

DHC working group  
Internet-Draft  
Intended status: Standards Track  
Expires: March 1, 2018

S. Nalluri  
Ericsson  
August 28, 2017

DHCPv6 Options for LWM2M bootstrap information  
draft-ietf-dhc-dhcpv6-lwm2m-bootstrap-options-00

## Abstract

This document defines Dynamic Host Configuration Protocol and Dynamic Host Configuration Protocol version 6 (DHCPv6) Options for LWM2M client bootstrap information, which are used to carry Uniform Resource Locator of LWM2M bootstrap server and certificate that validates the public key presented by server.

## Status of This Memo

This Internet-Draft is submitted in full conformance with the provisions of [BCP 78](#) and [BCP 79](#).

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF). Note that other groups may also distribute working documents as Internet-Drafts. The list of current Internet-Drafts is at <http://datatracker.ietf.org/drafts/current/>.

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."

This Internet-Draft will expire on March 1, 2018.

## Copyright Notice

Copyright (c) 2017 IETF Trust and the persons identified as the document authors. All rights reserved.

This document is subject to [BCP 78](#) and the IETF Trust's Legal Provisions Relating to IETF Documents (<http://trustee.ietf.org/license-info>) in effect on the date of publication of this document. Please review these documents carefully, as they describe your rights and restrictions with respect to this document. Code Components extracted from this document must include Simplified BSD License text as described in Section 4.e of the Trust Legal Provisions and are provided without warranty as described in the Simplified BSD License.

Internet-Draft

DHCPv6 Options for LWM2M

August 2017

## Table of Contents

<a href="#">1.</a>	Introduction . . . . .	<a href="#">2</a>
<a href="#">2.</a>	Terminology . . . . .	<a href="#">2</a>
<a href="#">3.</a>	LWM2M bootstrap server information through DHC . . . . .	<a href="#">3</a>
<a href="#">3.1.</a>	DHCPv6 option for LWM2M bootstrap server URI . . . . .	<a href="#">3</a>
<a href="#">3.2.</a>	DHCPv6 option for LWM2M server certificate . . . . .	<a href="#">4</a>
<a href="#">3.3.</a>	DHCPv4 option for LWM2M bootstrap server URI . . . . .	<a href="#">4</a>
<a href="#">3.4.</a>	DHCPv4 option for LWM2M server certificate . . . . .	<a href="#">5</a>
<a href="#">4.</a>	LWM2M-server-certificate encoding . . . . .	<a href="#">5</a>
<a href="#">5.</a>	Appearance of Option . . . . .	<a href="#">6</a>
<a href="#">5.1.</a>	Appearance of options in DHCPv6 control messages . . . . .	<a href="#">6</a>
<a href="#">5.2.</a>	Appearance of options in DHCPv4 control messages . . . . .	<a href="#">6</a>
<a href="#">6.</a>	Configuration Guidelines for the Server . . . . .	<a href="#">7</a>
<a href="#">7.</a>	DHCPv4/DHCPv6 Client Behavior . . . . .	<a href="#">7</a>
<a href="#">8.</a>	Relay agent Behavior . . . . .	<a href="#">8</a>
<a href="#">9.</a>	Security Considerations . . . . .	<a href="#">8</a>
<a href="#">10.</a>	Acknowledgement . . . . .	<a href="#">8</a>
<a href="#">11.</a>	IANA Considerations . . . . .	<a href="#">8</a>
<a href="#">12.</a>	References . . . . .	<a href="#">9</a>
<a href="#">12.1.</a>	Normative References . . . . .	<a href="#">9</a>
<a href="#">12.2.</a>	Informative References . . . . .	<a href="#">10</a>
	Author's Address . . . . .	<a href="#">10</a>

[1.](#) Introduction

Light weight machine to machine (LWM2M) protocol is used to manage end device life cycle in machine to machine communication scenarios. LWM2M device bootstrap is an optional life cycle phase for devices to get needed information when starting up for first time. Information gathered during bootstrapping might include management server details and security certificates required to establish connectivity with management server. Information required to connect with bootstrap server might be hard coded during device manufacturing phase.

Hard coding configuration by device manufacturer forces device operator to use same configuration as hard coded. It is possible that reachability information of bootstrap server that is hard coded may be outdated and boot strap server reachability might fail during first use of device. In such cases connectivity with bootstrap server is possible only through device software upgrade.

[2.](#) Terminology



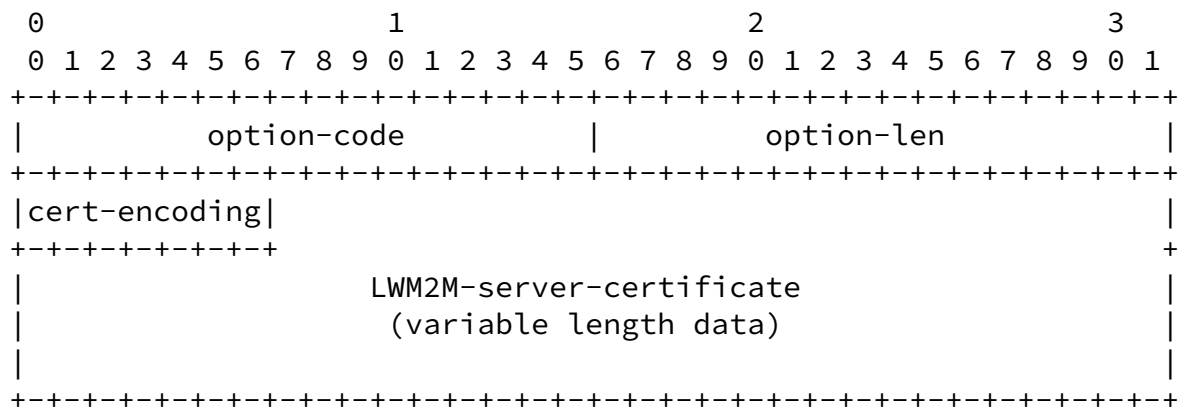
option-code: OPTION\_LWM2M\_BOOTSTRAP\_URI

option-len: Length of the 'LWM2M-bootstrap-URI' field in octets

LWM2M-bootstrap-URI: This string is URI of LWM2M bootstrap server.  
The string is not null-terminated.

### [3.2.](#) DHCPv6 option for LWM2M server certificate

DHCPv6 option OPTION\_LWM2M\_SERVER\_CERTIFICATE conveys security certificate which can be used by LWM2M client to establish secure connection with LWM2M server reachable through IPv6 network. The format of LWM2M server certificate option is as shown below:



option-code: OPTION\_LWM2M\_SERVER\_CERTIFICATE

option-len: Length of the 'LWM2M-server-certificate' field in octets  
+ 1

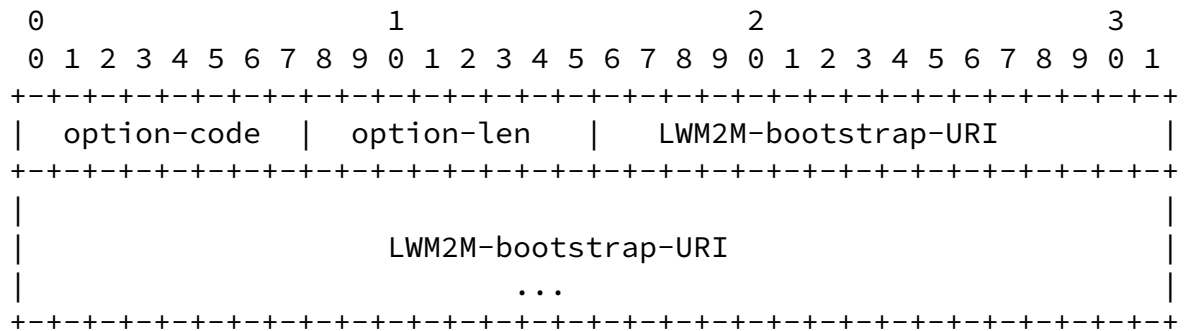
cert-encoding: This field indicates the type of certificate or certificate-related information contained in LWM2M-server-certificate field. See [Section 4](#) for details.

LWM2M-server-certificate: Digital certificate of LWM2M server

encoded according to cert-encoding. See [Section 4](#) for details

### 3.3. DHCPv4 option for LWM2M bootstrap server URI

DHCPv4 option OPTION\_LWM2M\_BOOTSTRAP\_URI conveys URI through which LWM2M client can reach LWM2M bootstrap server reachable through IPv4 network. The format of LWM2M bootstrap server URI option is as shown below:



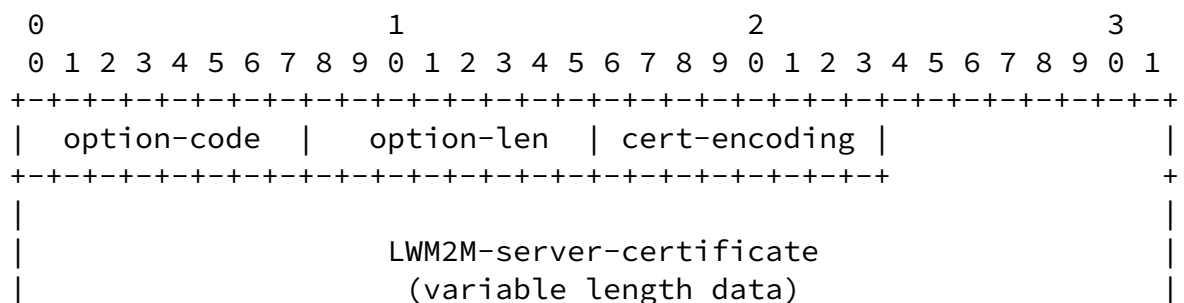
option-code: OPTION\_LWM2M\_BOOTSTRAP\_URI

option-len: Length of the 'LWM2M-bootstrap-URI' field in octets

LWM2M-bootstrap-URI: This string is URI of LWM2M bootstrap server.  
The string is not null-terminated.

### 3.4. DHCPv4 option for LWM2M server certificate

DHCPv4 option OPTION\_LWM2M\_SERVER\_CERTIFICATE conveys security certificate which can be used by LWM2M client to establish secure connection with LWM2M server reachable through IPv4 network. The format of LWM2M server certificate option is as shown below:





13	Hash and URL of X.509 bundle
14	OCSP Content
15	Raw Public Key
16-200	Unassigned
201-255	Private use

## 5. Appearance of Option

### 5.1. Appearance of options in DHCPv6 control messages

The OPTION\_LWM2M\_BOOTSTRAP\_URI and OPTION\_LWM2M\_SERVER\_CERTIFICATE options MUST NOT appear in messages other than the following: SOLICIT (1), ADVERTISE (2), REQUEST (3), REPLY (4), RENEW (5), REBIND (6), INFORMATION-REQUEST (11). If this option appears in messages other than those specified above, the receiver MUST ignore it.

The option number for OPTION\_LWM2M\_BOOTSTRAP\_URI and OPTION\_LWM2M\_SERVER\_CERTIFICATE options MAY appear in the "Option Request" option [[RFC3315](#)] in the following messages: SOLICIT (1), REQUEST (3), RENEW (5), REBIND (6), INFORMATION-REQUEST (11) and RECONFIGURE (10). If this option number appears in the "Option Request" option in messages other than those specified above, the receiver SHOULD ignore it.

### 5.2. Appearance of options in DHCPv4 control messages

The OPTION\_LWM2M\_BOOTSTRAP\_URI and OPTION\_LWM2M\_SERVER\_CERTIFICATE options MUST NOT appear in messages other than the following: DHCPDISCOVER (1), DHCPOFFER (2), DHCPREQUEST (3), DHCPACK (5) and DHCPINFORM (8). If this option appears in messages other than those specified above, the receiver MUST ignore it.

The option number for OPTION\_LWM2M\_BOOTSTRAP\_URI and OPTION\_LWM2M\_SERVER\_CERTIFICATE options MAY appear in the "Parameter Request List" option [[RFC2132](#)] in the following messages: DHCPDISCOVER (1), DHCPOFFER (2), DHCPREQUEST (3), DHCPACK (5) and DHCPINFORM (8). If this option number appears in the "Parameter Request List" option in messages other than those specified above, the receiver SHOULD ignore it.

Maximum possible value of DHCPv4 "option-len" is 255. LWM2M-server-certificate MAY be of length more than 255. To accommodate larger certificate, DHCP server SHOULD follow encoding as mentioned in [\[RFC3396\]](#).

## 6. Configuration Guidelines for the Server

DHCPv4 or DHCPv6 server that supports OPTION\_LWM2M\_BOOTSTRAP\_URI and OPTION\_LWM2M\_SERVER\_CERTIFICATE SHOULD be configured with one and only one LWM2M bootstrap server URI, and one and only one certificate that validates bootstrap server's public key.

In the absence of URI configuration, DHCP server SHOULD ignore option OPTION\_LWM2M\_BOOTSTRAP\_URI, and SHOULD continue processing of DHCP control message

In the absence of certificate configuration, DHCP server SHOULD ignore option OPTION\_LWM2M\_SERVER\_CERTIFICATE, and SHOULD continue processing of DHCP control message

## 7. DHCPv4/DHCPv6 Client Behavior

DHCP or DHCPv6 client MAY decide need for inclusion of OPTION\_LWM2M\_BOOTSTRAP\_URI and OPTION\_LWM2M\_SERVER\_CERTIFICATE options in DHCPv4 or DHCPv6 control messages if device is capable of supporting LWM2M client functionality irrespective of state of LWM2M client. It is possible that LWM2M client MAY not be active before DHCPv4 or DHCPv6 message exchanges happens. In such scenario, DHCPv4 or DHCPv6 client MAY collect LWM2M bootstrap server URI and LWM2M server certificate and keep ready for LWM2M client initialization

DHCPv4 or DHCPv6 client MAY prefer collecting LWM2M bootstrap server URI and LWM2M server certificate by including OPTION\_LWM2M\_BOOTSTRAP\_URI and OPTION\_LWM2M\_SERVER\_CERTIFICATE options in DHCPINFORM or INFORMATION-REQUEST message which MAY be send during LWM2M client initialization

LWM2M client devices running with IPv6 stack MAY use stateless auto address configuration to get IPv6 address. Such clients MAY use DHCPv6 INFORMATION-REQUEST to get LWM2M bootstrap URI and LWM2M



and OPTION\_LWM2M\_SERVER\_CERTIFICATE

## 8. Relay agent Behavior

This draft does not impose any new requirements on DHCPv4 or DHCPv6 relay agent functionality

## 9. Security Considerations

OPTION\_LWM2M\_BOOTSTRAP\_URI and OPTION\_LWM2M\_SERVER\_CERTIFICATE options could be used by an intruder to advertise the URI of a malicious LWM2M bootstrap server and certificate and can alter the LWM2M management server details provided to LWM2M client. The consequences of such an attack can be critical, because any data that is reported by LWM2M client MAY reach unwanted LWM2M management server. As an example, an attacker could collect data from secure locations by deploying malicious servers.

To prevent these attacks, it is strongly advisable to secure the use of this option by either:

- o Using authenticated DHCP as described in [\[RFC3315\], Section 21](#).
- o Using options OPTION\_LWM2M\_BOOTSTRAP\_URI and OPTION\_LWM2M\_SERVER\_CERTIFICATE only with trusted DHCP server

The security considerations documented in [\[RFC3315\]](#) are to be considered.

## 10. Acknowledgement

Particular thanks to A. Keraenen, J. Jimenez, J. Melen and S. Krishnan for the concept, inputs and review.

## 11. IANA Considerations

IANA is requested to assign new DHCPv6 option codes in the registry maintained in <http://www.iana.org/assignments/dhcpv6-parameters>:

Option Name	Value
OPTION_LWM2M_BOOTSTRAP_URI	TBA
OPTION_LWM2M_SERVER_CERTIFICATE	TBA

IANA is requested to assign new DHCPv4 option codes in the registry maintained in <http://www.iana.org/assignments/bootp-dhcp-parameters>:

---

Option Name	Value
OPTION_LWM2M_BOOTSTRAP_URI	TBA
OPTION_LWM2M_SERVER_CERTIFICATE	TBA

## [12.](#) References

### [12.1.](#) Normative References

- [RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", [BCP 14](#), [RFC 2119](#), DOI 10.17487/RFC2119, March 1997, <<https://www.rfc-editor.org/info/rfc2119>>.
- [RFC2131] Droms, R., "Dynamic Host Configuration Protocol", [RFC 2131](#), DOI 10.17487/RFC2131, March 1997, <<https://www.rfc-editor.org/info/rfc2131>>.
- [RFC2132] Alexander, S. and R. Droms, "DHCP Options and BOOTP Vendor Extensions", [RFC 2132](#), DOI 10.17487/RFC2132, March 1997, <<https://www.rfc-editor.org/info/rfc2132>>.
- [RFC3315] Droms, R., Ed., Bound, J., Volz, B., Lemon, T., Perkins, C., and M. Carney, "Dynamic Host Configuration Protocol for IPv6 (DHCPv6)", [RFC 3315](#), DOI 10.17487/RFC3315, July 2003, <<https://www.rfc-editor.org/info/rfc3315>>.
- [RFC3396] Lemon, T. and S. Cheshire, "Encoding Long Options in the Dynamic Host Configuration Protocol (DHCPv4)", [RFC 3396](#), DOI 10.17487/RFC3396, November 2002, <<https://www.rfc-editor.org/info/rfc3396>>.
- [RFC4306] Kaufman, C., Ed., "Internet Key Exchange (IKEv2) Protocol", [RFC 4306](#), DOI 10.17487/RFC4306, December 2005, <<https://www.rfc-editor.org/info/rfc4306>>.
- [RFC5280] Cooper, D., Santesson, S., Farrell, S., Boeyen, S., Housley, R., and W. Polk, "Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile", [RFC 5280](#), DOI 10.17487/RFC5280, May 2008, <<https://www.rfc-editor.org/info/rfc5280>>.
- [RFC7227] Hankins, D., Mrugalski, T., Siodelski, M., Jiang, S., and S. Krishnan, "Guidelines for Creating New DHCPv6 Options", [BCP 187](#), [RFC 7227](#), DOI 10.17487/RFC7227, May 2014, <<https://www.rfc-editor.org/info/rfc7227>>.

[RFC7296] Kaufman, C., Hoffman, P., Nir, Y., Eronen, P., and T. Kivinen, "Internet Key Exchange Protocol Version 2 (IKEv2)", STD 79, [RFC 7296](https://www.rfc-editor.org/info/rfc7296), DOI 10.17487/RFC7296, October 2014, <<https://www.rfc-editor.org/info/rfc7296>>.

## 12.2. Informative References

[IKEv2IANA] "Internet Key Exchange Version 2 (IKEv2) Parameters", n.d., <<https://www.iana.org/assignments/ikev2-parameters/ikev2-parameters.xhtml>>.

### Author's Address

Srinivas Rao Nalluri  
Ericsson  
Bangalore  
India

Email: [srinivasa.rao.nalluri@ericsson.com](mailto:srinivasa.rao.nalluri@ericsson.com)

Nalluri

Expires March 1, 2018

[Page 10]