EE certificate. Then the buyer verifies precedence certificates of the EE certificate and CRL. After all of this verification, the buyer can consider the holder of the IP address and the IP address itself as valid and trustworthy.

After verification of the IP address, the buyer would pay and the seller would provide a receipt. After step 6, actual trading is complete.

Steps 7, 8 and 9 are the processes through which the buyer registers his new IP address to the Internet Registry. Crucially in step 7, the buyer provides the evidence that proves trading is complete. This evidence includes the received ROA and receipts. Therefore, receipts MUST be protected by a cryptographic method.

3.2.2 ROA management

If a holder of an IP address sells his IP address, he MUST request to be issued an end-entity certificate containing that prefix in an IP Address Delegation extension. He then uses the corresponding private key to sign an ROA containing the designated prefix and the AS number for the AS. The resource holder may include more than one prefix in the EE certificate and corresponding ROA if desired. As a prerequisite, then, any address space holder that issues ROAs for a prefix must have a resource certificate for an allocation containing that prefix. The standard procedure for issuing an ROA is as follows:

(1) Create an end-entity certificate containing the prefix(es) to be authorized in the ROA.
(2) Construct the payload of the ROA, including the prefixes in the end-entity certificate and the AS number to be authorized.
(3) Sign the ROA using the private key corresponding to the end-entity certificate (the ROA is comprised of the payload encapsulated in a CMS signed message [3]).
(4) Upload the end-entity certificate and the ROA to the repository system.

The standard procedure for revoking an ROA is to revoke the corresponding end-entity certificate by creating an appropriate CRL and uploading it to the repository system. The revoked ROA and end-entity certificate should then be removed from the repository system. Care must be taken when revoking ROAs in that revoking an ROA may cause a relying party to treat routing advertisements corresponding to the prefixes and origin AS number in the ROA as unauthorized (and potentially even change routing behavior to no longer forward packets based on those

advertisements). In particular, resource holders should adhere to the principle of "make before break" as follows: Before revoking an ROA corresponding to a prefix which the resource holder wishes to be routable on the Internet, it is very important for the resource holder to ensure that there exists another valid alternative ROA that lists the same prefix (possibly indicating a different AS number). Additionally, the resource holder should ensure that the AS indicated in the valid alternative ROA is actually originating routing advertisements to the prefixes in question. Furthermore, a relying party must fetch new ROAs from the repository system before taking any routing action in response to an ROA revocation.

3.2.3 Certificate issuance

There are several operational scenarios that require certificates to be issued. Any allocation that may be sub-allocated requires a CA certificate, so that the certificates can be issued as necessary for the sub-allocations. Holders of provider-independent IP address space allocations also must have certificates, so that an ROA can be issued to each ISP that is authorized to originate a route to the allocation (since the allocation does not come from any ISP).

In the long run, a resource holder will not request resource certificates, but rather receive a certificate as a side effect of the allocation process for the resource. However, initial deployment of the RPKI will entail issuance of certificates to existing resource holders as an explicit event. Note that in all cases, the authority issuing a CA certificate will be the entity who allocates resources to the subject. This differs from most PKIs in which a subject can request a certificate from any certification authority.

If a resource holder receives multiple allocations over time, it may accrue a collection of resource certificates to attest to them. This is accomplished by consolidating the IP Address Delegation and AS Identifier Delegation Extensions into a single extension (of each type) in a new certificate. However, if the certificates for these allocations contain different validity intervals, creating a certificate that combines them might create problems, and thus is not recommended.

If a resource holder's allocations come from different sources, they will be signed by different CAs, and cannot be combined. When a set of resources is no longer allocated to a resource holder, any certificates attesting to such an allocation must be revoked. A resource holder should not use the same public key in multiple CA certificates that are issued by the same or differing authorities. Note that since the subject's distinguished name is chosen by the issuer, a subject who receives allocations from two sources generally will receive certificates with different subject names.

4. IMPLEMENTATION AND EVALUATIONS

4.1 Implementation

4.1.2 System Architecture

Fig. 4 describes the overall architecture. End Entity is the system that wants to assert its IP addresses and AS numbers. End Entity includes an ROA generation module. The Resource PKI CA system issues a resource certificate for the end entity. Resource PKI CA system receives an EE certificate issuance request from the End Entity and validates the request. ROA generated by End Entity and the certificate issued by the resource PKI CA system are uploaded to and stored in the repository system. The Relying party then downloads the ROA and resource certificate

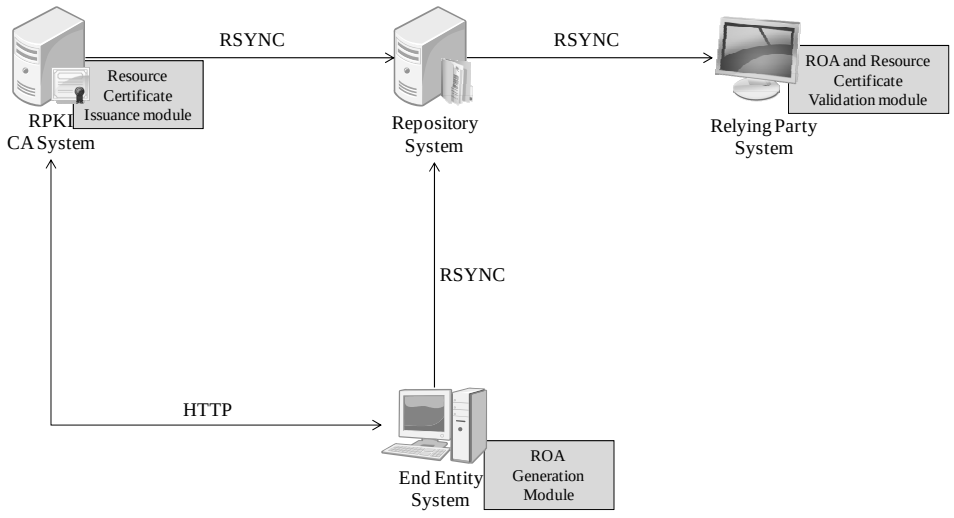

Fig. 4. System architecture

Table 1. Implementation Environments

Components	Implementation Environments
Resource CA System	-OS: Linux (Fedora) -Language: C/C++ -Library: openssl 1.0.0
Repository System	-OS: Linux (Fedora) -Language: C/C++ -Library: openssl 1.0.0 -DB: mysql
End Entity	-OS: Linux (Fedora) -Language: C/C++ -Library: rsync, openssl 1.0.0
Relying Party	-OS Linux (Fedora) -Language: C/C++ -Library: openssl 1.0.0

from the repository system and validates them. The relying party system includes an ROA and certificate validation module.

All communications from/to the repository system are implemented on the RSYNC protocol. And the end entity – resource PKI CA system uses HTTP. The Implementation environments are described in Table 1.

4.1.3 System Operations

This implementation is operated as follows:

(1) Seller generates public key pair. Also using generated public key pair, seller generates CSR (Certificate Signing Request).
(2) Seller uploads CSR, that is, requests EE certificate issuance (Fig. 5).

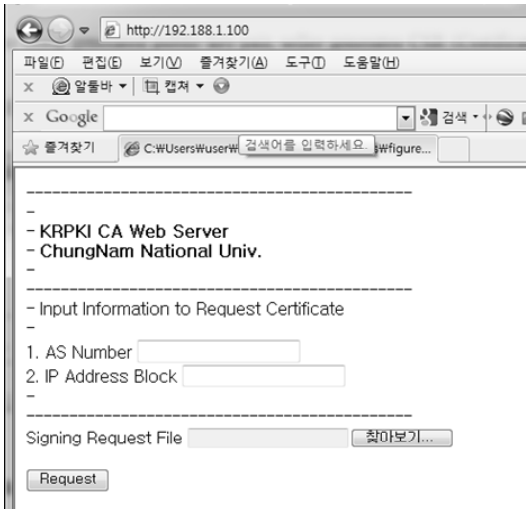

Fig. 5. Request of EE certificate issuance

(3) Resource CA system validates CSR and issues an EE certificate. Fig. 6 shows that the EE certificate includes an AS number and an IP address space.
(4) CA system uploads the issued EE certificate to the repository and notifies the seller.
(5) On receiving notification, seller generates ROA.
(6) Seller uploads issued ROA to repository.
(7) Buyer downloads ROA and related certificates from repository.

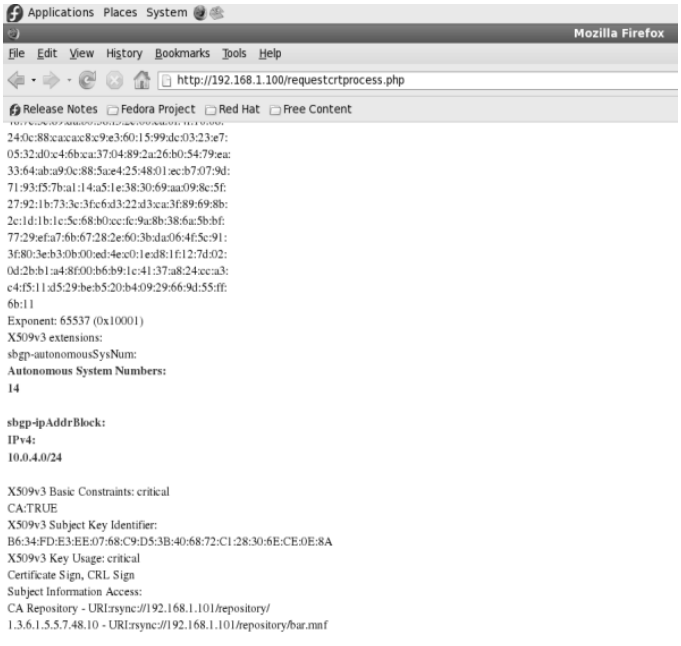

Fig. 6. Generated EE certificate

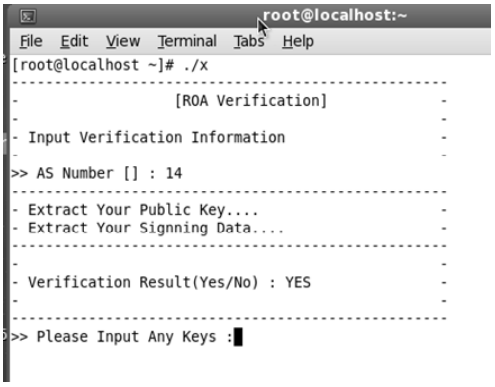

Fig. 7. ROA validation

(8) Buyer validates ROA and related certificates and validates the ownership of IP address resources. Fig. 7 describes success of ROA validation.

4.2 Evaluation of our model

Previously we provided 3 questions that are needed to guarantee the secure transaction of IP address trading. Now we describe how our trading model answers those questions.

(1) Is the seller who wants to sell the IP address(es) authorized?

To answer this question, our model can provide evidence that the seller has a valid IP address and has authorization of that address. The ROA issued by the seller is the signed object that includes IP addresses and AP numbers. The EE certificate issued by the CA is used to validate ROA. So if the buyer is successful and satisfied with the validation of the seller's ROA and related certificates, the buyer can authorize the IP address(es) including the ROA.

(2) Am I the only buyer?

If the buyer is convinced the seller hasn't sold the same IP address(es) to another, the buyer can then proceed with confidence that he/she is only buyer for the IP address(es) he/she bought. During the certificates issuing process, the CA verify that the IP address(es) in the ROA is under their management. In resource PKI, Internet Registry used to be the CA so the CA usually issues certificates to their customers who own IP address(es) managed by the CA.

(3) After the transaction, what is the mechanism that provides the proof of the buyer's purchase?

After the transaction, the buyer requests certificate issuance for his/her new IP address from the CA, and then issues the ROA. When the CA issues the new certificate and the buyer issues the ROA, the transaction is complete.

5. CONCLUSIONS

In this paper, we proposed a mechanism of secure IP address trading. This mechanism is

based on the Resource PKI. RPKI is the working item of IETF.

If the IPv4 address transfer market comes into existence, then it is important to consider the method of IPv4 address protection. If there is no security and confidence in the market, few people would want to participate in the transactions. Therefore, to guarantee secure transactions of IPv4 addresses, we must consider confidence in trading. Our proposed mechanisms maximize confidence in IP address trading using RPKI. Our mechanism also solves all of the questions related to security of IP address trading; e.g., 'Is the seller who wants to sell IP addresses authorized?', 'Am I the only buyer?', 'After the transaction, what is the mechanism that provides the proof of the buyer's purchase?' Using our mechanism, secure IP address trading is possible. Therefore, we conclude that this secure IP address trading can contribute to solving the problem of address shortages in the future.

REFERENCE

[1] Milton Muller, "Scarcity in IP addresses: IPv4 Address Transfer Markets and the Regional Internet Address Registries," Internet Governance Project, 20 Jul., 2008.

[2] M. Lepinski, S. Kent, "An Infrastructure to Support Secure Internet Routing (draft-ieth-sidr-arch-09.txt)," IETF sidr WG draft, 2009. 10.

[3] Michaelson, G., Kent, S., and Huston, G., "A Profile for Trust Anchor Material for the Resource Certificate PKI," draft-ietf-sidr-ta-02, September, 2009.

[4] S. Murphy, "RFC:4272 BGP Security Vulnerabilities Analysis," IETF, 2006. 1.

[5] S.M. Bellovin, "Security Problems in the TCP/IP Protocol Suite," Computer Communication Review, Vol.10, No.2, 1989. 4.

[6] Nordstrom, C. Dovrolis, "Beware of BGP Attacks," ACM SIGCOMM Computer Communications Review, Vol.34, No.2., 2004. 4.

[7] Hawkinson, J., Bates, T., "RFC1930: Guidelines for creation, selection, and registration of an autonomous syste (AS)," IETF, 1996.

[8] Stewart, J., "BGP4: Inter-Domain Routing in the Internet," Addison-Wesley, 1999.

[9] Z. Zhang, Y. Zhang, C. Hu, Z. M. Mao, "Practical Defenses Against BGP Prefix Hijacking," Proceeding of ACM CoNEXT, 2007. 12.

[10] D. Wendlandt, I. Avramopoulos, D. Andersenm J. Rexford, "Don't Secure Routing Protocols, Secure Data Delivery," Proceeding of ACM HotNets, 2006. 11.

[11] S. Kent, C. Lynn, K. Seo, "Secure Border Gateway Protocol (Secure-BGP)," IEEE Journal on Selected Areas in Communications (JSAC), Vol.18, No.4, 2000. 4.

Cheol-Soon Park

He is a director of Korea Communications Commission. He graduated from Seoul National University (SNU) with two bachelor's degrees (History, International Relations) and a master's degree (Public Policy). He is also a doctoral candidate in Technology and Management at SNU. Furthermore, he obtained one more bachelor's degree (Media Arts and Science) and two more master's degrees (Technology Management, European Policy) from other universities. His research interests are information security, technology innovation, and communications policy.

Jae-Cheol Ryou

He is a professor in the Division of Electrical and Computer Engineering at Chungnam National University in Korea. He is also the director of the Internet Intrusion Response Technology Research Center (IIRTRC), Chungnam National University, Korea. He received a B.S. degree in Industrial Engineering from Hanyang University in 1985, an M.S. degree in Computer Science from Iowa State University in 1988, and a Ph.D. degree in Electrical Engineering and Computer Science from Northwestern University in 1990. His research interests are Internet Security and Electronic Payment Systems including Wireless Internet Security.

Yong-Tae Park

He is a professor in the Department of Industrial Engineering at Seoul National University (SNU) in Korea. He holds a B.S. in Industrial Engineering from SNU and an M.S. and Ph.D. in Operations Management from the University of Wisconsin-Madison. He won the Technology Innovation Management (TIM) Research Award in 2009. His research interests lie in areas of innovation management, industrial knowledge networks, information economics and security, etc.