

IETF PANA Working Group  
Internet Draft

H. Tschofenig  
Siemens  
Corporate Technology  
A. Yegin  
DoCoMo USA Labs  
D. Forsberg  
Nokia

Document:

[draft-tschofenig-pana-bootstrap-rfc3118-01.txt](#)

Expires: April 2004

October 2003

Bootstrapping [RFC3118](#) Delayed authentication using PANA  
<[draft-tschofenig-pana-bootstrap-rfc3118-01.txt](#)>

## Status of this Memo

This document is an Internet-Draft and is subject to all provisions of [Section 10 of RFC2026](#).

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/lid-abstracts.html>

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

## Abstract

DHCP authentication extension ([RFC3118](#)) cannot be widely deployed due to lack of an out-of-band key agreement protocol for DHCP clients and servers. This draft outlines how EAP methods carried over PANA can be used to establish a local trust relation and generate keys that can be used in conjunction with [RFC3118](#).

## Table of Contents

<a href="#">1.</a>	Introduction.....	<a href="#">2</a>
<a href="#">2.</a>	Terminology.....	<a href="#">3</a>
<a href="#">3.</a>	Overview and Building Blocks.....	<a href="#">4</a>
<a href="#">3.1</a>	PaC to PAA Communication.....	<a href="#">5</a>
<a href="#">3.2</a>	PAA to DHCP Communication.....	<a href="#">5</a>
<a href="#">3.3</a>	Key Derivation.....	<a href="#">6</a>
<a href="#">4.</a>	Requirements.....	<a href="#">6</a>
<a href="#">5.</a>	Security parameters for <a href="#">RFC 3118</a> .....	<a href="#">7</a>
<a href="#">5.1</a>	Authentication Option of <a href="#">RFC 3118</a> .....	<a href="#">7</a>
<a href="#">5.1.1</a>	Code Field.....	<a href="#">8</a>
<a href="#">5.1.2</a>	Length Field.....	<a href="#">8</a>
<a href="#">5.1.3</a>	Protocol Field.....	<a href="#">8</a>
<a href="#">5.1.4</a>	Algorithm Field.....	<a href="#">8</a>
<a href="#">5.1.5</a>	Replay Detection Method (RDM) Field.....	<a href="#">8</a>
<a href="#">5.1.6</a>	Replay Detection Field.....	<a href="#">8</a>
<a href="#">5.1.7</a>	Authentication Information Field.....	<a href="#">9</a>
<a href="#">5.2</a>	Lifetime of the DHCP security association.....	<a href="#">9</a>
<a href="#">6.</a>	Processing Details and Payloads.....	<a href="#">9</a>
<a href="#">6.1</a>	Capability Indication and Trigger Message.....	<a href="#">9</a>
<a href="#">6.2</a>	Key Derivation.....	<a href="#">11</a>
<a href="#">6.3</a>	DHCP SA Sub-option.....	<a href="#">12</a>
<a href="#">7.</a>	Example message flow.....	<a href="#">13</a>
<a href="#">8.</a>	Security Considerations.....	<a href="#">14</a>
<a href="#">9.</a>	IANA Considerations.....	<a href="#">17</a>
<a href="#">10.</a>	Open Issues.....	<a href="#">18</a>
<a href="#">11.</a>	References.....	<a href="#">18</a>
<a href="#">12.</a>	Acknowledgments.....	<a href="#">19</a>
<a href="#">13.</a>	Author's Addresses.....	<a href="#">19</a>

[1.](#) Introduction

PANA [[PANA](#)] provides network access authentication by carrying Extensible Authentication Protocol (EAP) between the hosts and the access networks. The combination of EAP with an 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. Various EAP authentication methods are capable of generating cryptographic keys (e.g., shared secrets) between the client and the authentication agent after successful authentication.

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

[RFC 3118](#) is the DHCP authentication protocol which defines how to authenticate various DHCP messages. It does not support roaming  
Tschofenig et al. Expires - April 2004 [Page 2]

---

Internet Draft      Bootstrapping [RFC3118](#) using PANA      October 2003

clients and assumes out-of band or manual key establishment. These limitations have been inhibiting widespread deployment of this security mechanism.

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 trust relation created during the access authentication process can be used with [RFC 3118](#) to provide security for DHCP. This document defines how to use PANA to bootstrap [RFC 3118](#) for securing DHCP.

PANA protocol allows clients to use this protocol even before they are assigned an IP address. A PANA client (PaC) can use the unspecified IP address as its source address during this phase.

This approach provides a two-step solution:

- Authentication and key exchange (provided by EAP methods carried over PANA)
- DHCP message protection by generating the required shared secrets for [RFC 3118](#).

Instead of adding EAP support to DHCP itself (which requires modifications to the DHCP protocol due to the nature of EAP messaging) we keep the two protocols separate.

This document is organized as follows. [Section 2](#) describes new terms. [Section 3](#) gives an overview of the basic communication and describes the building blocks. Requirements are presented in [Section 4](#). The details of the established parameters for the DHCP SA are listed in [Section 5](#). Processing details and payload formats are illustrated in [Section 6](#). A short message flow describes the protocol interaction in [Section 6.3](#). Finally in [Section 8](#) additional security considerations are discussed.

## [2.](#) Terminology

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 PaC (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). Once a DHCP server is selected the DHCP SA is use between the DHCP client and the DHCP server.

- DHCP Key

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

Further PANA related terms can be found in [PY+02].

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

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

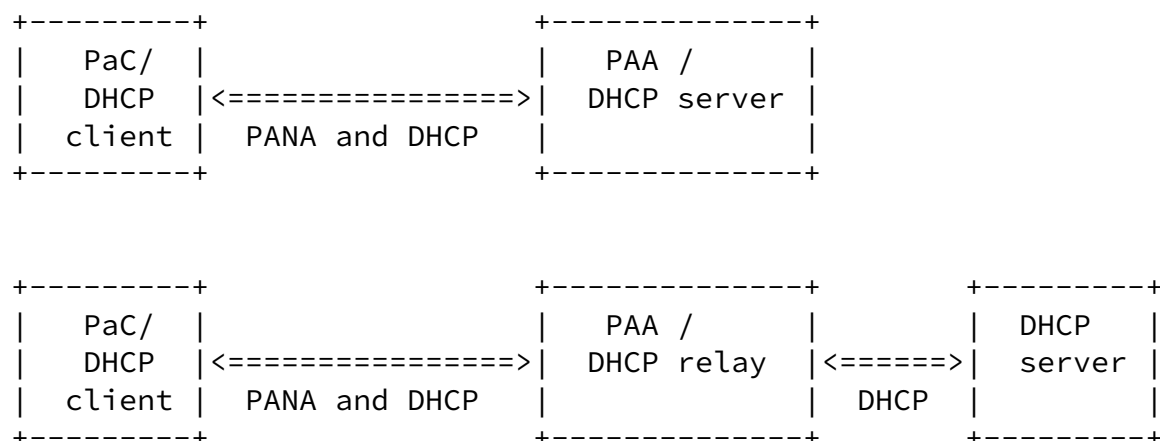
Based on the PANA protocol interaction this bootstrapping mechanism requires protocol interaction between the PaC (which acts as DHCP client), the PANA Authentication Agent (PAA) and the DHCP server. A security association will be established between the DHCP server and the DHCP client to protect DHCP messages.

DHCP SA is generated based on the PANA SA after a successful PANA authentication. DHCP SA information needs to be transferred from the PAA (where it is generated) to the DHCP server (where it will be needed).

PAA is located one IP hop away from the PaC. If the DHCP server is on the same link, it can be co-located with the PAA. When PAA and 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, PAA should be co-located with the DHCP relay. The SA information can be communicated to the DHCP server using the DHCP relay agent information options [DS02]. For the purpose of confidentiality protection IPsec protection MUST be applied as described in [RD03].

Two different scenarios are illustrated in Figure 1.



Legend:

Tschofenig et al.

Expires - April 2004

[Page 4]

Internet Draft

Bootstrapping [RFC3118](#) using PANA

October 2003

PaC - PANA Client

PAA - PANA Authentication Agent

Figure 1: DHCP Protocol Bootstrapping

When the DHCP SA information is received by the DHCP server and client, it can be used along with [RFC3118](#) to protect DHCP messages against various security threats.

The following building blocks have been identified:

### [3.1](#) PaC to PAA Communication

Additional payloads are required within PANA in order to bootstrap [RFC3118](#). These payloads therefore provide the following functionality:

a) Capability indication

A capability describes a certain functionality which is either supported or not. In order to trigger an action or to obtain a certain kind of data item it is necessary to execute some message exchanges. This message exchange allows both entities to learn commonly supported functionality.

#### b) Trigger message

A trigger message allows one entity (either PaC or PAA) to request a certain action to be executed. For this protocol a trigger message sent by the PaC causes the PAA to create the DHCP security association for support with [\[RFC3118\]](#).

[Section 6](#) describes the message payloads for the additional objects required in PANA usage with this bootstrapping protocol.

### [3.2](#) PAA to DHCP Communication

If the PAA and the DHCP server are co-located then only an API call is required for transferring the necessary information from the PAA to the DHCP server. If the PAA and the DHCP server are not co-located then an additional protocol is needed. [WH+02] points to the importance of this communication as: "Key distribution is not merely a data transport operation; it is also a mechanism for building transitive trust;". Indeed the trust relationship between the PaC and the PAA, which was dynamically established during network access authentication, is used to extend the trust relationship to the DHCP server. The PAA, which is co-located with the DHCP Relay, and the DHCP server trust each other and both entities belong to the same administrative domain as the PAA.

Tschofenig et al. Expires - April 2004

[Page 5]

Security sensitive information has to be exchanged (such as session keys) between the DHCP relay (PAA) and the DHCP server. This protocol is not part of PANA but the security implications must be considered.

[DS02] enables transmission of AAA-related RADIUS attributes from DHCP relay to 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. Protection of this exchange MUST be provided. [\[RD03\]](#) 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.

### [3.3](#) Key Derivation

As a result of the EAP authentication and key exchange method a Master Session Key (MSK) is established which is used to establish a PANA security association. The key derivation procedure for establishing PANA SA is defined in [[PANA](#)]. Another security association for usage with DHCP according to [[RFC3118](#)] needs to be established. A discussion of the required parameters for the security association is given in [Section 5](#) and the key derivation function is provided in [Section 6.2](#)

Since different bootstrapping applications need different keys it is necessary to derive these keys from the session key provided by the EAP method. It would be possible to reuse work done by members of the EAP working group on key derivation for multiple applications [[SE03](#)]. The key derivation mechanism used in this document is similar.

## [4.](#) Requirements

The following requirements regarding protocol design and deployment have to be met:

- The DHCP protocol as defined in [[RFC2131](#)] MUST NOT be modified.
- The security mechanism defined in [[RFC3118](#)] MUST NOT be modified.
- The key derivation procedure MUST establish a unique and fresh session key for the usage with [[RFC3118](#)]. The session key MUST never be used again in later protocol run.
- It MUST be ensured that only the intended parties have access to the session key. Hence the key transport between the PAA and the DHCP server MUST be authenticated, integrity, replay and confidentiality protected. The security mechanism used to protect

Tschofenig et al. Expires - April 2004

[Page 6]

the transport of the session key between the PAA and the DHCP server MUST have an adequate key strength. [Section 5.4](#) of [AS+03] offers a description of issues concerning key wrapping.

- The DHCP server MUST ensure that only authorized nodes are allowed to install keying material for subsequent DHCP message protection.

- The established DHCP security association MUST provide data origin authentication, integrity protection and replay protection. A non-goal of this draft is to provide confidentiality protection for DHCP messages.

- The lifetime of the DHCP session key is limited to the PANA session lifetime. The session key MUST NOT be used beyond that lifetime. The first DHCP message provides key confirmation of the established session key between the PaC and the DHCP server. The DHCP is active after a successful completion of the bootstrapping procedure (indicated by the PAA).

- Key Naming

Both the DHCP client and the DHCP server MUST have means to uniquely identify the DHCP SA.

The derived session key (DHCP key) MUST be bound to a particular session between the particular PaC and an entity in the access network. It MUST be possible for the two peers (PaC and DHCP server) to verify that each other is indeed the intended recipients of the distributed session key. Once the established DHCP SA is selected for protection of DHCP messages (implicit) key confirmation is provided.

## [5. Security parameters for \[RFC 3118\]\(#\)](#)

### [5.1 Authentication Option of \[RFC 3118\]\(#\)](#)

[RFC3118] defines two security protocols with a newly defined authentication option:

- Configuration token
- Delayed authentication

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

- Code (8 bits)
- Length (8 bits)
- Protocol (8 bits)
- Algorithm (8 bits)
- Replay Detection Method - RDM (8 bits)
- Replay Detection (64 bits)



- Authentication Information (variable length)

#### [5.1.1](#) Code Field

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

#### [5.1.2](#) Length Field

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

#### [5.1.3](#) Protocol Field

[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 \[RFC3118\]](#) 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.

#### [5.1.4](#) Algorithm Field

[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.

#### [5.1.5](#) Replay Detection Method (RDM) Field

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.

#### [5.1.6](#) Replay Detection Field

This field contains the value that is used for replay protection. This value MUST be monotonically increasing according to the

Internet Draft      Bootstrapping [RFC3118](#) using PANA

October 2003

An initial value must, however, be set. In case of bootstrapping with PANA an initial value of zero is used. The length of 64 bits (and a start-value of zero) ensure that a sequence number roll-over is very unlikely to occur.

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

#### [5.1.7](#) Authentication Information Field

The content of this field depends on the type of message where the authentication option is used. [Section 5.2 of \[RFC3118\]](#) 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.

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

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

The Secret ID is chosen by the PAA to prevent collisions.

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 [\[RFC3118\]](#).

#### [5.2](#) Lifetime of the DHCP security association

The lifetime of the DHCP security association has to be limited to prevent the DHCP from storing state information over a long time.

The lifetime of the DHCP SA should be set to the lifetime of PANA SA which is determined by the PANA session lifetime. The PaC (i.e. DHCP client), PAA, and DHCP server should be aware (directly or indirectly) about the lifetime.

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.

## 6. Processing Details and Payloads

This section defines the necessary extensions for PANA and a key derivation procedure.

### 6.1 Capability Indication and Trigger Message

Tschofenig et al.

Expires - April 2004

[Page 9]

Internet Draft

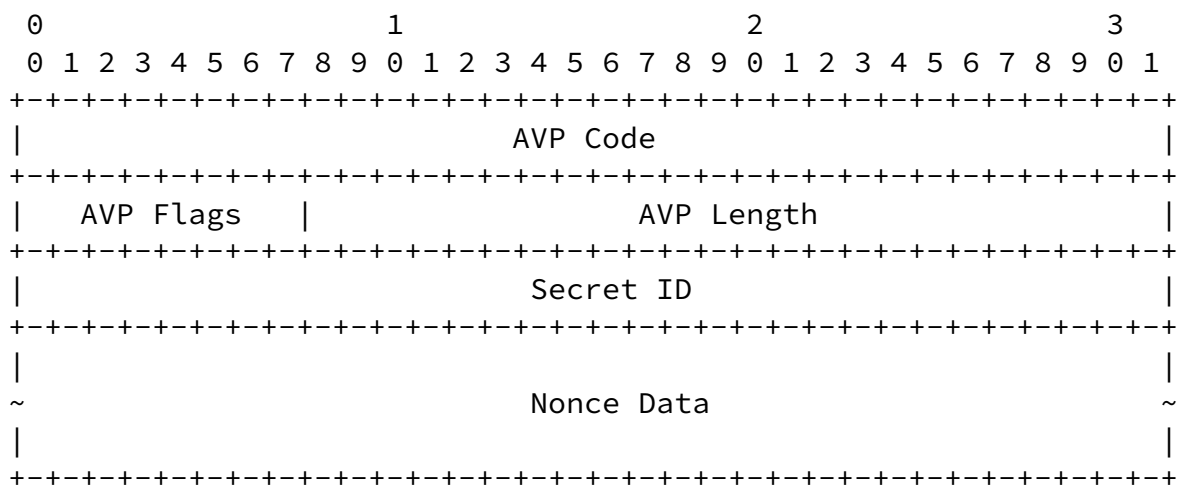
## Bootstrapping [RFC3118](#) using PANA

October 2003

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 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 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 PaC, it may or may not include the AVP in its response depending on its desire to create DHCP SA. 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.



AVP Code

TBD

## AVP Flags

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

```
0 1 2 3 4 5 6 7
+---+---+---+---+
|V M r r r r r r|
+---+---+---+---+
```

M(andatory)

- 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)

Tschofenig et al.

Expires - April 2004

[Page 10]

---

Internet Draft

Bootstrapping [RFC3118](#) using PANA

October 2003

- 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)

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

AVP Length

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

32 bit value that identifies the DHCP Key produced as a result of the bootstrapping process. This value is determined by PAA and sent to PaC. PAA determines this value by randomly picking a number from the available session 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 DHCP SA expires. PaC MUST set this field to all 0s in its response.

## Nonce Data (variable length)

Contains the random data generated by the transmitting entity. This field contains Nonce\_PaC when the AVP is sent by PaC, and Nonce\_PAA 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.

### [6.2](#) Key Derivation

This section describes the key derivation procedure which allows to establish a DHCP security association. The key derivation procedure is reused from IKE [[RFC2409](#)]. The character '|' denotes concatenation.

DHCP Key = HMAC-MD5(MSK, const | Session ID | Nonce\_PaC | Nonce\_PAA)

The values of have the following meaning:

- MSK

The Master Session Key (MSK) is provided by the EAP method as part of the PANA/EAP protocol execution.

- const

This is a string constant. The value of the const parameter is set to "PANA [RFC3118](#) Bootstrapping".

- Session ID

This is the PANA session ID as defined in [[PANA](#)]. It is used to identify a unique session between the PaC and PAA.

- Nonce\_PaC

This random number is provided by the PaC and exchanged within the PANA protocol.

- Nonce\_PAA

This random number is provided by the PAA/DHCP server and exchanged with the PANA protocol.

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 Transient Session Keys (TSKs).

When PAA and DHCP server are not co-located, the DHCP SA information is carried from the PAA (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.

```

+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+
| SubOpt Code | Length | Secret ID | ~ |
+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+
~ Secret ID (continued) | |
+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+
| |
+ |
| |
+ DHCP Key |
| |
+ +-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+
Tschofenig et al. Expires - April 2004 [Page 12]

```

Secret ID

This is the 32-bit value assigned by the PAA which is used to identify the DHCP key.

DHCP Key

128-bit DHCP key computed by PAA is carried in this field.

Lifetime

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

7. Example message flow

Figure 2 depicts a message flow that enables DHCP bootstrapping. The PANA message flow starts with a discovery of the PAA, followed by network access authentication. Finally, when the authentication succeeds a PANA security association is established. The DHCP-AVP payload contains parameters described in [Section 6](#).

PaC	PAA	Message(tseq,rseq) [AVPs]
-----		
----->		PANA-PAA-Discover(0,0)
<-----		PANA-Start-Request(x,0) [Cookie]
----->		PANA-Start-Answer(y,x) [Cookie]
<-----		PANA-Auth-Request(x+1,y) [Session-Id, EAP{Request}]
----->		PANA-Auth-Answer(y+1,x+1) [Session-Id, EAP{Response}]
	.	
	.	
<-----		PANA-Auth-Request(x+n,y+n-1) [Session-Id, EAP{Request}]
----->		PANA-Auth-Answer(y+n,x+n)
Tschofenig et al.		Expires - April 2004
		[Page 13]

	[Session-Id, EAP{Response}]
<-----	PANA-Bind-Request(x+n+1,y+n) [EAP{Success}, Session-Id, Device-Id, DHCP-AVP, Lifetime, MAC]
----->	PANA-Bind-Answer(y+n+1,x+n+1) [Session-Id, Device-Id, DHCP-AVP, MAC]

Figure 2: Message flow for PANA DHCP bootstrapping

PANA SA will be created based on the PANA authentication. Since PaC and PAA have exchanged DHCP-AVPs, additionally a DHCP SA will be generated as outlined earlier. DHCP SA parameters can be immediately provided to the DHCP server when PAA and DHCP server are co-located. When they are on separate nodes, the next DHCP request sent by the DHCP client (PaC) can piggyback the DHCP SA parameters to the DHCP server as it is relayed by the DHCP relay (PAA).

## 8. Security Considerations

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

PANA uses EAP to support a number of authentication methods. With the functionality of EAP this document therefore supports DHCP security for roaming users.

This document separates the different security mechanisms in a modular way:

- a) The appropriate EAP method for a certain scenario, environment or architecture can be chosen. The security properties heavily depend on the chosen EAP method.
- b) PANA carries EAP messages and provides additional security. The security features of PANA are described in [[PANA](#)].
- c) The security mechanism in [[RFC3118](#)] is reused for providing authentication, integrity and replay protection for DHCP messages.

If the PAA 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 PAA 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 [AS+03]). Figure 3 is taken from [Section 4.1](#) of [AS+03] and adjusted accordingly. A major difference from [AS+03] is that the communication between the PAA and DHCP server takes place within the same administrative domain. Hence the security



Secondly, even after DHCP client and DHCP server acquire the DHCP key, the PAA host continues to be on the DHCP path when acting as a DHCP relay.

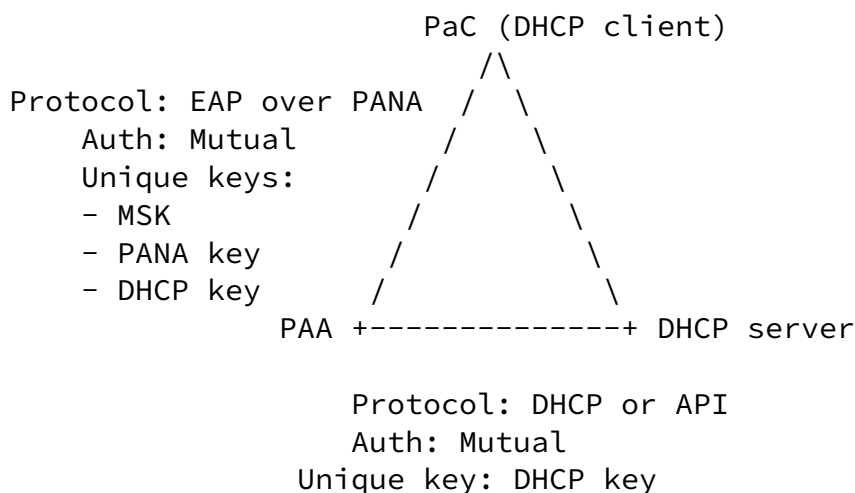


Figure 3: Keying Architecture

Figure 3 describes the participating entities and the protocol executed between them. It must be ensured that the derived session key between the PaC and the DHCP server is fresh and unique.

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

- Confidentiality protection
- Replay protection
- Integrity protection

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

Russ Housley recently (at the 56th IETF) presented a list of recommendations for key management protocols which describe requirements for an acceptable solution. Although the presentation focused on NASREQ some issues might also be applicable in our context. We will address the presented issues briefly:

- Algorithm independence

Our proposal bootstraps a DHCP security association based on [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)

PANA relies on EAP to provide strong and fresh session keys for each initial authentication and key exchange protocol run. Furthermore the key derivation function provided in [Section 6.2](#) contains random numbers provided by the PaC and the PAA 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 which is carried over PANA (between the PaC and the PAA) MUST provide a replay protection mechanism.

Additionally random numbers and the session id is included in the key derivation procedure which aims to provide a fresh and unique session key between the PaC (DHCP client) and the DHCP server.

Furthermore, the key transport mechanism between the PAA 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 PaC and the PAA is provided by the PANA protocol which utilizes EAP. Key confirmation of PANA SA is accomplished at the final stage of the PANA exchange.

Key confirmation between the PaC and the DHCP server is provided with the first protected DHCP message exchange.

- Perform authorization

Authorization for network access is provided during the PANA exchange. The authorization procedure for DHCP bootstrapping is executed by the PAA before this service is offered to the PaC. The PAA might choose not to include DHCP-AVP in a PANA-Bind-Request based on its local policies.

- Maintain confidentiality of session keys

The DHCP session keys are only known to the intended parties (i.e., to the PaC, PAA and the DHCP server).

The PANA protocol 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 [[RD03](#)] with non-null IPsec encryption.

- Confirm selection of "best" ciphersuite

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 PAA and DHCP server

A compromised PAA may leak the DHCP session key, the EAP derived session key (e.g., MSK) and the PANA SA. It will furthermore allow corruption of the DHCP protocol executed between the hosts and the DHCP server since PAA node either acts as a DHCP relay or DHCP server.

A compromised PAA may also allow creation of further DHCP SAs or other known attacks on the DHCP protocol (e.g., address depletion).

A compromised PAA will not be able to modify, replay, inject DHCP messages which use security associations established without the PANA bootstrapping protocol (e.g., manually configured DHCP SAs).

On the other hand, a compromised DHCP server may only leak the DHCP key information. MSK and PANA SA will not be compromised in this case.

- Bind key to appropriate context

The key derivation function described in [Section 6.2](#) includes parameters (such as the PANA session ID and a constant) which prevents reuse of the established session key for other purposes. The key derivation includes the session identifier to associate the key to the context of a certain PANA protocol session and therefore to a particular client.

## [9.](#) IANA Considerations

TBD

Tschofenig et al.

Expires - April 2004

[Page 17]

---

Internet Draft

Bootstrapping [RFC3118](#) using PANA

October 2003

## [10.](#) Open Issues

This document describes a bootstrapping procedure for [\[RFC3118\]](#). The same procedure could be applied for [\[DHCPv6\]](#).

Some text is required to describe the details of the DHCP multi-server model. When multiple DHCP servers send DHCP OFFER in response to the DHCP DISCOVER where each server has a distinct server id and the client chooses a single server among multiple DHCP OFFER messages. For the client there is no difference between any of the DHCP server.

## [11.](#) References

[DHCPv6] R. Droms, J. Bound, B. Volz, T. Lemon, C. Perkins and M. Carney: "Dynamic Host Configuration Protocol for IPv6 (DHCPv6)", Internet-Draft, (work in progress), November, 2002.

[PANA] D. Forsberg, Y. Ohba, B. Patil, H. Tschofenig and A. Yegin: "Protocol for Carrying Authentication for Network Access (PANA)", Internet-Draft, (work in progress), March, 2003.

[RFC3118] R. Droms and W. Arbaugh: "Authentication for DHCP Messages", [RFC 3118](#), June 2001.

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

[RFC2408] Maughan, D., Schertler, M., Schneider, M., and J. Turner, "Internet Security Association and Key Management Protocol (ISAKMP)", [RFC 2408](#), November 1998.

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", [BCP 14](#), [RFC 2119](#), March 1997.

[PY+02] Penno, R., Yegin, A., Ohba, Y., Tsirtsis, G., Wang, C.: "Protocol for Carrying Authentication for Network Access (PANA) Requirements and Terminology", Internet-Draft, (work in progress), April, 2003.

[DS02] Droms, R. and Schnizlein, J.: "RADIUS Attributes Sub-option for the DHCP Relay Agent Information", Internet-Draft, (work in progress), October, 2002.

[SL+03] Stapp, M. and Lemon, T. and R. Droms: "The Authentication Suboption for the DHCP Relay Agent Option", Internet-Draft, (work in progress), April, 2003.

[AS+03] Aboba, B., Simon, D., Arkko, J. and H. Levkowitz: "EAP Keying Framework", Internet-Draft, (work in progress), October 2003.

Tschofenig et al. Expires - April 2004

[Page 18]

---

Internet Draft Bootstrapping [RFC3118](#) using PANA

October 2003

[RFC2132] Alexander, S. and Droms, R.: "DHCP Options and BOOTP Vendor Extensions", [RFC 2132](#), March 1997.

[RFC2131] R. Droms: "Dynamic Host Configuration Protocol", [RFC 2131](#), March 1997.

[WH+03] J. Walker, R. Housley, and N. Cam-Winget, "AAA key distribution", Internet Draft, (work in progress), April 2002.

[RFC2548] Zorn, G., "Microsoft Vendor-Specific RADIUS Attributes", [RFC 2548](#), March 1999.

[CFB02] Calhoun, P., Farrell, S., Bulley, W., "Diameter CMS Security Application", Internet-Draft, (work in progress), March 2002.

[RD03] R. Droms: "Authentication of DHCP Relay Agent Options Using IPsec", Internet-Draft (work in progress), August 2003.

[SE03] J. Salowey and P. Eronen: "EAP Key Derivation for Multiple Applications", Internet-Draft (work in progress), June 2003.

## [12](#). Acknowledgments

We would like to thank Yoshihiro Ohba for his comments to this

draft.

### 13. Author's Addresses

Hannes Tschofenig  
Siemens AG  
Otto-Hahn-Ring 6  
81739 Munich  
Germany  
EMail: Hannes.Tschofenig@siemens.com

Alper E. Yegin  
DoCoMo USA Labs  
181 Metro Drive, Suite 300  
San Jose, CA, 95110  
USA  
Phone: +1 408 451 4743  
Email: alper@docomolabs-usa.com

Dan Forsberg  
Nokia Research Center  
P.O. Box 407  
FIN-00045 NOKIA GROUP, Finland  
Phone: +358 50 4839470  
EMail: dan.forsberg@nokia.com

Tschofenig et al.

Expires - April 2004

[Page 19]

---

Internet Draft

Bootstrapping [RFC3118](#) using PANA

October 2003

#### Full Copyright Statement

Copyright (C) The Internet Society (2001). All Rights Reserved.  
This document and translations of it may be copied and furnished to others, and derivative works that comment on or otherwise explain it or assist in its implementation may be prepared, copied, published and distributed, in whole or in part, without restriction of any kind, provided that the above copyright notice and this paragraph are included on all such copies and derivative works. However, this document itself may not be modified in any way, such as by removing the copyright notice or references to the Internet Society or other Internet organizations, except as needed for the purpose of developing Internet standards in which case the procedures for copyrights defined in the Internet Standards process must be followed, or as required to translate it into languages other than English.

The limited permissions granted above are perpetual and will not be

revoked by the Internet Society or its successors or assigns.

This document and the information contained herein is provided on an "AS IS" basis and THE INTERNET SOCIETY AND THE INTERNET ENGINEERING TASK FORCE DISCLAIMS 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.