

Network Working Group	G. Zorn
Internet-Draft	Network Zen
Intended status: Standards Track	Q. Wu
Expires: October 24, 2011	Y. Wang
	Huawei
	April 22, 2011

The ERP Local Domain Name DHCPv6 Option
draft-ietf-hokey-ldn-discovery-10

Abstract

In order to derive a Domain-Specific Root Key (DSRK) from the Extended Master Session Key (EMSK) generated as a side-effect of an Extensible Authentication Protocol (EAP) method, the EAP peer must discover the name of the domain to which it is attached.

This document specifies a Dynamic Host Configuration Protocol Version 6 (DHCPv6) option designed to allow a DHCPv6 server to inform clients using the EAP Re-authentication Protocol (ERP) EAP method of the name of the local domain for ERP.

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 October 24, 2011.

Copyright Notice

Copyright (c) 2011 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.

[Table of Contents](#)

- *1. [Introduction](#)
- *2. [Terminology](#)
 - *2.1. [Standards Language](#)
 - *2.2. [Acronyms](#)
- *3. [Option Format](#)
 - *3.1. [DHCPv6 ERP Local Domain Name Option](#)
- *4. [Client Behavior](#)
- *5. [Relay Agent Behavior](#)
- *6. [Security Considerations](#)
- *7. [IANA considerations](#)
- *8. [References](#)
 - *8.1. [Normative References](#)
 - *8.2. [Informative References](#)
- *[Authors' Addresses](#)

1. Introduction

The EAP Re-authentication Protocol (ERP) [\[RFC5296\]](#) is designed to allow faster re-authentication of a mobile device which was previously authenticated by means of the Extensible Authentication Protocol [\[RFC3748\]](#). Given that the local root key (e.g., DSRK [RFC 5295](#) [\[RFC5295\]](#)) is generated using the local domain name (LDN), LDN discovery is an important part of re-authentication. As described in [RFC 5296](#) [\[RFC5296\]](#), the LDN to be used in ERP can be learned by the mobile device through the ERP exchange or via a lower-layer mechanism. However, no lower-layer mechanisms for LDN discovery have yet been defined.

This document specifies an extension to DHCPv6 for LDN to be used in ERP.

[2. Terminology](#)

[2.1. Standards Language](#)

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 [\[RFC2119\]](#).

[2.2. Acronyms](#)

FQDN Fully Qualified Domain Name

AAA Authentication, Authorization and Accounting

DSRK Domain-Specific Root Key

[3. Option Format](#)

In DHCPv6-based local domain name discovery, the LDN option is used by the DHCPv6 client to obtain the local domain name from the DHCPv6 Server after full EAP authentication has taken place.

The contents of the ERP Local Domain Name option are intended only for use with ERP and do not represent the name of a local domain for any other purposes.

[3.1. DHCPv6 ERP Local Domain Name Option](#)

```
0                               1                               2                               3
0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+
| OPTION_ERP_LOCAL_DOMAIN_NAME |          option-length          |
+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+
| erp-local-domain-name...   |
+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--
```

The format of this option is:

option code

OPTION_ERP_LOCAL_DOMAIN_NAME (TBD)

option-length

Length of the erp-local-domain-name field, in octets

erp-local-domain-name

This field contains the name of the local ERP domain and MUST be encoded as specified in [Section 8 of RFC 3315](#) [\[RFC3315\]](#). Note that this encoding does enable the use of internationalized domain names, but only as a set of A-labels [\[RFC5890\]](#).

4. Client Behavior

If a DHCPv6 client doesn't know the ERP LDN and requires the DHCPv6 Server to provide the DHCPv6 ERP LDN option, it MUST include an Option Request option requesting the DHCPv6 ERP Local Domain Name option, as described in Section 22.7 of RFC 3315 [\[RFC3315\]](#).

When the DHCPv6 client receives an ERP Local Domain Name option with the ERP LDN present in it, it MUST verify that the option length is no more than 256 octets (the maximum length of a single fully-qualified domain name (FQDN) allowed by the DNS), and that the local domain name is a properly encoded single FQDN, as specified in Section 8, "Representation and Use of Domain Names" of RFC3315 [\[RFC3315\]](#).

5. Relay Agent Behavior

If a DHCPv6 relay agent has pre-existing knowledge of the ERP local domain name for a client (for example, from a previous AAA exchange), it SHOULD include it in an instance of the DHCPv6 ERP Local Domain Name option and forward to the DHCPv6 server as a suboption of the Relay-Supplied Options option [\[I-D.ietf-dhc-dhcpv6-relay-supplied-options\]](#).

6. Security Considerations

The communication between the DHCPv6 client and the DHCPv6 server for the exchange of local domain name information is security sensitive and requires server authentication and integrity protection. DHCPv6 security [\[RFC3315\]](#) can be used for this purpose.

7. IANA considerations

IANA is requested to assign one new option code from the registry of DHCP Option Codes maintained at <http://www.iana.org/assignments/dhcpv6-parameters>, referencing this document.

8. References

8.1. Normative References

[RFC2119]	Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels" , BCP 14, RFC 2119, March 1997.
[RFC5296]	Narayanan, V. and L. Dondeti, " EAP Extensions for EAP Re-authentication Protocol (ERP) ", RFC 5296, August 2008.
[RFC5295]	Salowey, J., Dondeti, L., Narayanan, V. and M. Nakhjiri, " Specification for the Derivation of Root Keys from an Extended Master Session Key (EMSK) ", RFC 5295, August 2008.
[RFC3315]	

	Droms, R., Bound, J., Volz, B., Lemon, T., Perkins, C. and M. Carney, " Dynamic Host Configuration Protocol for IPv6 (DHCPv6) ", RFC 3315, July 2003.
[I-D.ietf-dhc-dhcpv6-relay-supplied-options]	Lemon, T and W Wu, " Relay-Supplied DHCP Options ", Internet-Draft draft-ietf-dhc-dhcpv6-relay-supplied-options-04, October 2010.

8.2. Informative References

[RFC3748]	Aboba, B., Blunk, L., Vollbrecht, J., Carlson, J. and H. Levkowetz, " Extensible Authentication Protocol (EAP) ", RFC 3748, June 2004.
[RFC5890]	Klensin, J., " Internationalized Domain Names for Applications (IDNA): Definitions and Document Framework ", RFC 5890, August 2010.

Authors' Addresses

Glen Zorn
Zorn Network Zen 227/358 Thanon Sanphawut
Bang Na, Bangkok 10260 Thailand Phone: +66 (0) 87-040-4617 EMail:
gwz@net-zen.net

Qin Wu
Wu Huawei Technologies Co., Ltd. 101 Software Avenue, Yuhua
District Nanjing, Jiangsu 21001 China Phone: +86-25-84565892 EMail:
sunseawq@huawei.com

Yungui Wang
Wang Huawei Technologies Co., Ltd. Site B, Floor 10,
HuiHong Mansion, No.91 BaiXia Rd. Nanjing, Jiangsu 210001 P.R. China
Phone: +86 25 84565893 EMail: w52006@huawei.com