Bootstrapping Mobile IPv6 using EAP

Julien Bournelle*, Maryline Laurent-Maknavicius*, Gerardo Giaretta†,
Ivano Guardini†, Elena Demaria† and Loris Marchetti†
*GET/INT
9, rue Charles Fourier, 91011 Evry, France
Email: {Julien.Bournelle, Maryline.Maknavicius}@int-evry.fr
†Telecom Italia Lab
274 via G. Reiss Romoli, 10148 Torino, Italy
Email: {Gerardo.Giaretta, Ivano.Guardini, Elena.Demaria, Loris.Marchetti}@tilab.com

***Abstract*— Mobile IPv6 is the protocol defined by the Internet Engineering Task Force (IETF) to enable nodes to roam between IP subnets. Its specification requires the mobile node to be configured with at least a Home prefix to discover a Home Agent Address, a Home Address and the cryptographic materials needed to protect Mobile IPv6 signaling. In a real deployment perspective, manual configuration is cumbersome and a dynamic bootstrapping solution is needed. This is referred to as the Mobile IPv6 bootstrapping problem.**

This paper describes a solution where mobility and network access services are provided by the same entity. Our idea is to use the AAA infrastructure so the authorization and configuration of the mobility service are both performed during the network access authentication phase.

Our solution is based on the Extensible Authentication Protocol (EAP) that usually serves to authenticate users. We solve the bootstrapping problem by using existing extensions of some EAP authentication methods to carry Mobile IPv6 parameters from the home domain to the mobile node. This solution has been implemented in Telecom Italia laboratory.

GLOSSARY

AAA	Authentication Authorization Accounting
AVP	Attribute Value Pair
ASA	Access Service Authorizer
ASP	Access Service Provider
BA	Binding Acknowledgement
BU	Binding Update
CoA	Care-of Address
CN	Correspondent Node
EAP	Extensible Authentication Protocol
HA	Home Agent
HoA	Home Address
IKE	Internet Key Exchange
MN	Mobile Node
MSA	Mobility Service Authorizer
MSP	Mobility Service Provider
SA	Security Association
TLV	Type Length Value

I. INTRODUCTION

New access technologies are currently defined (IEEE 802.11 and 802.16, 3GGP, 3GGP2) and deployed to support ambiant Internet, that is, the possibility for users to get access to the IP network from everywhere. Even if layer two currently offers wireless access supporting user's movement, the IP layer is not adapted to mobility as one IP address always refers to a specific position of the mobile in an IP network and after it moves, the mobile is no longer reachable through the same IP address. To introduce mobility support, the Internet Engineering Task Force (IETF) defined the Mobile IPv6 protocol [1]. As a prerequisite for Mobile IPv6, the mobile node and a special router called home agent are assumed to be preconfigured with necessary parameters. In a real deployment perspective, the manual preconfiguration of these parameters is cumbersome and a dynamic bootstrapping solution is needed.

In this article, we describe the Mobile IPv6 protocol and possible deployment scenarios in section II. We present the Mobile IPv6 bootstrapping problem in section III. This problem may be solved using the AAA infrastructure that operators use to perform customers'authentication, to grant them to some services and to perform accounting. Description of AAA infrastructure is given in section IV. We focus on the integrated scenario where mobility and network access services are provided by the same operator. Our proposal based on the *Extensible Authentication Protocol* [2] is described in section V. Finally, this proposal was implemented at the Telecom Italia Laboratory and the platform is described in section VI.

II. MOBILE IPV6

A. An overview of Mobile IPv6

The *Internet Engineering Task Force (IETF)* defined the Mobile IPv6 protocol to allow IP nodes to roam between different IP subnets while remaining reachable. Moreover Mobile IPv6 supports IPv6 handovers with no disruption of TCP connections. This is possible thanks to the mobile node (MN) having the two addresses (cf. figure 1): a home address (HoA) and a care-of address (CoA). The home address is the address permitting the mobile to be reached whatever its position and which is valid on the home link where a Home Agent (HA) is expected to relay the packets to the current mobile node's location, i.e. its care-of address.

The mobile node sends the *Binding Update* message to inform its home agent (HA) of its current location (CoA). The HA replies with a *Binding Acknowledgement* message to the MN. These two signalling messages must be protected in order to avoid attacks such as traffic redirection. Document [3]

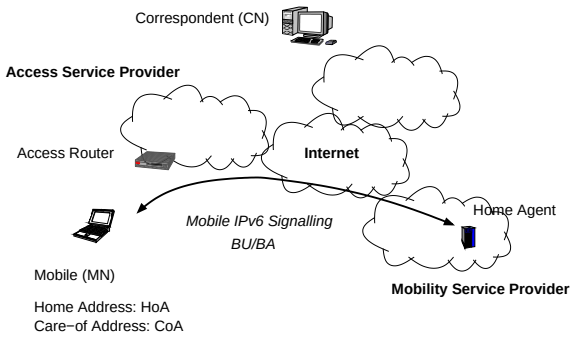

Fig. 1. Mobile IPv6 Architecture

specifies how IPsec may be used for this purpose but a new authentication option is being defined at the IETF (cf. [4]). This new authentication option requires a shared key.

A correspondent node (CN) on the Internet needing to reach the mobile, should send a packet with a destination address set to the mobile's home address. The packet is then intercepted by the HA and tunneled to the CoA. The mobile sends traffic back either using the reverse tunnel through the HA to the CN, or using the Return Routability test for route optimization [1]. In this latter case, the mobile and CN directly exchange IPv6 packets.

B. Mobile IPv6 deployment scenarios

Two deployment scenarios may be considered. Document [5] introduces the following entities: the Access Service Provider (ASP), the Access Service Authorizer (ASA), the Mobility Service Provider (MSP) and the Mobility Service Authorizer (MSA). The ASP affords basic IP services such as address allocation and traffic relay and the MSP manages Mobile IPv6 oriented devices such as home agents to support the mobility service. The ASA and MSA are the entities which authorize related services (i.e. basic Internet Service and Mobility Service). Basically, the Authorizer is the entity with whom the subscriber has a contract. The provider is the entity which provides the service.

In the first deployment scenario, access and mobility service authorizers are integrated, and the operator authorizing network access also authorizes the mobility service. This scenario is known as *Integrated scenario*. This is the scenario that we consider in this proposal.

In the second one, authorizers are separated, that is, the mobile is authorized by ASA to get access to basic IP services, and for access to the IPv6 mobility service, the MSA should be contacted. This means that the user has a separate contract for both services. This scenario, known as *Split scenario*, is not able to combine the authentication phase used for network access with the authorization and configuration for the IPv6 mobility service.

III. The Mobile IPv6 bootstrapping problem

A. Mobile IPv6 parameters

To initialize the Mobile IPv6 service, the mobile node must acquire a home address, a home agent and the necessary

Mobile Node	Home Agent
Home Agent Address	
Home Address	MN's Home Address
MN-HA SA	MN-HA SA

Fig. 2. Mobile IPv6 parameters

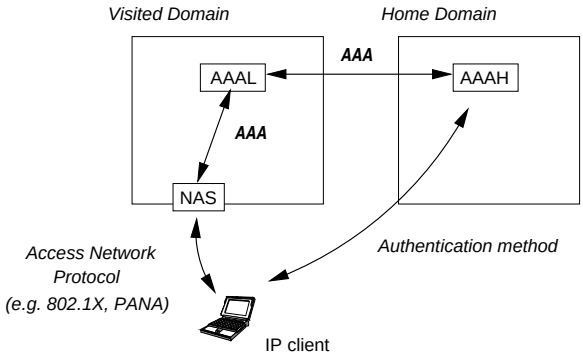

Fig. 3. AAA Infrastructure

security association to protect signalling messages as described in [5]. On the other side, the home agent must share a security association (SA) with the mobile node and must know the associated home address (cf. Fig 2).

B. The Mobile IPv6 bootstrapping problem

As an operator is usually in charge of millions of mobile nodes, manual preconfiguration of the above parameters in the mobile nodes appears as too cumbersome. For instance, for the home address assignement, preconfiguration means that a static home address is assigned to the mobile, it appears as a major constraint since the operator may prefer dynamic allocation. Moreover, a static home address assignement would also force operators to keep corresponding IPv6 prefix available in their networks.

For the home agent address parameter, dynamic assignment is also preferred. As an example, home agents may be shutdown for management purpose. Moreover, an operator may want to perform some load balancing between its differents home agents to enhance reliability and performance of its service. It may also need to redeploy some home agents.

The Mobile IPv6 protocol does not propose any solution to the dynamic configuration problem, despite it appears as a major problem to the real deployment of Mobile IPv6. This problem is known as the *Mobile IPv6 bootstrapping problem*.

IV. Overview of AAA infrastructure

In the *integrated scenario* that we consider in this paper, the basic idea to solve the above bootstrapping problem is to use the AAA infrastructure.

A. The three components of a AAA infrastructure

The AAA infrastructure is used by an operator to authenticate its subscribers, to explicitely authorize them some services and to perform some accounting on rendered services. It can be divided into three major components (cf. Fig. 3):

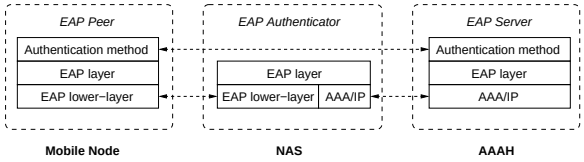

Fig. 4. EAP Architecture

1) The AAA protocol used in the core network. AAA stands for *Authentication, Authorization and Accounting* and is used between the *Network Access Server* (NAS) and AAA servers. The most widely deployed and known AAA protocol is RADIUS [6].
2) The *Access Network Protocol (ANP)* used between the IP client and the NAS. ANPs include PPP, 801.1X, and PANA.
3) The authentication method is the algorithm ran between the IP client and its home AAA server (AAAH). It is usually based on a secret shared between the client and the home operator such as a *login/password*. Some authentication methods support mutual authentication.

Fig. 3 describes the three components in the roaming case. The mobile node requests access to the NAS in the visited domain using the ANP. The NAS forwards the request to its local AAA server (AAAL). Based on the user/device's identity, the AAA server forwards the request to the home AAA server (AAAH) located in the home domain. The authentication method is only implemented in the mobile node and its home AAA server. The ANP and AAA protocols serve to carry authentication parameters during the authentication phase. Depending on the result of the authentication, the AAA server grants access to the mobile node and may configure some services such as QoS. The IETF recently designed a new AAA protocol called Diameter.

B. An overview of EAP

An operator uses an authentication method to authenticate its subscribers. The *Extensible Authentication Protocol (EAP)* is defined in RFC 3748 [2] as an authentication framework which supports various authentication methods.

Fig. 4 presents the basic architecture of EAP. The EAP peer is located in the client; the EAP authenticator is within the NAS and the EAP server is located in the AAA server. The authentication method is encapsulated and decapsulated by the EAP layer. The EAP lower-layer is the protocol used to carry EAP packets between the EAP peer (client) and the EAP authenticator (NAS). The latter uses a AAA protocol such as RADIUS [7] or Diameter [8] to exchange EAP packets with the EAP server. Thus, the NAS does not know the authentication methods. It only serves as an EAP relay between the client and the server.

Depending on the authentication method, some keys may be derived at the EAP peer and server. Document [9] describes the framework for the generation and management of these keys within the EAP architecture. One interesting feature is that the EAP peer and server can derive a key called *AAA-Key* which can be sent to the EAP authenticator. From this key, the client and the NAS can derive new keys used to protect the EAP lower-layer.

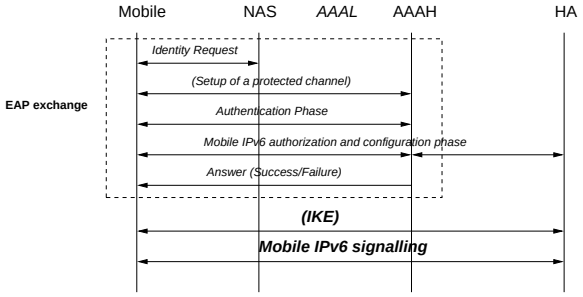

Fig. 5. EAP to bootstrap Mobile IPv6 service messages flow

V. Use of EAP for Mobile IPv6

EAP is an efficient protocol designed to manage authentication methods (cf. section IV-B). It is a two-party protocol used between the EAP peer (located in the mobile node) and the EAP server (located in the home AAA server). For this reason, the NAS does not need to be modified even if authentication methods change. Moreover some existing ANPs such as 802.1X and PANA already use it for network access authentication. Our proposal is to use EAP to solve the bootstrapping problem by carrying needed mobility parameters in the EAP exchange.

A. Requirements for EAP authentication methods

Our solution based on EAP to bootstrap Mobile IPv6 parameters provides an explicit authorization of the Mobile IPv6 service, a dynamic allocation of home agent to the mobile and a dynamic parameters configuration.

We propose to introduce extra exchanges into the EAP authentication phase for mobility configuration purpose. This implies that the selected authentication method must support the exchange of general purpose configuration parameters. Some of the existing methods already provide this feature by defining *Type-Length-Value (TLV)* or *Attribute Value Pair (AVP)* information being embedded into existing EAP packets. Note that EAP only defines four types of packets: `EAP-Request`, `EAP-Response`, `EAP-Success` and `EAP-Failure`. The encapsulation of TLVs or AVPs in EAP message permits to directly exchange arbitrary parameters between the EAP peer (mobile) and its EAP server (AAAH). Moreover, some of the authentication methods, such as PEAPv2 [10], provide a native support for encryption, authentication and integrity protection of exchanged configuration data. This means that the mobility parameters will be securely transmitted to the mobile.

B. Protocol details

Fig. 5 presents the messages of our proposal. The bootstrapping processing may be divided into the following steps:

1) When the mobile enters in an IP network using EAP for access control, it first discovers the NAS (which hosts

an EAP authenticator and a AAA client). This discovery phase is handled by the EAP lower-layer such as 802.1X or PANA. Then, the mobile is polled for its identity using EAP Request Identity message. The mobile provides its *Network Access Identifier (NAI)* (e.g. user@realm) to the NAS within an EAP-Response Identity message. The NAS (AAA client) forwards the response to the local AAA server within a AAA message. As the NAI contains the realm of the mobile, the AAAL is able to route the message to the AAAH (eventually through a AAA broker). Depending on the user's profile, the AAAH chooses an EAP authentication method. If the profile indicates that this user may want to become mobile, it chooses an adequate authentication method (i.e. supporting exchange of arbitrary parameters). The AAA message sent by the AAAH to the NAS through the AAAL contains the EAP Request packet indicating the method. This EAP request packet is forwarded to the mobile by the EAP lower-layer.

2) After this handshake, the mobile and the AAAH server enter in the authentication phase. Depending on the chosen authentication method, they may setup a protected channel. As an example, PEAPv2 provides a channel protected by TLS. This channel provides privacy and integrity protection to subsequent EAP exchanges.
3) The authentication phase uses this protected channel. It may require various exchanges. The number of exchanges depends on the chosen method.
4) After the authentication phase, the AAAH server affords to configure the mobility service for the user. All the subsequent messages to configure the mobility are encoded in EAP TLVs or AVPs which are embedded within a generic Mobile IPv6 TLV/AVP container. Depending on the implementation at the mobile side, the mobility service may be prompted to the user. The mobile answers with needed parameters. The AAAH server possibly selects a home agent and then interacts with it to obtain and configure the necessary parameters. The interaction between AAAH and HA is discussed in section V-C .
5) While completing the HA configuration, the AAAH provides the mobile with all the Mobile IPv6 configuration data through the EAP exchanges. For that purpose, an EAP-Request is sent by AAAH containing the generic Mobile IPv6 TLV/AVP container. This TLV/AVP container includes sub-TLV/AVPs: Home-Address-TLV/AVP, Home-Agent-Address-TLV/AVP, IKE-bootstrap-Information-TLV/AVP and an Authorization-Lifetime-TLV/AVP. The mobile then sends back an EAP-Response stating whether the parameters negotiation is accepted, denied or if it needs renegotiation.
6) Finally, the mobile knows the required information to bootstrap Mobile IPv6; it is also authorized to get access to the network and to use Mobile IPv6.

After completion of the EAP exchanges, the mobile gets a care-of address using the stateless autoconfiguration [11] or the stateful approach based on DHCPv6. Then IKE may be used to setup IPsec Security Associations with the HA according to the specification [3]. If the authentication option is used instead of IKE, the mobile obtains the corresponding key.

As soon as the mobile shares a security association, it sends a *Binding Update* message to the allocated HA. The HA responds with a *Binding Acknowledgement* indicating the result of the binding. At the end of this exchange the mobility service is operational.

C. AAA-HA interaction

After the authentication phase, the AAA server communicates with the allocated home agent. During this phase, the AAA server sets some configuration data and retrieves some others. SNMPv3, COPS or even a new Diameter application are possible candidates for this. Note that the protocol used between the AAA server and the home agent is independent of our solution. However, the protocol should have the following features:

- *Use of Network Access Identifier (NAI)*: the AAA server should be able to use the NAI as the mobile node's identifier.
- *Setting Authorization Lifetime*: the AAA server should be able to setup an authorization lifetime for the allocated session to the mobile node.
- *Home Address configuration*: the AAA server should be able to query the home agent to allocate a home address for a particular mobile node.
- *Explicit Termination of a Mobile IPv6 session*: the AAA server should be able to explicitly terminate session for a particular mobile node.
- *Provide security parameters*: to configure IPsec or to setup the authentication option, the AAA server may need to provide cryptographic material to the HA. This implies a strong relationship between AAA and HA. Moreover, these parameters need to be securely transferred from the AAA to the HA.

Securely providing parameters from the AAA to the HA introduces the following security requirements:

- The AAA server and the HA must authenticate each other in order to avoid impersonation.
- Exchanged parameters must be integrity protected to avoid alteration of information.
- The protocol used between AAA and HA must provide replay protection.
- The protocol must also provide confidentiality to protect security parameters sent from the AAA server to the HA.

The AAA-HA interface is an important piece of the whole architecture. One of the next steps of our proposal is to correctly identify the protocol which does best suit the above requirements.

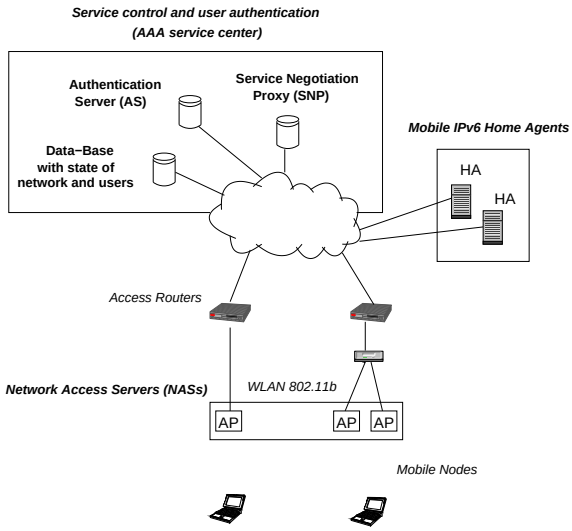

Fig. 6. - *Blinded* - platform architecture

VI. Telecom Italia Laboratory Platform

An experimental solution for Mobile IPv6 authorization and configuration has been implemented at Telecom Italia Laboratory premises. The overall platform architecture is depicted in Fig. 6.

Since the authentication phase occurs once, we consider that the extra delay introduced for the Mobile IPv6 bootstrapping is not relevant and thus we do not provide any measures.

The access infrastructure is a Wireless LAN compliant to the IEEE 802.11b standard. In order to gain access to the network the WLAN, terminals are required to undertake an authentication phase based on EAP. The TILab prototype is based on PEAPv2, a tunneled EAP method supporting the exchange of general purpose configuration parameters. In PEAPv2, the conversation between the terminal (i.e. EAP peer) and the AAA server (i.e. EAP backend authentication server) is encrypted, authenticated, integrity and replay protected within a TLS channel.

As a whole, the network elements that build the Telecom Italia platform are the following:

- Terminals (or Mobile Nodes): laptops equipped with a Wireless LAN NIC conformant to the IEEE 802.11b standard. Each terminal supports Mobile IPv6 thanks to the MIPL 2.0 rc1 software (Mobile IPv6 for Linux). It plays the role of IEEE 802.1X supplicant. The software client implementing the IEEE 802.1x supplicant is Xsupplicant 1.0. The employed EAP methods (i.e. PEAPv2 and MSCHAPv2), have been extended to support dynamic Mobile IPv6 authorization and configuration, these methods are provided in the Xsupplicant package.
- Wireless LAN Access Points (APs): standard (commercially available) IEEE 802.11b APs playing the role of IEEE 802.1X EAP authenticators and AAA clients. The APs are the NASes responsible for checking the user credentials, through the AAA infrastructure, and enforcing the correspondent authorization policies;
- Access Routers: standard (commercially available) IPv4/IPv6 routers;
- Service Negotiation Proxy (SNP): AAA server working as EAP backend authentication server for PEAPv2 (i.e. outer EAP method). SNP works as AAA proxy for the inner EAP method and interacts with the MN and the HA to control all the phases of the Mobile IPv6 authorization and configuration procedure. These functionalities are based on the FreeRADIUS package available on April 2nd, 2004;
- Authentication Server (AS): AAA server working as EAP backend authentication server for the inner EAP method (i.e. MSCHAPv2). AAA functionalities are provided by FreeRADIUS. The PEAPv2 implementation has been modified to support this proposal;
- Home Agents: Mobile IPv6 HAs extended with the capability to interact with the SNP to achieve dynamic Mobile IPv6 authorization and configuration, for this purpose FreeRADIUS has been used;
- Data-Base: MySQL data-base where all the service profiles, and the current status of network and users, are stored.

VII. Conclusion

This paper proposes an optimized approach to the Mobile IPv6 bootstrapping problem for operators offering both IP network access and IP mobility service. This solution assumes that the operator uses EAP as the mechanism to authenticate subscribers querying network access. EAP is particularly interesting as some EAP authentication methods provide the facility to carry arbitrary parameters between the EAP client (Mobile Node) and the EAP server (home AAA server). Moreover, these methods usually ensure the security of the transferred parameters (integrity protection, confidentiality and per-packet authentication). As such, this particular feature is used to securely push Mobile IPv6 parameters from the home domain to the mobile node.

In the proposed solution, the Mobile IPv6 service within the mobile is configured after the EAP authentication phase. The home AAA server first allocates and configures a home agent for a specific mobile node, and, the home AAA server then provides parameters to the mobile node. In the final EAP exchanges, the mobile node is authenticated and authorized for IP network access and Mobile IPv6 service.

This proposal was implemented at Telecom Itala Laboratory and the mobile node is correctly configured during the authentication phase. One of the great advantage of this solution is its ease of deployment since the IP operator does not need to change its NAS.

Acknowledgements

Authors address their special thanks to the members of the IETF mip6 working group for the beneficial discussions within the area of Mobile IPv6 bootstrapping.

Authors would also address their thanks to Thierry Ernst (Keio University) and Saber Zrelli (Japan Advanced Institute of Science Technology) for careful review of this document.

GET/INT also addresses thanks to Mr Jean-Michel Combes (France Telecom R&D) for his valuable technical advices and his financial support.

REFERENCES

[1] D. Johnson, C. Perkins, and J. Arkko, "Mobility Support in IPv6," RFC 3775, June 2004.

[2] B. Aboba, L. Blunk, J. Vollbrecht, J. Carlson, and H. Levkowetz, "Extensible Authentication Protocol (EAP)," RFC 3748, June 2004.

[3] J. Arkko, V. Devarapalli, and F. Dupont, "Using IPsec to Protect Mobile IPv6 Signaling between Mobile Nodes and Home Agents," RFC 3776, July 2003.

[4] A. Patel, K. Leung, M. Khalil, H. Akhtar, and K. Chowdhury, "Authentication Protocol for Mobile IPv6," draft-ietf-mip6-auth-protocol-04.txt, February 2005.

[5] A. Patel, "Problem Statement for bootstrapping Mobile IPv6," draft-ietf-mip6-bootstrap-ps-01.txt, October 2004.

[6] C. Rigney, A. Rubens, W. Simpson, and S. Willens, "Remote Authentication Dial In User Service," RFC 2865, June 2000.

[7] B. Aboba and P. Calhoun, "RADIUS support for EAP," RFC 3579, June 2003.

[8] P. Eronen, T.Hiller, and G. Zorn, "Diameter Extensible Authentication Protocol (EAP) Application," draft-ietf-aaa-diameter-eap-04.txt, February 2004, work in progress.

[9] B. Aboba, D. Simon, J. Arkko, , P. Eronen, and H. Levkowetz, "Extensible Authentication Protocol (EAP) Key Management Framework," draft-ietf-eap-keying-06.txt, April 2006, work in progress.

[10] A. Palekar, D. Simon, J. Salowey, H. Zhou, G. Zorn, and S. Josefsson, "Protected EAP Protocol (PEAP) Version 2," draft-josefsson-pppext-eap-tls-eap-10.txt, October 2004, work in progress.

[11] S. Thomson and T. Narten, "IPv6 Stateless Address Autoconfi guration," RFC 2462, December 1998.