Network Working Group
Internet-Draft
Expires: August 28, 2008

C. Popoviciu
R. Droms
E. Levy-Abegnoli
Cisco Systems
February 25, 2008

# DHCPv6 Delegation of Certificates Option
<draft-popoviciu-dhc-certificate-opt-01.txt>

## Status of this Memo

By submitting this Internet-Draft, each author represents that any applicable patent or other IPR claims of which he or she is aware have been or will be disclosed, and any of which he or she becomes aware will be disclosed, in accordance with Section 6 of BCP 79.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF), its areas, and its working groups. Note that other groups may also distribute working documents as Internet-Drafts.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

The list of current Internet-Drafts can be accessed at http://www.ietf.org/ietf/1id-abstracts.txt.

The list of Internet-Draft Shadow Directories can be accessed at http://www.ietf.org/shadow.html.

This Internet-Draft will expire on August 28, 2008.

## Copyright Notice

Copyright (C) The IETF Trust (2008).

## Abstract

The Certificate options for DHCP-PD RFC3633 [4] provide a mechanism to deliver, along with the IPv6 prefix, the certificate or the information needed to obtain a certificate entitling the client router to advertise the prefix delegated to it. This information is neccesary if Secure Neighbor Discovery RFC3971 [6] is used by the devices connected to the DHCP-PD client router.

Table of Contents

## 1. Introduction

The Prefix Delegation capabilities of Dynamic Host Configuration Protocol (DHCP) offer a convenient mechanism to dynamically provision a router and enable it to, in turn, provision the devices connected to it. In the context of Secure Neighbor Discovery however, a router must posses a digital certificate provided by a Certificate Authority for the prefixes it advertises through Router Advertisements. In this scenario, a receiving router needs to acquire the certificate for the prefixes received via DHCP-PD.

This document describes new options for DHCP which enable or facilitate the dynamic acquisition and management of certificates by DHCP-PD clients for the prefixes delegated to them. In one use case example, these options will be used by a Customer Premises Equipment(CPE) router acting as the gateway between a subscriber's network and the service provider network. The protocol extensions proposed in this document can be leveraged in any environment where dynamicaly provisioned routers must support SEND.

The mechanisms described in this document leverage DHCP which operates under the authentication and security considerations described in the DHCPv6 specification RFC3315 [3] and the DHCP-PD specification RFC3633. In the context of SEND deployments however, these considerations might not be sufficient and additional functionality might be neccesary to ensure that certficates are provided to the right router. In deployments, DHCP leverages various mechanisms (DHCP snooping, anti-spoofing tools) to secure its operation. These mechanisms should be taken into consideration as well when analysing the security requirements of deploying the enhancements proposed by this document.

## 2. Definitions and Terminology

For a complete specification of the options defined, this document should be read in conjunction with the DHCPv6 (RFC3315) and DHCP-PD (RFC3633) specifications. Definitions for terms and acronyms not explicitly detailed in this document can be found in RFC3315.

This document uses the terminology defined in RFC2460 [2], RFC3315 and RFC3971.

This document also relies on the terminology and concepts defined in RFC3779 [5] and RFC4211 [8], as well as the framework defined in RFC4210 [7].

## 3. Requirements

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in BCP 14, RFC 2119 [1]. RFC 2119 defines the use of these key words to help make the intent of standards track documents as clear as possible. While this document uses these keywords, this document is not a standards track document.

## 4. Model and Applicability

The environment in which the certificate DHCP options can be used is similar to the typical DHCP-PD deployment environment and is shown in Figure 1. A DHCP Delegating Server (DS) which can be located on the aggregation device, in which case we have a Delegating Router (DR), or somewhere in the network, provides a prefix to the Requesting Router (RR). The requesting router subnets the prefix into /64 prefixes which it assigns to its own, subscriber facing interfaces. It then advertises the /64 prefixes through RAs to enable hosts to autoprovisioning themselves.

If the subscriber hosts are implementing SEND (RFC3971 and RFC3872), the RR will have to use CryptoGraphic Addresses (CGA) to peer with them. These addresses will be derived from an RSA key pair public/ private. Before accepting the /64 prefix advertised by the RR, the hosts will require a certificate from the RR, for the advertised prefix. The RR will have to acquire a certificate corresponding to its public key, including the prefix delegated to it, using X.509 extensions for IP addresses (RFC3779) A Certificate Authority (CA) will provide the certificate which the RR can use to confirm that it is allowed to advertise the /64 subnets over its subscriber facing interface via router advertisements.

Figure 1 illustrates a deployment scenario which benefits form the certificate options of DHCP.

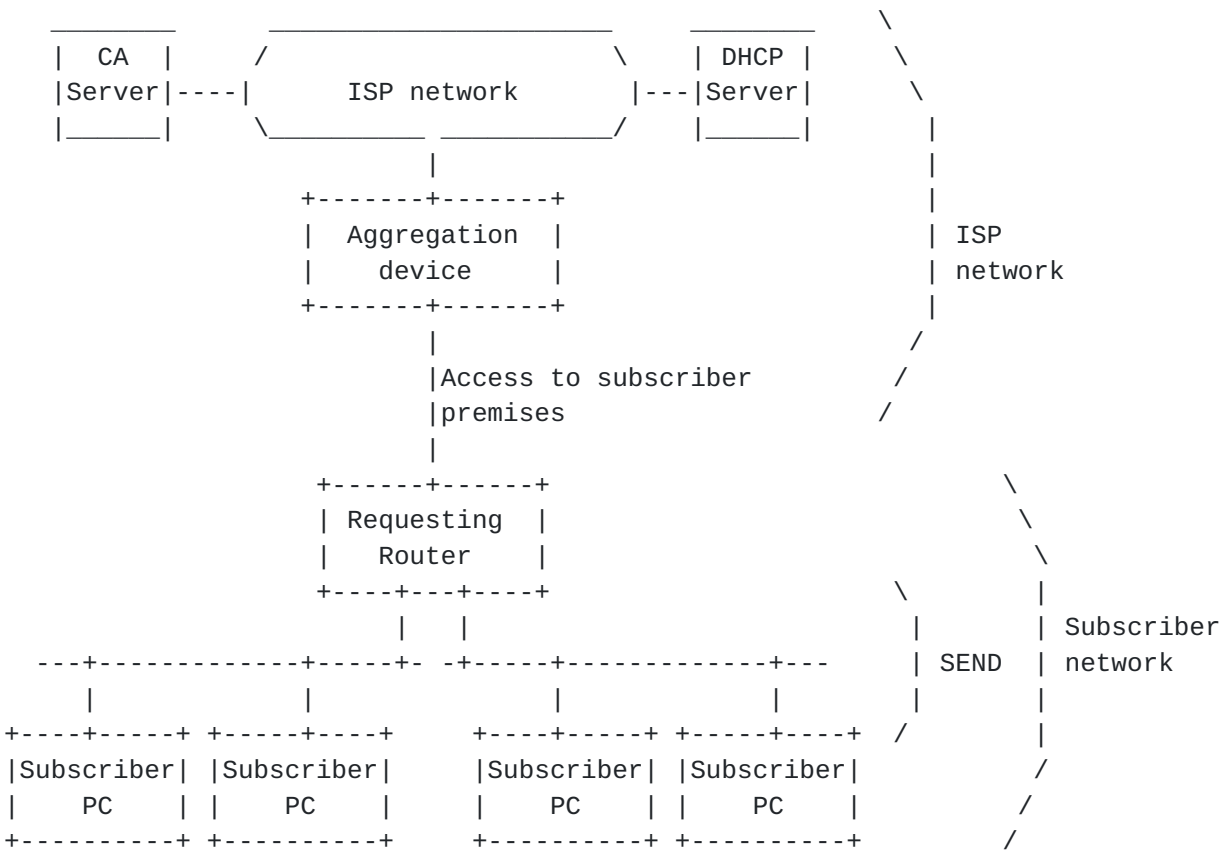


Figure 1

In the environment described in Figure 1, the delegating server can be either the aggregating device (the gateway for the requesting router) or a DHCP server located somewhere within its network.

While there are several mechanisms by which the RR can acquire the certificate (manual provisioning, using a File System, SCEP, PKCS12, HTTP or using Self-Signed certificates), their use would imply a less dynamic CPE provisioning mechanism and additional control plane or operational functions needed for the CA to learn and maintain the state of prefixes allocated by the DHCP-PD server. Alternatively, the distribution of the certificate can be facilitated by the DHCP-PD server along with the process of delegating the prefix which has to be certified.

With the DHCP certificate options, the DHCP-PD server can offer, upon request, to intermediate the process of acquiring a certificate or to provide the information needed by the RR to acquire the certificate through an alternative mechanism. Since RR's clients can require certificates originated in various certificate authorities, the services requested and offered through this option must be related to

a certification chain trust anchor as described in RFC4210 [7].

A DHCP server which ends up facilitating the certificate acquisition (and not just providing a pointer) can be seen to be similar to the Registration Authority (RA) entity described in RFC4210. Figure 2 shows the relationship between the subscriber PC, the Requesting Router (RR), the Delegating Router (DR) and the Certificate Authority (CA). Figure 2 also describes conceptually the message exchanges that, along with the prefix delegation facilitate the acquisition of a certificate.

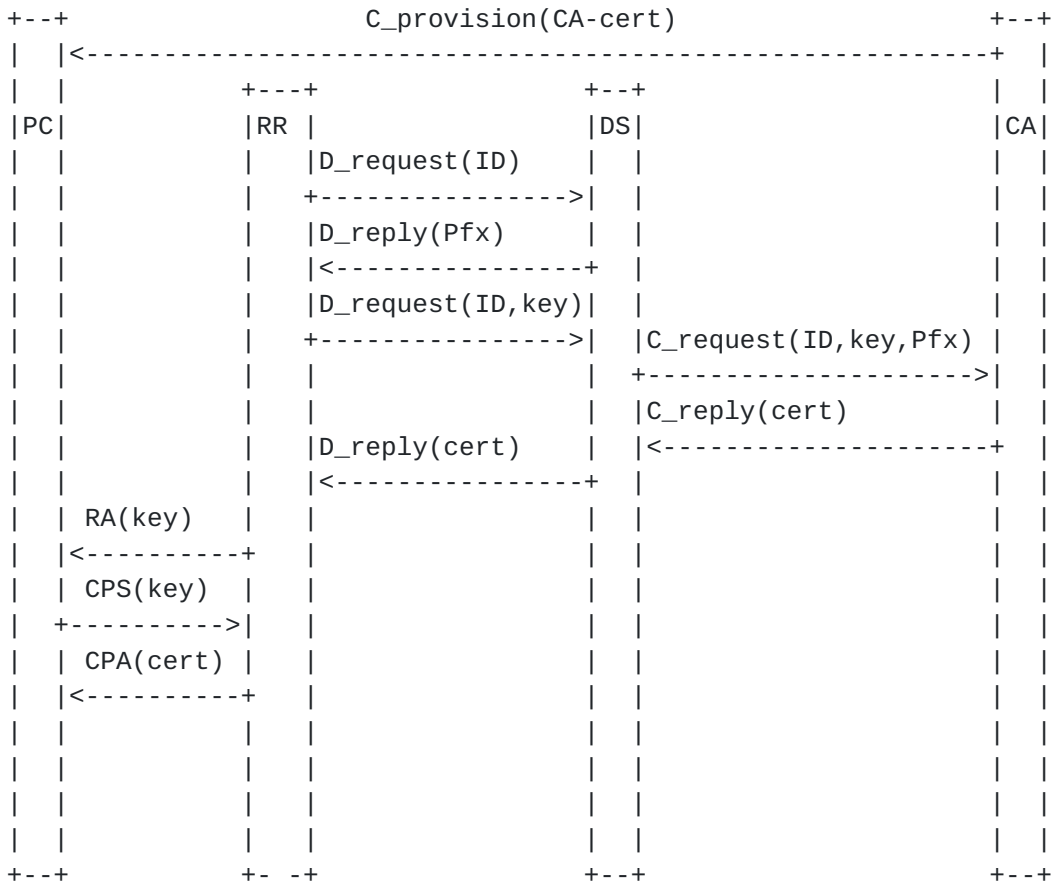


Figure 2

The Delegating Server acts as a Registration Authority between the Requesting Router (RR) and the Certification Authority (CA). It receives the RR public key and identity ID, thru DHCP flows, then builds a certificate request that it sends to the CA.

The certificate request is built with the syntax specified in [8], Section 5. The subject is filled with the DUID of the RR. The

publicKey is the one provided by the Requesting Router in the DHCP request. It is under the responsability of the DS (or other devices leveraged by the DHCP deployment for this purpose) to verify the RR identity, so no Proof Of Possession is provided by the DS in the certificate request.

## 5. Identity Association for Prefix Delegation

In the context of DHCP facilitated certificate distribution, the requesting router and the delegating server use the Identity Association for Prefix Delegation (IA_PD) described in RFC3633 to identify, group and manage the delegated prefixes. The IA_PD option code is 25, the IAID is 4 octets and the T1, T2 timers are used to manage the communication between the requesting router and the delegating server as described in section 9 of RFC3633. Operational status information is exchanged via Status Code options.

The certificate is related to a delegated prefix or to all delegated prefixes. The new option called "Certificate Option" (CO) is defined for the IA_PD to enable the requesting router and the delegating server to identify and manage the certificates corresponding to delegated prefixes.

The option can appear multiple times in the DHCP messages. It must provide the resources to indicate what type of assistance is needed or can be provided in the process of acquiring a certificate. In certain circumstances a full certificate is requested from the DHCP server while in other a pointer (IP address of FQDN) to the certificate server is sufficient.

The process of facilitating the acquisition of a certificate requires the CO option to carry various information types between the DHCP client and the DHCP server. The option can be used to inform the client or the server of a preferred Trust Anchor for the certificate chain. It can be used by the client to provide its public key to the DHCP server which in turn uses it to obtain the certificate. The server uses the option to deliver a certificate to the client or to provide a pointer (IP address or FQDN) to a Certificate server.

Note: In the case where the DHCP server provides a certificate to the client, one certificate can be built for each prefix under the IA_PD or a single certificate can be built for all prefixes under the IA_PD.

The format of the CO option is shown in Figure 2.

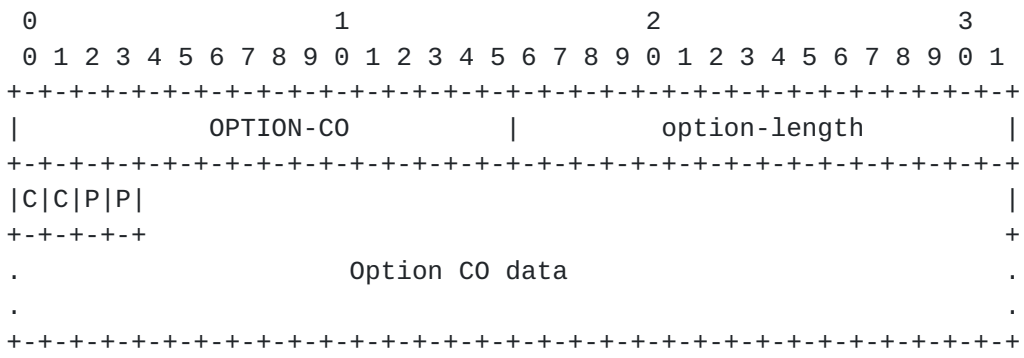


Figure 2

OPTION_CO: Certificate option

CO option-length: Length of the CO-option

C Flag: Two bits field indicating the capabilities requested or offered. The C flag values are:
00 - Any capability
01 - Pointer to Certificate Server
10 - Certificate
11 - Both pointer and certificate

P Flag: Two bits field indicating the type of data present in the CO option payload. The P flag values are:
00 - Certificate chain trust anchor
01 - Public key
10 - Pointer to certificate server
11 - Certificate

Option data: The CO option can contain various types of data as indicated through the P flag: Public Key, Certificate pointer, certificate chain trust anchor.

The usage of the CO option is described in Section 7.

## 6. Mode of Operation Overview

The mode of operation described in Sections 11, 12 and 13 of RFC3633 remain unchanged in the context of certificate management. Additional information however will be exchanged between the requesting router and the delegating server to indicate interest in a certificate, to advertise the ability to facilitate the acquisition of a certificate and to exchange certificate related information.

Sections 11, 12 and 13 of RFC3633 should be read in conjunction with the subsequent sections of this document for a complete understanding of DHCP's mode of operation in the context of managing certificates.

## 7. Delegating Server Solicitation

In the process of discovering a prefix delegating router, the requesting router can choose to indicate interest in a server with the capability to facilitate the acquisition of a certificate and it can select a server based on its level of support for managing certificates.

### 7.1. Requesting Router Behavior

The requesting router creates and transmits a Solicit message with a IA_PD option as described in section 11.1 of RFC3633. To indicate interest in certificate related information, the requesting router includes a CO-option which can contain the following information:

- It sets the C flag bits to indicate the level of assistance it wants: any, pointer, certificate or both pointer and certificate
- In the payload it can include the certificate chain trust anchor of interest in which case the P flag bits are set to 00. Otherwise the payload is set to all zeros

The requesting router processes any received Advertise messages as described in Section 11.1 of RFC3633. The requesting router selects an advertising server based on the level of service offered for certificate management and the provisioning requirements of the requesting router. Since the delegating server is required to advertise its full capabilities related to certificate management, the requesting router must select a server which will be able to provide the information requested through the follow up Request message described in Section 8.1.

Should a requesting router receive no Advertisements from servers with the certificate management capabilities needed, the requesting router SHOULD default to the lowest level of support which might be simple prefix delegation with no certificate management assistance. In this situation, the requesting router will rely on other mechanisms to acquire its certificates should they be needed.

### 7.2. Delegating Server Behavior

In response to a Solicit message containing an IA_PD option, the delegating server MUST include in its Advertise message described in section 11.2 of RFC3633 the CO-option to indicate its capabilities of supporting the certificate management process for the prefixes it

delegates.

The certificate management services offered by the delegating server can be advertised for each certificate chain trust anchor for which the server can facilitate the process of acquiring a certificate. One CO option will be included for each certificate trust anchor with the following settings:

- The C flag bits are set to indicate servers capabilities for a given certificate trust anchor: any, pointer, certificate or both pointer and certificate
- P flag is set to 00 and the payload contains the identifier for the certificate chain trust anchor

## 8. Requesting Router Initiated Prefix and Certificate Delegation

A requesting router uses the same messages described in Section 12 of RFC3633 to populate the IA_PD with prefixes. Additionally, it can acquire a certificate for the delegated prefixes or a locator for a certificate authority which it can later contact via other mechanisms to acquire a certificate.

This section addresses environments similar to the one described in Figure 1 where the DHCP-PD requesting router requires a certificate for the delegated prefix. The requesting router selected from received advertisements a delegating server which has the desired capabilities to support certificate management.

### 8.1. Requesting Router Behavior

To acquire the certificates, the requesting router uses the private key of a pair of RSA keys it previously generated independently of the provisioning mechanism described in this document. After identifying a delegating server which has the capability to assist with the process of acquiring a certificate for the delegated prefixes and possibly a trust anchor of interest, the requesting router creates and transmits a Request message as described in section 11.2 of RFC3633. The message is sent to the selected delegating sever and it contains one or more CO-options formatted in accordance with the capabilities of the selected server.

If assistance can be provided in relation to multiple trust anchors, the Request indicates, with the help of a CO option, which is the trust anchor of interest. This CO option proceeds subsequent CO options that might carry additional, certificate related information as described in the following two cases.

The server can provide a pointer to a certificate authority for a

given trust anchor:

- The C flag is set to 01 (pointer)
- The P flag can be set to 00 (certificate trust anchor) and the payload contains the ID of the trust anchor of interest. If the trust anchor is not important, the payload field can be set to all zeros.

The server can provide a complete certificate for a given trust anchor:

First CO option

* The C flag is set to 10 (certificate)
* The P field is set to 00 (certificate trust anchor) and the payload contains the ID of the trust anchor of interest.

Second CO option

* The C flag is set to 10
* The P field is set to 01 (public key) and the payload contains the public key of the requesting router

If the trust anchor is not important, then only the second CO option if included in the Request message.

As described in section 12.1 of RFC3633, the requesting router might need verification of the information bound to the IA_PD. The requesting router includes the IA_PD options in the Renew and Rebind messages where, along with the prefix information, it MUST include certificate related information according to the capabilities of the delegating server and optionally the trust anchor of interest.

In the Renew/Rebind messages, the CO option has the following settings:

- The C flag is set to indicates the level of certificate assistance support needed
- The P flag is set to 00 with the payload including the trust anchor of interest or the payload set to all zeros should the trust anchor not be relevant.

Upon the receipt of a valid Reply message for each IA_PD, a reply that can include either a pointer or a certificate, the requesting router will manage the delegated prefix as described in section 12.1. If a full certificate is provided, the requesting router will store it and use it in accordance with the recommendations of RFC3971 or any other related processes. If the delegating server provided only the pointer to the certificate authority, the requesting router will use an alternative mechanism to request a certificate.

Note that it is assumed that the requesting router does not require a certificate to authenticate the recommended certificate authority or the certificate authority which provided the certificate. It is assumed that the requesting router trusts the DHCP delegating server

the same way it trusts the server in providing the delegated prefix.

## 8.2. Delegating Server Behavior

In response to a Request message containing an IA_PD option with CO options, the delegating server MUST include in its Reply, along with the information described in section 12.2 of RFC3633, the CO-option containing the relevant information according to its advertised capabilities.

The server can provide a pointer to a certificate server or a complete certificate for a given trust anchor:

First CO option

* The C flag is set to the service being offered: 01 (pointer) or 10 (certificate)
* The P field is set to 00 (certificate trust anchor) and the payload contains the ID of the trust anchor of interest.

Second CO option

* The C flag is set to the service being offered: 01 (pointer) or 10 (certificate)
* The P field is set to 10 (pointer) or 11 (certificate) depending on the service offered

If the trust anchor is not important, then only the second CO option is included in the Request message.

If the delegating server can provide a complete certificate, upon the receipt of the Request with the public key of the requesting router, the delegating server contacts a pre-provisioned certificate authority (which can provide certificates chained to a trust anchor of interest) through a mechanism outside the scope of this document. The server submits to the CA the certificate request tuple (ID, public key, delegated prefix) along with the relevant state maintenance timers for the delegated prefix. The CA generates a certificate and sends it back to the delegating server.

Handling of Renew and Rebind messages is dictated by the procedures defined in section 12.2 of RFC3633. From the certificate maintenance perspective, if the delegating server identifies an active IA_PD binding, it will resubmit in response the location of the certificate authority (stateless information) or would acquire a new certificate and send it in response.

# 9. Delegating Server Triggered Reconfiguration

The CO option can be included in a Reconfigure message as described in RFC3315. This enables the server to request a client to renew its certificates for an IA_PD for which it has an active biniding. The

triggered reconfiguration can be in relation to a given trust anchor.

The Co option in the Reconfigure message can have the following format:

First CO option

* The C flag is set to the service being offered: 01 (pointer) or 10 (certificate)
* The P field is set to 00 (certificate trust anchor) and the payload contains the ID of the trust anchor of interest.

Second CO option

* The C flag is set to the service being offered: 01 (pointer) or 10 (certificate)
* The P field is set to 11 (certificate) and the payload set to all zeros

If the trust anchor is not important, then only the second CO option is included in the Reconfigure message.

## 10. Security Considerations

The mechanism described in this document is subject to the same security considerations as the ones described in section 15 of RFC3633. No additional security considerations are necessary.

Note: Through its binding to the IA_PD, the certificate acquisition process described adopts the trust model of the DHCP-PD process. If the information used to build an IA_PD binding is sufficient for the server to delegate a prefix to a CPE, it is considered sufficient to have the server facilitate the process of acquiring a certificate. When the server provides a certificate to the client, it acts similar to a Registration Authority [8] and contacts the certificate authority for the certificate. In that process, the server might need to provide, along with the other relevant information (ID, public key, prefix) a client's proof-of-possession. This scenario is not addressed in this document.

## 11. IANA Considerations

This document does not define any new namespaces or other constants for which IANA must maintain a registry..

## 12. References

## 12.1. Normative References

[1] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, March 1997.

[2] Deering, S. and R. Hinden, "Internet Protocol, Version 6 (IPv6) Specification", RFC 2460, December 1998.

[3] Droms, R., Bound, J., Volz, B., Lemon, T., Perkins, C., and M. Carney, "Dynamic Host Configuration Protocol for IPv6 (DHCPv6)", RFC 3315, July 2003.

[4] Troan, O. and R. Droms, "IPv6 Prefix Options for Dynamic Host Configuration Protocol (DHCP) version 6", RFC 3633, December 2003.

[5] Lynn, C., Kent, S., and K. Seo, "X.509 Extensions for IP Addresses and AS Identifiers", RFC 3779, June 2004.

[6] Arkko, J., Kempf, J., Zill, B., and P. Nikander, "SEcure Neighbor Discovery (SEND)", RFC 3971, March 2005.

[7] Adams, C., Farrell, S., Kause, T., and T. Mononen, "Internet X.509 Public Key Infrastructure Certificate Management Protocol (CMP)", RFC 4210, September 2005.

[8] Schaad, J., "Internet X.509 Public Key Infrastructure Certificate Request Message Format (CRMF)", RFC 4211, September 2005.

## 12.2. Informative References

Authors' Addresses

Ciprian Popoviciu
Cisco Systems
Kit Creek Road
RTP, North Carolina 27709
USA

Phone: 919 787 8162
Email: cpopovic@cisco.com

Ralph Droms
Cisco Systems
1414 Massachusetts Avenue
Boxborough MA 01719
USA

Phone: +1 978.936.1674
Email: rdroms@cisco.com

Eric Levy-Abegnoli
Cisco Systems
Village d'Entreprises Green Side - 400, Avenue Roumanille Batiment T 3
Biot - Sophia Antipolis PROVENCE-ALPES-COTE D'AZUR 06410
France

Phone: +33 49 723 2620
Email: elevyabe@cisco.com

## Full Copyright Statement

Copyright (C) The IETF Trust (2008).

This document is subject to the rights, licenses and restrictions contained in BCP 78, and except as set forth therein, the authors retain all their rights.

This document and the information contained herein are provided on an "AS IS" basis and THE CONTRIBUTOR, THE ORGANIZATION HE/SHE REPRESENTS OR IS SPONSORED BY (IF ANY), THE INTERNET SOCIETY, THE IETF TRUST AND THE INTERNET ENGINEERING TASK FORCE DISCLAIM ALL WARRANTIES, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO ANY WARRANTY THAT THE USE OF THE INFORMATION HEREIN WILL NOT INFRINGE ANY RIGHTS OR ANY IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.

## Intellectual Property

The IETF takes no position regarding the validity or scope of any Intellectual Property Rights or other rights that might be claimed to pertain to the implementation or use of the technology described in this document or the extent to which any license under such rights might or might not be available; nor does it represent that it has made any independent effort to identify any such rights. Information on the procedures with respect to rights in RFC documents can be found in BCP 78 and BCP 79.

Copies of IPR disclosures made to the IETF Secretariat and any assurances of licenses to be made available, or the result of an attempt made to obtain a general license or permission for the use of such proprietary rights by implementers or users of this specification can be obtained from the IETF on-line IPR repository at http://www.ietf.org/ipr.

The IETF invites any interested party to bring to its attention any copyrights, patents or patent applications, or other proprietary rights that may cover technology that may be required to implement this standard. Please address the information to the IETF at ietf-ipr@ietf.org.

## Acknowledgment

Funding for the RFC Editor function is provided by the IETF Administrative Support Activity (IASA).