

Dynamic Host Configuration  
Internet-Draft  
Intended status: Standards Track  
Expires: January 15, 2009

H. Tschofenig  
Nokia Siemens Networks  
A. Yegin  
Samsung  
D. Forsberg  
Nokia  
July 14, 2008

Bootstrapping [RFC3118](#) Delayed DHCP Authentication Using EAP-based  
Network Access Authentication  
draft-yegin-eap-boot-rfc3118-03.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 January 15, 2009.

Internet-Draft

Bootstrapping [RFC 3118](#)

July 2008

## Abstract

The DHCP authentication extension ([RFC 3118](#)) cannot be widely deployed due to lack of a key agreement protocol. This document outlines how EAP-based network access authentication mechanisms can be used to establish bootstrap keying material that can be used to subsequently use [RFC 3118](#) security.

## Table of Contents

<a href="#">1.</a>	Introduction . . . . .	<a href="#">3</a>
<a href="#">2.</a>	Terminology . . . . .	<a href="#">5</a>
<a href="#">3.</a>	Overview and Building Blocks . . . . .	<a href="#">6</a>
<a href="#">4.</a>	Buliding DHCP SA . . . . .	<a href="#">8</a>
<a href="#">4.1.</a>	802.1X . . . . .	<a href="#">8</a>
<a href="#">4.2.</a>	PPP . . . . .	<a href="#">8</a>
<a href="#">4.3.</a>	PANA . . . . .	<a href="#">9</a>
<a href="#">4.4.</a>	Computing DHCP SA . . . . .	<a href="#">11</a>
<a href="#">5.</a>	Delivering DHCP SA . . . . .	<a href="#">13</a>
<a href="#">6.</a>	Using DHCP SA . . . . .	<a href="#">15</a>
<a href="#">7.</a>	Security Considerations . . . . .	<a href="#">18</a>
<a href="#">8.</a>	IANA Considerations . . . . .	<a href="#">22</a>
<a href="#">9.</a>	Open Issues . . . . .	<a href="#">23</a>
<a href="#">10.</a>	Acknowledgments . . . . .	<a href="#">24</a>
<a href="#">11.</a>	References . . . . .	<a href="#">25</a>
<a href="#">11.1.</a>	Normative References . . . . .	<a href="#">25</a>
<a href="#">11.2.</a>	Informative References . . . . .	<a href="#">25</a>
	Authors' Addresses . . . . .	<a href="#">27</a>
	Intellectual Property and Copyright Statements . . . . .	<a href="#">28</a>

## 1. Introduction

The Extensible Authentication Protocol (EAP) [[RFC3748](#)] provides a network access authentication framework by carrying authentication process between the hosts and the access networks. The combination of EAP with a AAA architecture allows authentication and authorization of a roaming user to an access network. A successful authentication between a client and the network produces a dynamically created trust relation between the two. Almost all EAP methods (e.g., EAP-TLS, EAP-SIM) are capable of generating cryptographic keys between the EAP peer and the EAP server. Using key transport via the AAA infrastructure the EAP server makes the EAP-provided keying material available to the Authenticator (e.g., Network Access Server; NAS) after a successful authentication attempt. These keys are commonly used in conjunction with per-packet security mechanisms (e.g., link-layer ciphering). This procedure is described in [[I-D.ietf-eap-keying](#)].

DHCP [[RFC2131](#)] is a protocol which provides a host with configuration parameters. The base DHCP does not include any security mechanism, hence it is vulnerable to a number of security threats. The security considerations section of [RFC 2131](#) [[RFC2131](#)] identifies it as "quite insecure" and lists various security threats.

[RFC 3118](#) [[RFC3118](#)] is the DHCP authentication protocol that defines how to authenticate various DHCP messages. It does not support roaming clients and assumes out-of-band or manual key establishment. These limitations have been inhibiting widespread deployment of this security mechanism as noted in a DHCPv4 threat analysis [[I-D.ietf-dhc-v4-threat-analysis](#)].

It is possible to use the authentication and key exchange procedure executed during the network access authentication to bootstrap a security association for DHCP. The access authentication procedure can be utilized to dynamically provide the keying material to [RFC 3118](#) based security protection for DHCP. This document defines how

to use the EAP-based access authentication procedure to bootstrap [RFC 3118](#) security.

The general framework of the mechanism described in this I-D can be outlined as follows:

1. The client gains network access by utilizing an EAP method that generates session keys. As part of the network access process, the client and the authentication agent (NAS) communicate their intention to create a DHCP security association and exchange the required parameters (e.g., nonce, key ID, etc.) The required information exchange is handled by the EAP lower-layer which also

carries EAP.

2. Although the newly generated DHCP SA is already available to the DHCP client, in case the NAS (acting as a DHCP relay) and the DHCP server are not co-located, the SA parameters need to be communicated to the DHCP server. This requires a protocol exchange, which can be piggybacked with the DHCP signaling.
3. The DHCP signaling that immediately follows the network access authentication process utilizes [RFC 3118](#) to secure the protocol exchange. Both the client and the server rely on the DHCP SA to compute and verify the authentication codes.

This framework requires extensions to the EAP lower-layers (PPP [[RFC1661](#)], IEEE 802.1X , PANA [[RFC5191](#)]) to carry the supplemental parameters required for the generation of the DHCP SA. Another extension is required to carry the DHCP SA parameters from a DHCP relay to a DHCP server. [RFC 3118](#) can be used without any modifications or extensions.

## [2.](#) Terminology

In this document, the key words "MAY", "MUST", "MUST NOT", "OPTIONAL", "RECOMMENDED", "SHOULD", and "SHOULD NOT", are to be interpreted as described in [[RFC2119](#)].

This document uses the following terms:

### DHCP Security Association:

To secure DHCP messages a number of parameters including the key that is shared between the client (DHCP client) and the DHCP server have to be established. These parameters are collectively referred to as DHCP security association (or in short DHCP SA).

DHCP SA can be considered as a group security association. The DHCP SA parameters are provided to the DHCP server as soon as the client chooses the server to carry out DHCP. The same DHCP SA can be used by any one of the DHCP servers that are available to the client.

### DHCP Key:

This term refers to the fresh and unique session key dynamically established between the DHCP client and the DHCP server. This key is used to protect DHCP messages as described in [[RFC3118](#)].

### [3.](#) Overview and Building Blocks

The bootstrapping mechanism requires protocol interaction between the client host (which acts as a DHCP client), the NAS and the DHCP server. A security association will be established between the DHCP server and the DHCP client to protect the DHCP messages.

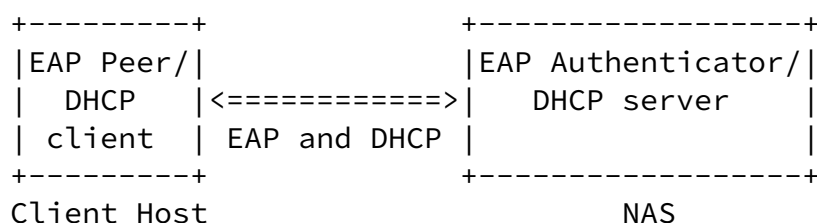
A DHCP SA is generated based on the EAP method derived key after a successful EAP method protocol run. Both the client and the NAS should agree on the generation of a DHCP SA after the EAP SA is created. This involves a handshake between the two and exchange of additional parameters (such as nonce, key ID, etc.). These additional information needs to be carried over the EAP lower-layer that also carries the EAP payloads.

The DHCP SA is ultimately needed by the DHCP client and the DHCP server. On the network side, the DHCP SA information needs to be transferred from the NAS (where it is generated) to the DHCP server (where it will be used). On the client host side, it is transferred from the network access authentication client to the DHCP client.

NAS is always located one IP hop away from the client. If the DHCP server is on the same link, it can be co-located with the NAS. When the NAS and the DHCP server are co-located, an internal mechanism, such as an API, is sufficient for transferring the SA information. If the DHCP server is multiple hops away from the DHCP client, then there must be a DHCP relay on the same link as the client. In that case, the NAS should be co-located with the DHCP relay

[RFC4014] enables transmission of AAA-related RADIUS attributes from a DHCP relay to a DHCP server in the form of relay agent information options. DHCP SA is generated at the end of the AAA process, and therefore it can be provided to the DHCP server in a sub-option carried along with other AAA-related information. Confidentiality, replay, and integrity protection of this exchange MUST be provided. [\[I-D.ietf-dhc-relay-agent-ipsec\]](#) proposes IPsec protection of the DHCP messages exchanged between the DHCP relay and the DHCP server. DHCP objects (protected with IPsec) can therefore be used to communicate the necessary parameters.

Two different deployment scenarios are illustrated in Figure 1.



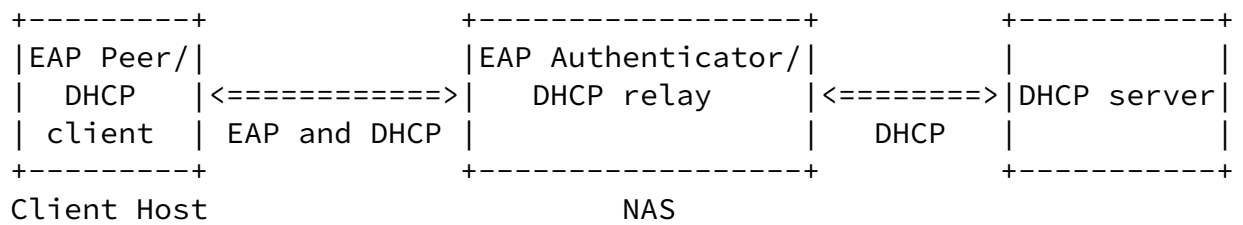


Figure 1: Protocols and end points.

When the DHCP SA information is received by the DHCP server and client, it can be used along with [RFC 3118](#) to protect DHCP messages against various security threats. This draft provides the guidelines regarding how the [RFC 3118](#) protocol fields should be filled in based on the DHCP SA.



DHCP SA is created at the end of the EAP-based access authentication process. This section describes extensions to the EAP lower-layers for exchanging the additional information, and the process of generating the DHCP SA.

#### [4.1.](#) 802.1X

This work needs to be done in the IEEE and hence this section is intentionally left blank.

#### [4.2.](#) PPP

A new IPCP configuration option is defined in order to bootstrap DHCP SA between the PPP peers. Each end of the link must separately request this option for mutual establishment of DHCP SA. Only one side sending the option will not produce any state.

The detailed DHCP-SA Configuration Option is presented below.

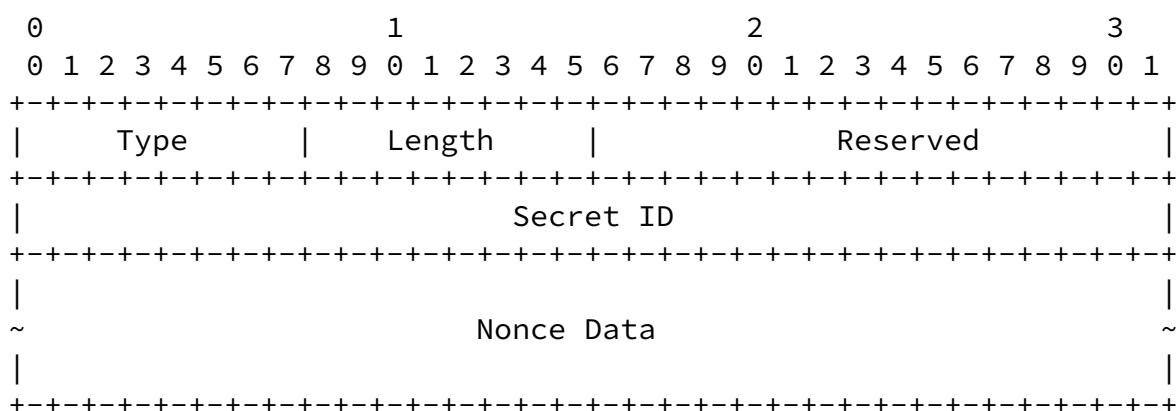


Figure 2: DHCP SA Configuration Option

Type

- o TBD

Length

- o  $\geq 24$

Reserved

- o A 16-bit value reserved for future use. It MUST be initialized to zero by the sender, and ignored by the receiver.

#### Secret ID

- o 32 bit value that identifies the DHCP Key produced as a result of the bootstrapping process. This value is determined by the NAS and sent to the client. The NAS determines this value by randomly picking a number from the available secret ID pool. If the client does not request DHCP-SA configuration option, this value is returned to the available identifiers pool. Otherwise, it is allocated to the client until the DHCP SA expires. The client MUST set this field to all 0s in its own request.

#### Nonce Data (variable length)

- o Contains the random data generated by the transmitting entity. This field contains the Nonce\_client value when the option is sent by client, and the Nonce\_NAS value when the option is sent by NAS. Nonce value MUST be randomly chosen and MUST be at least 128 bits in size. Nonce values MUST NOT be reused.

### [4.3.](#) PANA

A new PANA AVP is defined in order to bootstrap DHCP SA. The DHCP-AVP is included in the PANA-Bind-Request message if PAA (NAS) is offering DHCP SA bootstrapping service. If the PaC wants to proceed with creating DHCP SA at the end of the PANA authentication, it MUST include DHCP-AVP in its PANA-Bind-Answer message.

Absence of this AVP in the PANA-Bind-Request message sent by the PAA indicates unavailability of this additional service. In that case, PaC MUST NOT include DHCP-AVP in its response, and PAA MUST ignore received DHCP-AVP. When this AVP is received by the PaC, it may or may not include the AVP in its response depending on its desire to create a DHCP SA. A DHCP SA can be created as soon as each entity has received and sent one DHCP-AVP.

The detailed DHCP-AVP format is presented below:

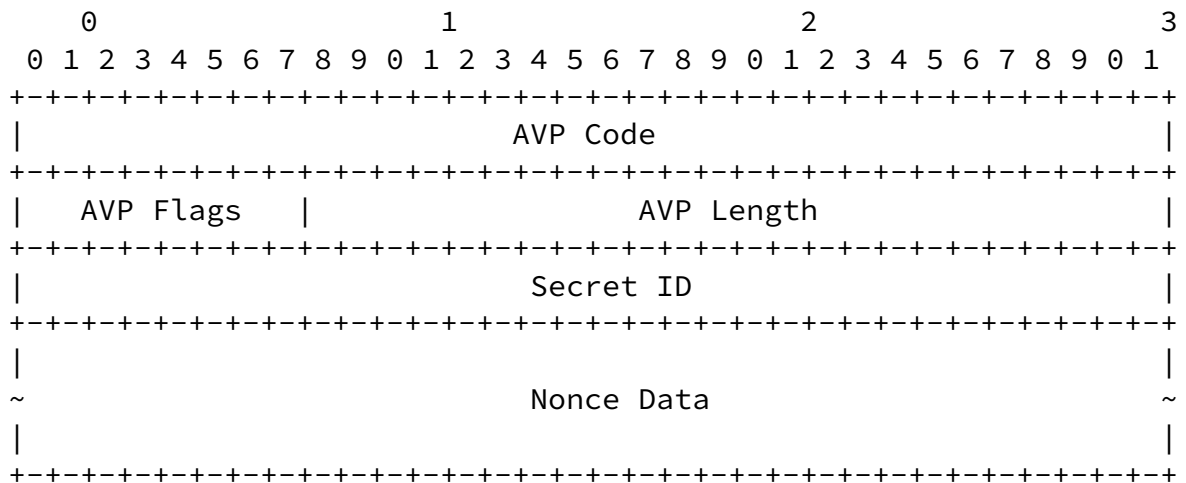


Figure 3: DHCP AVP Format

## AVP Code

- o TBD

## AVP Flags

- o The AVP Flags field is eight bits. The following bits are assigned:

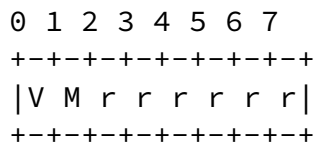


Figure 4: DHCP AVP Flags

## M(andatory)

- o The 'M' Bit, known as the Mandatory bit, indicates whether support of the AVP is required. This bit is not set in DHCP-AVP.

## V(endor)

- o The 'V' bit, known as the Vendor-Specific bit, indicates whether the optional Vendor-Id field is present in the AVP header. This bit is not set in DHCP-AVP.

r(eserved)

- o These flag bits are reserved for future use, and MUST be set to zero, and ignored by the receiver.

AVP Length

- o The AVP Length field is three octets, and indicates the number of octets in this AVP including the AVP Code, AVP Length, AVP Flags, and AVP data.

Secret ID

- o A 32-bit value that identifies the DHCP Key produced as a result of the bootstrapping process. This value is determined by the PAA and sent to the PaC. The PAA determines this value by randomly picking a number from the available secret ID pool. If PaC's response does not contain DHCP-AVP then this value is returned to the available identifiers pool. Otherwise, it is allocated to the PaC until the DHCP SA expires. The PaC MUST set this field to all 0s in its response.

Nonce Data (variable length)

- o Contains the random data generated by the transmitting entity. This field contains the Nonce\_client value when the AVP is sent by PaC, and the Nonce\_NAS value when the AVP is sent by PAA. Nonce value MUST be randomly chosen and MUST be at least 128 bits in size. Nonce values MUST NOT be reused.

#### [4.4.](#) Computing DHCP SA

The key derivation procedure is reused from IKE [[RFC2409](#)]. The character '|' denotes concatenation.

DHCP Key = HMAC-SHA1(MSK, const | Secret ID | Nonce\_client | Nonce\_NAS)

The values have the following meaning:

**MSK:**

A key derived by the EAP peer and EAP (authentication) server at the end of the successful network access AAA.

**const:**

This is a string constant. The value of the const parameter is set to "EAP [RFC 3118](#) Bootstrapping".

Tschofenig, et al.	Expires January 15, 2009	[Page 11]
--------------------	--------------------------	-----------

---

Internet-Draft	Bootstrapping <a href="#">RFC 3118</a>	July 2008
----------------	--	-----------

**Secret ID:**

The unique identifier of the DHCP key as carried by the EAP lower-layer protocol extension.

**Nonce Client:**

This random number is provided by the client and carried by the EAP lower-layer protocol extension.

**Nonce NAS:**

This random number is provided by the NAS and carried by the EAP lower-layer protocol.

**DHCP Key:**

This session key is 128-bit in length and used as the session key for securing DHCP messages. Figure 1 of [EAP-Key] refers to this derived key as a Transient Session Key (TSK).

The lifetime of the DHCP security association has to be limited to

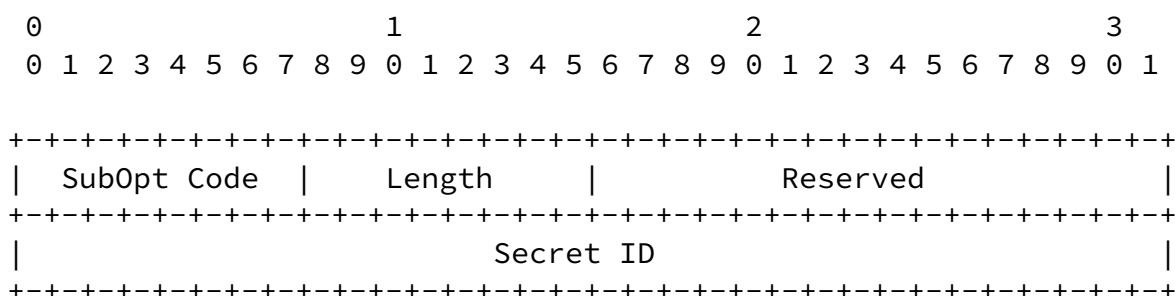
prevent the DHCP server from storing state information indefinitely. The lifetime of the DHCP SA SHOULD be set equal to the lifetime of the network access service. The client host, NAS, and the DHCP server SHOULD be (directly or indirectly) aware of this lifetime at the end of a network access AAA.

The PaC can at any time trigger a new bootstrapping protocol run to establish a new security association with the DHCP server. The IP address lease time SHOULD be limited by the DHCP SA lifetime

## 5. Delivering DHCP SA

When the NAS and the DHCP server are not co-located, the DHCP SA information is carried from the NAS (DHCP relay) to the DHCP server in a DHCP relay agent info option. This sub-option can be included along with the RADIUS attributes sub-option that is carried after the network access authentication.

The format of the DHCP SA sub-option is:





## Lifetime:

The lifetime of the DHCP SA. This Unsigned32 value contains the number of seconds remaining before the DHCP SA is considered expired.

## [6.](#) Using DHCP SA

Once the DHCP SA is in place, it is used along with [RFC 3118](#) to secure the DHCP protocol exchange.



[RFC 3118](#) [[RFC3118](#)] defines two security protocols with a newly defined authentication option:

- o Configuration token
- o Delayed authentication

The generic format of the authentication option is defined in [Section 2 of RFC 3118](#) [[RFC3118](#)] and contains the following fields:

- o Code
- o Delayed authentication

The value for the Code field of this authentication option is 90.

- o Length

The Length field indicates the length of the authentication option payload.

- o Protocol

[RFC 3118](#) [[RFC3118](#)] defines two values for the Protocol field - zero and one. A value of zero indicates the usage of the configuration token authentication option.

As described in [Section 4 of RFC 3118](#) [[RFC3118](#)] the configuration token only provides weak entity authentication. Hence its usage is not recommended. This authentication option will not be considered for the purpose of bootstrapping.

A value of one in the Protocol field in the authentication option indicates the delayed authentication. The usage of this option is subsequently assumed in this document.

Since the value for this field is known in advance it does not need to be negotiated between the DHCP client and DHCP server.

- o Algorithm

[RFC 3118](#) [[RFC3118](#)] only defines the usage of HMAC-MD5 (value 1 in the Algorithm field). This document assumes that HMAC-MD5 is used to

protect DHCP messages.

Since the value for this field is known in advance it does not need to be negotiated. [Editor's Note: Based on crypto agility requirements it seems reasonable to consider future algorithm support as well.]

- o Replay Detection Method (RDM)

The value of zero for the RDM name space is assigned to use a monotonically increasing value.

Since the value for this field is known in advance it does not need to be negotiated.

- o Replay Detection

This field contains the value that is used for replay protection. This value MUST be monotonically increasing according to the provided replay detection method. An initial value must, however, be set. In case of bootstrapping with EAP an initial value of zero is used. The length of 64 bits (and a start-value of zero) ensures that a sequence number rollover is very unlikely to occur.

Since the value for this field is known in advance it does not need to be negotiated.

- o Authentication Information

The content of this field depends on the type of message where the authentication option is used. [Section 5.2 of RFC 3118](#) [[RFC3118](#)] does not provide content for the DHCPDISCOVER and the DHCPINFORM message. Hence for these messages no additional considerations need to be specified in this document.

Since the value for this field is known in advance it does not need to be negotiated.

For a DHCP OFFER, DHCPREQUEST or DHCPACK message the content of the Authentication Information field is given as:

- o Secret ID (32 bits)
- o HMAC-MD5 (128 bits)

The Secret ID is chosen by the NAS to prevent collisions. [NOTE: If there are multiple NASes per DHCP server, this identifier space might

need to be pre-partitioned among the NASes.]

Tschofenig, et al.

Expires January 15, 2009

[Page 16]

---

Internet-Draft

Bootstrapping [RFC 3118](#)

July 2008

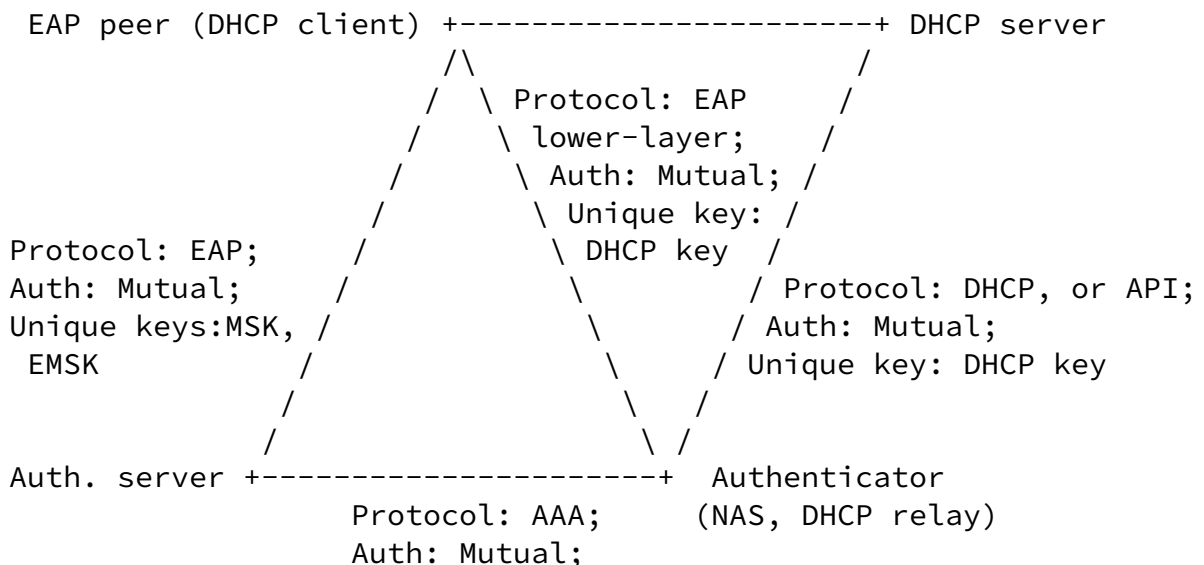
HMAC-MD5 is the output of the key message digest computation. Note that not all fields of the DHCP message are protected as described in [RFC 3118](#) [[RFC3118](#)].

## 7. Security Considerations

This document describes a mechanism for dynamically establishing a security association to protect DHCP signaling messages.

If the NAS and the DHCP server are co-located then the session keys and the security parameters are transferred locally (via an API call). Some security protocols already exercise similar methodology to separate functionality.

If the NAS and the DHCP server are not co-located then there is some similarity to the requirements and issues discussed with the EAP Keying Framework (see [\[I-D.ietf-eap-keying\]](#)). The DHCP key is a Transient Session Key (TEK) from [\[I-D.ietf-eap-keying\]](#). The key is generated by both the DHCP client and the DHCP relay, and transported from the DHCP relay to the DHCP server. The DHCP protocol exchange between the DHCP client and DHCP server is protected using this key.



Unique key:  
AAA session key

### Figure 6: Keying Architecture

Figure 6 describes the participating entities and the protocols executed among them. It must be ensured that the derived session key between the DHCP client and the DHCP server is fresh and unique.

The key transport mechanism, which is used to carry the session key between the NAS and DHCP server, must provide the following functionality:

Tschafenig, et al. Expires January 15, 2009 [Page 18]

---

Internet-Draft Bootstrapping [RFC 3118](#) July 2008

- o Confidentiality protection
- o Replay protection
- o Integrity protection

Furthermore, it is necessary that the two parties (DHCP server and the NAS) authorize the establishment of the DHCP security association.

Below we provide a list of security properties of the suggested mechanism:

Algorithm independence:

This proposal bootstraps a DHCP security association for [RFC 3118](#) where only a single integrity algorithm (namely HMAC-MD5) is proposed which is mandatory to implement.

Establish strong, fresh session keys (maintain algorithm independence):

This scheme relies on EAP methods to provide strong and fresh session keys for each initial authentication and key exchange protocol run. Furthermore the key derivation function provided in [Section 4.4](#) contains random numbers provided by the client and the

NAS which additionally add randomness to the generated key.

#### Replay protection:

Replay protection is provided at different places. The EAP method executed between the EAP peer and the EAP server MUST provide a replay protection mechanism. Additionally random numbers and the secret ID are included in the key derivation procedure which aim to provide a fresh and unique session key between the DHCP client and the DHCP server. Furthermore, the key transport mechanism between the NAS and the DHCP server must also provide replay protection (in addition to confidentiality protection). Finally, the security mechanisms provided in [RFC 3118](#), for which this draft bootstraps the security association, also provides replay protection.

#### Authenticate all parties:

Authentication between the EAP peer and the EAP server is based on the used EAP method. After a successful authentication and protocol run, the host and the NAS in the network provide MSK confirmation either based on the 4-way handshake in IEEE 802.11i

or based on the protected PANA exchange. DHCP key confirmation between the DHCP client and server is provided with the first protected DHCP message exchange.

#### Perform authorization:

Authorization for network access is provided during the EAP exchange. The authorization procedure for DHCP bootstrapping is executed by the NAS before this service is offered to the client. The NAS might choose not to include DHCP-AVP or DHCP SA Configuration Option during network access authorization based on the authorization policies.

#### Maintain confidentiality of session keys:

The DHCP session keys are only known to the intended parties (i.e., to the DHCP client, relay, and server). The EAP protocol itself does not transport keys. The exchanged random numbers which are incorporated into the key derivation function do not

need to be kept confidential. DHCP relay agent information MUST be protected using [[RFC4014](#)] with non-null IPsec encryption.

Confirm selection of 'best' cipher-suite:

This proposal does not provide confidentiality protection of DHCP signaling messages. Only a single algorithm is offered for integrity protection. Hence no algorithm negotiation and therefore no confirmation of the selection occur.

Uniquely name session keys:

The DHCP SA is uniquely identified using a Secret ID (described in [[RFC3118](#)] and reused in this document).

Compromised NAS and DHCP server:

A compromised NAS may leak the DHCP session key and the EAP derived session key (e.g., MSK). It will furthermore allow corruption of the DHCP protocol executed between the hosts and the DHCP server since NAS either acts as a DHCP relay or a DHCP server. A compromised NAS may also allow creation of further DHCP SAs or other known attacks on the DHCP protocol (e.g., address depletion). A compromised NAS will not be able to modify, replay, inject DHCP messages which use security associations established without the EAP-based bootstrapping mechanism (e.g., manually configured DHCP SAs). On the other hand, a compromised DHCP server may only leak the DHCP key information. MSK will not be compromised in this case.

Bind key to appropriate context:

The key derivation function described in [Section 4.4](#) includes parameters (such as the secret ID and a constant) which prevents reuse of the established session key for other purposes.

## [8.](#) IANA Considerations

[Editor's Note: A future version of this draft will provide IANA considerations.]





## 9. Open Issues

This document describes a bootstrapping procedure for DHCPv4. The same procedure could be applied for DHCPv6 but is not described in this document.

## [10.](#) Acknowledgments

We would like to thank Yoshihiro Ohba and Mohan Parthasarathy for their feedback to this document. Additionally, we would to thank Ralph Droms, Allison Mankin and Barr Hibbs for their support to continue this work.

Internet-Draft

Bootstrapping [RFC 3118](#)

July 2008

## [11.](#) References

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

- [RFC1661] Simpson, W., "The Point-to-Point Protocol (PPP)", STD 51, [RFC 1661](#), July 1994.
- [RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", [BCP 14](#), [RFC 2119](#), March 1997.
- [RFC2131] Droms, R., "Dynamic Host Configuration Protocol", [RFC 2131](#), March 1997.
- [RFC3118] Droms, R. and W. Arbaugh, "Authentication for DHCP Messages", [RFC 3118](#), June 2001.
- [RFC3748] Aboba, B., Blunk, L., Vollbrecht, J., Carlson, J., and H. Levkowitz, "Extensible Authentication Protocol (EAP)", [RFC 3748](#), June 2004.
- [RFC4014] Droms, R. and J. Schnizlein, "Remote Authentication Dial-In User Service (RADIUS) Attributes Suboption for the Dynamic Host Configuration Protocol (DHCP) Relay Agent Information Option", [RFC 4014](#), February 2005.

### [11.2.](#) Informative References

- [I-D.ietf-dhc-relay-agent-ipsec]  
Droms, R., "Authentication of DHCP Relay Agent Options Using IPsec", [draft-ietf-dhc-relay-agent-ipsec-02](#) (work in progress), May 2005.
- [I-D.ietf-dhc-v4-threat-analysis]  
Hibbs, R., "Dynamic Host Configuration Protocol for IPv4 (DHCPv4) Threat Analysis",

[draft-ietf-dhc-v4-threat-analysis-03](#) (work in progress),  
June 2006.

[I-D.ietf-eap-keying]

Aboba, B., Simon, D., and P. Eronen, "Extensible  
Authentication Protocol (EAP) Key Management Framework",  
[draft-ietf-eap-keying-22](#) (work in progress),  
November 2007.

[RFC2409] Harkins, D. and D. Carrel, "The Internet Key Exchange  
(IKE)", [RFC 2409](#), November 1998.

[RFC5191] Forsberg, D., Ohba, Y., Patil, B., Tschofenig, H., and A.

Tschofenig, et al. Expires January 15, 2009 [Page 25]

---

Internet-Draft Bootstrapping [RFC 3118](#) July 2008

Yegin, "Protocol for Carrying Authentication for Network  
Access (PANA)", [RFC 5191](#), May 2008.

#### Authors' Addresses

Hannes Tschofenig  
Nokia Siemens Networks  
Linnoitustie 6  
Espoo 02600  
Finland

Phone: +358 (50) 4871445  
Email: [Hannes.Tschofenig@gmx.net](mailto:Hannes.Tschofenig@gmx.net)  
URI: <http://www.tschofenig.priv.at>

Alper E. Yegin  
Samsung  
Istanbul,  
Turkey

Phone:  
Email: [a.yegin@partner.samsung.com](mailto:a.yegin@partner.samsung.com)

Dan Forsberg  
Nokia Research Center  
P.O. Box 407  
FIN-00045  
Finland

Phone: +358 50 4839470  
Email: dan.forsberg@nokia.com

Tschofenig, et al. Expires January 15, 2009 [Page 27]

---

Internet-Draft Bootstrapping [RFC 3118](#) July 2008

#### 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

## 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](mailto:ietf-ipr@ietf.org).