Credential and Provisioning
(Enroll)
Internet-Draft
Expires: January 19, 2006

H. Tschofenig
Siemens
G. Giaretta
TILab
A. Gomez-Skarmeta
University of Murcia
J. Polk
Cisco
July 18, 2005

Enriching Bootstrapping with Authorization Information
draft-tschofenig-enroll-bootstrapping-saml-01.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 19, 2006.

Copyright Notice

Copyright (C) The Internet Society (2005).

Abstract

Bootstrapping refers to the process of creating state (typically security associations) between two or more entities based on a trust relationship between these two or more parties AND a trusted third

party. Some work has been done in the area of bootstrapping in the IETF recently. So far, the focus was on creating security associations. This document aims to attach authorization information to the bootstrapping process.

Table of Contents

1. Introduction and Problem Statement

Some work has been done in the area of bootstrapping in the IETF recently. The goal of bootstrapping is to create state (typically security related information such as security associations) between two or more entities. We focus on the two party case and call them Alice and Bob. To securely establish state is simple if (a) Alice and Bob share some information to protect the signaling exchange (e.g., shared secret or the ability to verify a digital signature) and (b) if they are able to authorize the other party. The following statements describe (a) the problem of key management and (b) addresses an important aspect in real world deployments - authorization.

Hence, to develop a satisfactory bootstrapping solution it is necessary to solve these two aspects:

- In order to solve the key management problem, a number of mechanisms have been introduced including bootstrapping mechanisms. For example, [9] and [10] give an overview of bootstrapping (and imprinting) and describe protocol and architectural considerations. Moreover, the problem of bootstrapping is a hot topic in MIP6 WG: for a Mobile IPv6 bootstrapping problem statement see [11]. Several solutions have also been proposed so far: some of them, such as [12] and [13], exploit the authentication and protocol exchanges performed by the mobile node for network access (e.g., PANA, EAP) in order to bootstrap a Mobile IPv6 security association with the HA: in this way, to bootstrap a MIPv6 SA no other authentication phase is needed. Other solutions are completely independent from network access authentication: for example, [14] proposes to use IKEv2, while with [15] a MIPv6 security association for [16] is created using PANA [1]. Finally, a solution for bootstrapping a DHCP RFC 3118 [17] security association using EAP/PANA was specified in [18] and in [19] and a proposal to bootstrap a Kerberos Ticket Granting Ticket based on a successful EAP protocol exchange is

provided in [20]. Recently, two further contributions [21] and [22] were published that aim to reuse EAP for the purpose of bootstrapping information.

- The aspect of authorization has received little attention in the existing literature. Its importance has been discovered during the work on the EAP keying framework [23] document but does not go beyond investigating information carried by AAA protocols. Actually, the authentication and the implicit authorization performed through a pre-shared key or a key management protocol may not be sufficient to conclude that a node (a user) is authorized for a particular service. Considering the case of

Mobile IPv6 service as an example, the fact that the MN shares a pre-shared key with the Home Agent and is able to setup an IPsec Security Association to protect Mobile IPv6 signaling does not imply that it is authorized to provide the Mobile IPv6 service. For example, the Mobility Service Provider (MSP) might want to prevent the usage of MIPv6 if the credit of the MN is going to exhaust or based on the time of the day. This implies that solving the key management problem is not enough to bootstrap a service: a mechanism to explicitly authorize the user is needed to design a bootstrapping solution.

This document describes a "single sign-on" framework that addresses these issues through the usage of EAP and the AAA infrastructure of the involved service providers (i.e., the home and the visited service providers). This framework does not depend on a particular EAP method, the EAP lower layer, the AAA protocol used. Several mechanisms can be used to carry authorization data, such as Diameter, PANA or EAP.

This document addresses authorization by utilizing capabilities of the Security Assertion Markup Language (SAML). For details about SAML see [2], [3] and [24]. Please note that it would be possible to use other languages for describing authorization capabilities as well, such as SPKI [25] or X.509 Authorization Certificates [26].

Based on the previously published solution, it can be seen that the Extensible Authentication Protocol (EAP) [4] plays an important role in a bootstrapping solution since

- it provides support for multiple authentication and key exchange protocols.

- allows three entities to be involved (EAP peer, EAP server and the Authenticator).

- extensively deployed in the context of operational environments.

As a protocol between the Authenticator and the EAP server RADIUS [5] and DIAMETER [6] are important to complete the architecture.

The manage of the authorization process related to the bootstrapping is being considered as an important aspect of the services deployment within the next generation networks. In this context, this document aims to describe how the SAML could be used to provide the user consumer of a service of the material needed to access in a secure way the services and to link it with the permission and grants associated to the user.

2. Terminology

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in [7].

3. Framework

This section illustrates the bootstrapping framework and the involved entities. The framework is based on a single sign-on paradigm: a first authentication and authorization protocol exchange is exploited to exchange general authorization data and to bootstrap subsequent security associations and services. The framework is independent from the container used to carry the needed authorization data; however, in this draft the usage of SAML has been taken into account, since it offers several advantages such as extensility, flexibilty etc.,

Figure 1 shows the entities typically involved in bootstrapping.

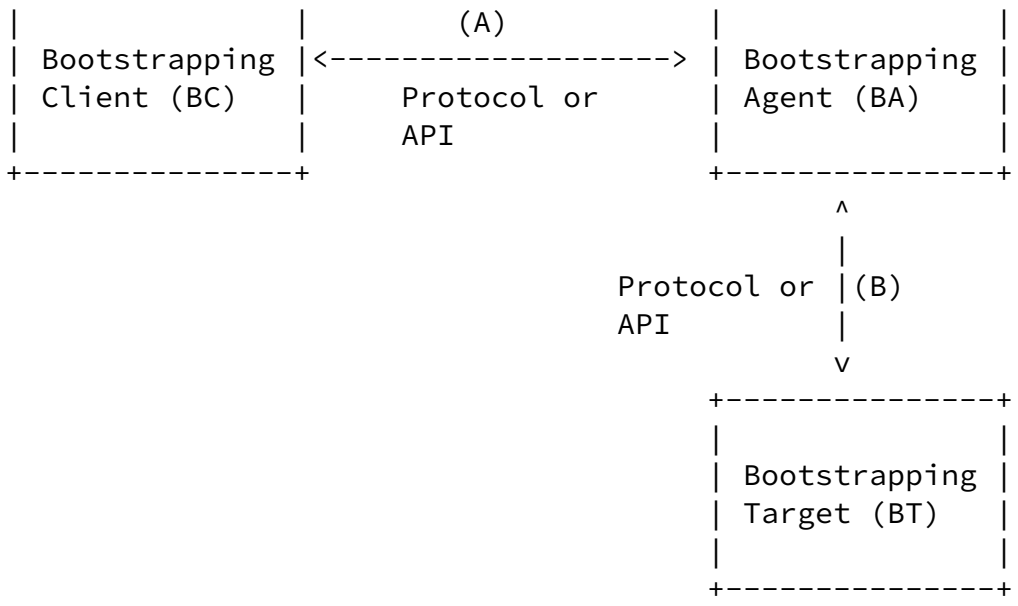


Figure 1: Bootstrapping Framework

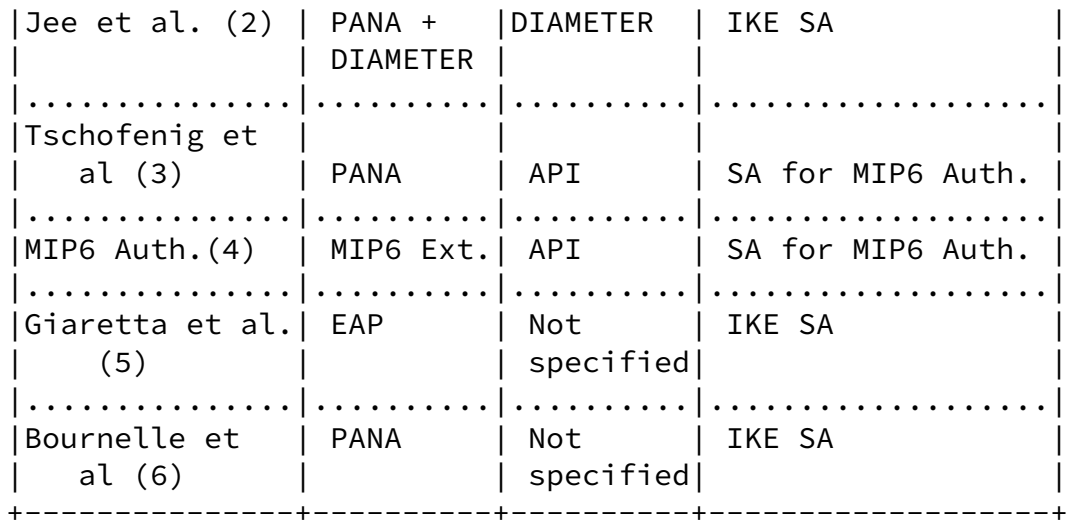
Existing bootstrapping proposals nicely fit into this architecture. Below, we provide an attempt for classification based on the following distinguishing properties:

- Which protocol is used between the BC and the BA?
- Which protocol is used between the BA and the BT?
- What information is bootstrapped?

Ideally, a generic bootstrapping protocol would provide enough flexibility for bootstrapping a variety of (bootstrapping) data items.

As an example, we list a few proposals and show their properties in the subsequent table below:

Proposal	BC<->BA	BA<->BT	Bootstrapped Info
IKEv2 (1)	IKEv2	API	IPsec SAs



where (1) refers to [27], [14] and also to , (2) refers to [12], (3) refers to [15], (4) refers to [16], (5) refers to [13] and (6) refers to [28]. It is a matter of taste to call [27] or [16] a bootstrapping protocol.

The bootstrapping framework, shown in Figure 1, can nicely be mapped to the Authorization Framework shown in Figure 3. The Bootstrapping client corresponds to the entity that is used to request the assertion/artifact, the Bootstrapping Agent can be related to the Assertion Granting Entity and the Assertion Verifying Entity corresponds to the Bootstrapping Target.

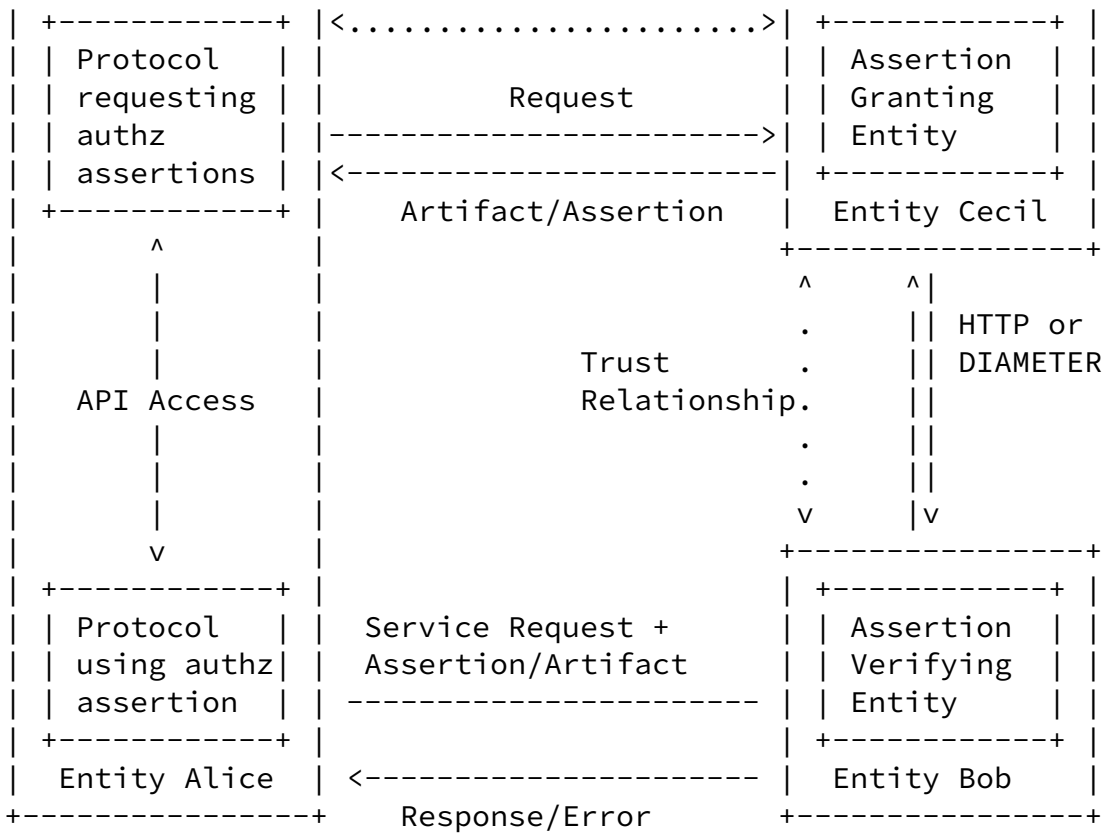


Figure 3: Authorization Framework

When Alice is successfully authenticated and authorized by Bob, he receives the Artifact either via PANA, IKEv2 or any other protected channel established via certain EAP methods. Alice might want to make the Artifact available to other protocols. When Alice wants to make a service request with Bob then the Artifact is attached. Bob will need to interact with Cecil in order to fetch the Assertion. Bob might want to use DIAMETER to fetch the Assertion and to execute functions such as accounting and credit control. DIAMETER is particularly attractive if keying material needs to be distribtued to create a security association between Alice and Bob to secure subsequent communication. If the establishment of keying material is not important then other mechanisms (such as HTTP) could be used.

4. Scenarios

The content of this section is partially based on [29] which addresses trait-based authorization in SIP. This document has a strong relationship with [29] but aims to be more generic (instead of focusing on SIP). Furthermore, Section 4.1 borrows also from [30] and from [31].

Two scenarios are meant to illustrate the functionality of SAML for authorization in combination with bootstrapping. First, we describe how authorization in a QoS signaling environment can be used and then we illustrate a SIP service authorization example.

4.1 Authorization in QoS signaling protocols

Cryptographic computations are expensive and computing authorization decisions might require a lot of time and also requires multiple messages between the entity enforcing the decisions and the entity computing the authorization decision. Particularly, in a mobile environment these entities are physically separated - or not even in the same administrative domain. Accordingly, the notion of "single sign-on" is another potential application of authorization assertions, and trait-based authorization - a user is authenticated and authorized through one protocol, and can reuse the resulting authorization assertion in other, unrelated protocol exchanges.

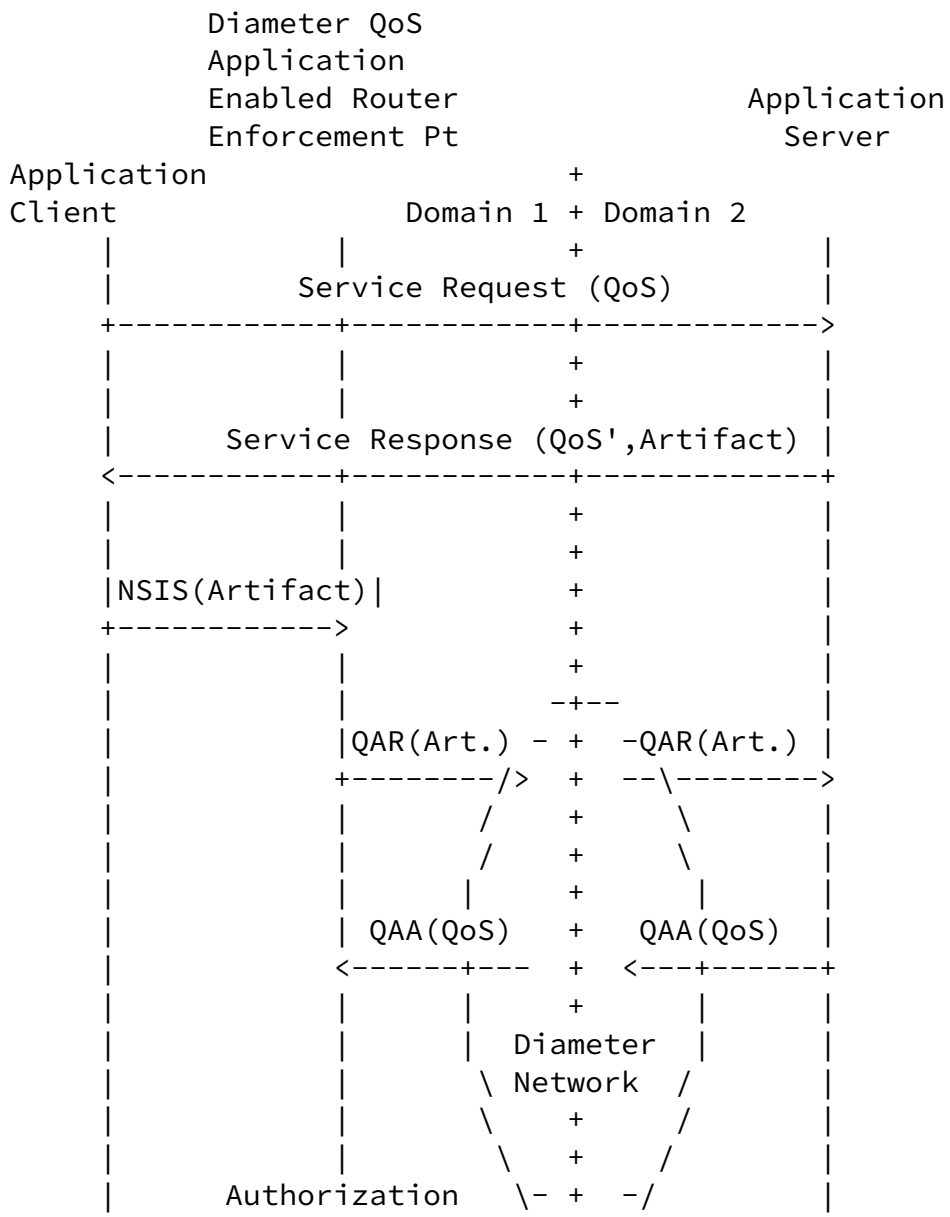
For example, in some environments it is useful to make the authorization decision for a "high-level" service (such a voice call). The authorization for the "voice call" itself might include authorization for SIP signaling and also for lower level network functions, for example a quality-of-service (QoS) reservation to improve the performance of real-time media sessions established by SIP. Since the SIP signaling protocol and the QoS reservation protocol are totally separate, it is necessary to link the authorization decisions of the two protocols. The authorization decision might be valid for a number of different protocol exchanges, for different protocols and for a certain duration or some other attributes.

To enable this mechanism as part of the initial authorization step, an authorization assertion is returned to the end host of the SIP UAC (cryptographically protected). If QoS is necessary, the end host might reuse the returned assertion in the QoS signaling protocol. Any domains in the federation that would honor the assertion generated to authorize the SIP signaling would similarly honor the use of the assertion in the context of QoS. Upon the initial

generation of the assertion by an authorization server, traits could be added that specify the desire level of quality that should be

granted to the media associated with a SIP session.

The message flow shown in Figure 4 illustrates such an exchange where a client (such as a SIP user agent) uses some signaling exchange which allows the end host to obtain an Artifact. This is Artifact is later used as an input for a QoS signaling protocol and provides client authorization. The QoS aware router can either process the request locally or use the Diameter QoS application for verifying the authorization decision at the entity which created the Artifact. In order to perform the processing locally, it is required to obtain an Assertion rather than an Artifact (which is not further illustrated in Figure 4). The DIAMETER QoS application contacts the Application Server to obtain the Assertion, to authorize the request and to start accounting.


Diameter QoS
Application
Enabled Router
Enforcement Pt
Application
Server
Application
Client
Domain 1
Domain 2
Service Request (QoS)
Service Response (QoS',Artifact)
NSIS(Artifact)
QAR(Art.)
QAR(Art.)
QAA(QoS)
QAA(QoS)
Diameter
Network
Authorization

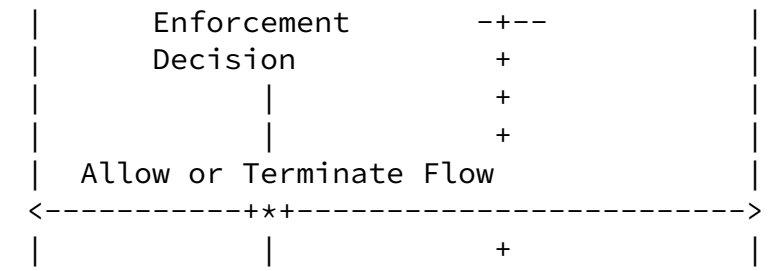
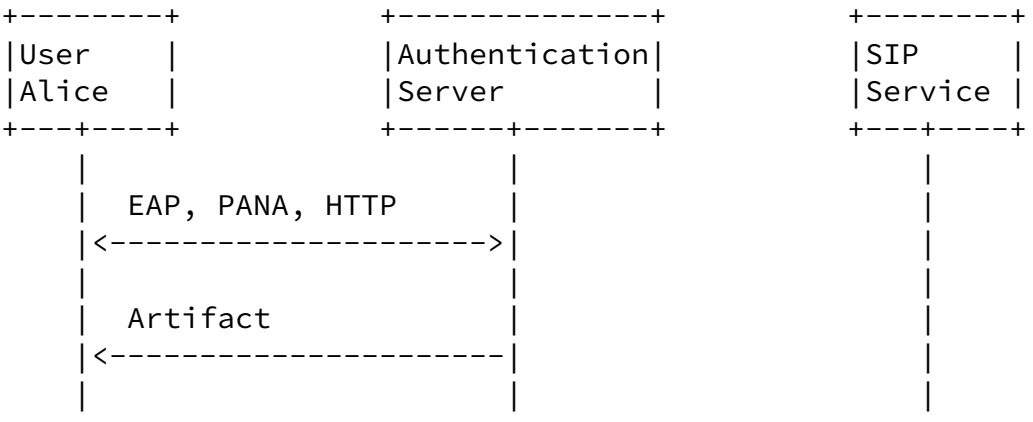


Figure 4: Message flow with NSIS and Diameter QoS Application

4.2 SIP Service Bootstrapping

This scenario exploits the inclusion of SAML for SIP which has been introduced with [32].

In Figure 5, user Alice runs a protocol with an Authentication Server whereby authentication and authorization is provided. This protocol exchange might be based on a number of protocols, such as EAP, PANA, HTTP or something similar. It is not required that the authentication and key exchange protocol terminates at this entity but the Artifact is created and returned the user (based on a successful protocol execution). When a SIP message (e.g., an INVITE) is sent towards a SIP Server or even to another SIP UA then the Artifact is attached to the SIP message. As shown in Figure 5 the SIP service contacts the Authentication Server (for example via DIAMETER) to request the Assertion. This message exchange also allows the SIP service to obtain keying material.



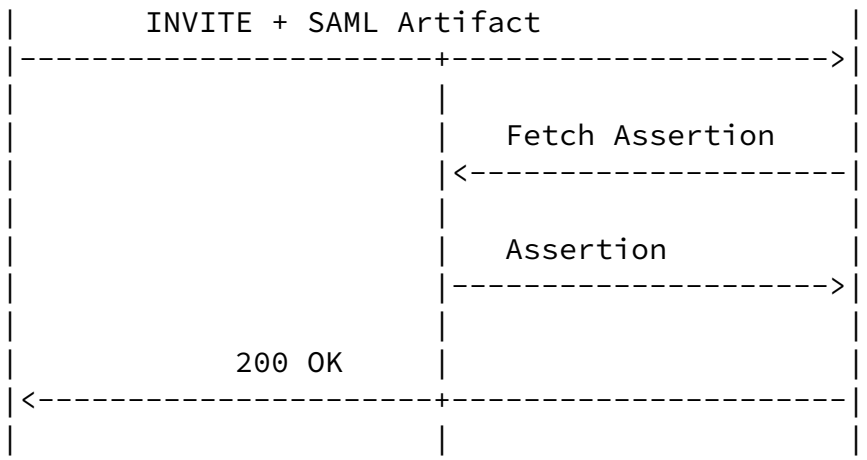


Figure 5: Message flow for SIP service authorization

5. Obtaining a SAML Artifact/Assertion

This section describes how an end host obtains an Artifact via PANA or EAP which subsequently be used for service authorization. Depending on whether the home network or the visited network should create an Assertion/Artifact EAP and/or PANA will be used. If for example, services in the visited network should be authorized then an entity in the visited network should create the Assertion/Artifact and it will be returned via PANA to the end host.

It is not suggested to exchange a SAML Assertion either via EAP or via PANA. An Assertion is an XML document which is, for security reasons, digitally signed. Both PANA and EAP/EAP methods suffer from size limitations. EAP and most EAP methods do not support fragmentation. PANA should avoid IP layer fragmentation.

A number of mechanisms exist to fetch an Assertion with the help of an Artifact. HTTP is the most common mechanisms. This document also

suggests to use DIAMETER to assist in this step since it additionally allows to distribute previously created keying material, to benefit from accounting extensions [33] and other DIAMETER applications such as Credit Control [34].

EDITOR's Note: A "notification" mechanism might be useful to indicate that the user wants to obtain an Artifact (or that the server does not provide this extension).

5.1 SAML Artifact transport in EAP methods

Currently, there are a number of EAP authentication methods that have the capability to convey generic information items (e.g., PEAPv2 [35], EAP-PSK [36] or EAP-IKEv2 [37]). In fact they are being used to send additional information during authentication process inside a protected channel between an EAP peer and the authenticator or between the EAP peer and the EAP server in the case authenticator is acting as a pass-through. This capability is, for example, being considered to transport MIPv6 authorization data [13]. Following this approach, a SAML artifact could be conveyed within an EAP method (by creating another payload/AVP that carries this information).

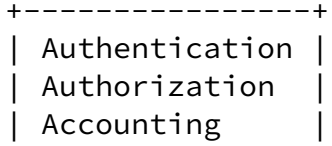
5.2 SAML Artifact transport in PANA

Another alternative, that would allow to use EAP methods that are not able to transport generic information (e.g., EAP-TLS [38]), is to use PANA protocol to convey authorization information (SAML artifact) from the PANA Authentication Agent (PAA) to the PANA Authentication Client (PaC). The usage of PANA provides more flexibility with respect to the entity creating the artifact and the bootstrapped

service. This circumstance is shown in Figure 6. The PANA protocol is used between the PAA and PaC. It might be necessary that a AAA server is contacted. EAP is carried inside PANA and might then again be encapsulated into a AAA protocol such as RADIUS or DIAMETER (see [39] and [40]). AAA interaction with EAP is typically the case if a user roams to a visited network and the EAP method runs between the EAP peer and the EAP server (whereby the EAP server is at the user's home network). The service which will be later used might be at a different administrative domain. The service could be at the visited network, at the home network or at any other network. To allow bootstrapping to work, it is necessary to have an existing trust

relationship between the entity that created the SAML assertion and the service which will later use it. DIAMETER might be used between these two entities to transfer keying material (and other information).

If PANA terminates at the first hop router, as proposed in [1], then PANA allows to create the SAML artifact in the visited network (by some entity) and to subsequently use services either in the visited network itself (as shown in Figure 4 or in networks which have some trust relationship with the visited network with regard to the later service usage.



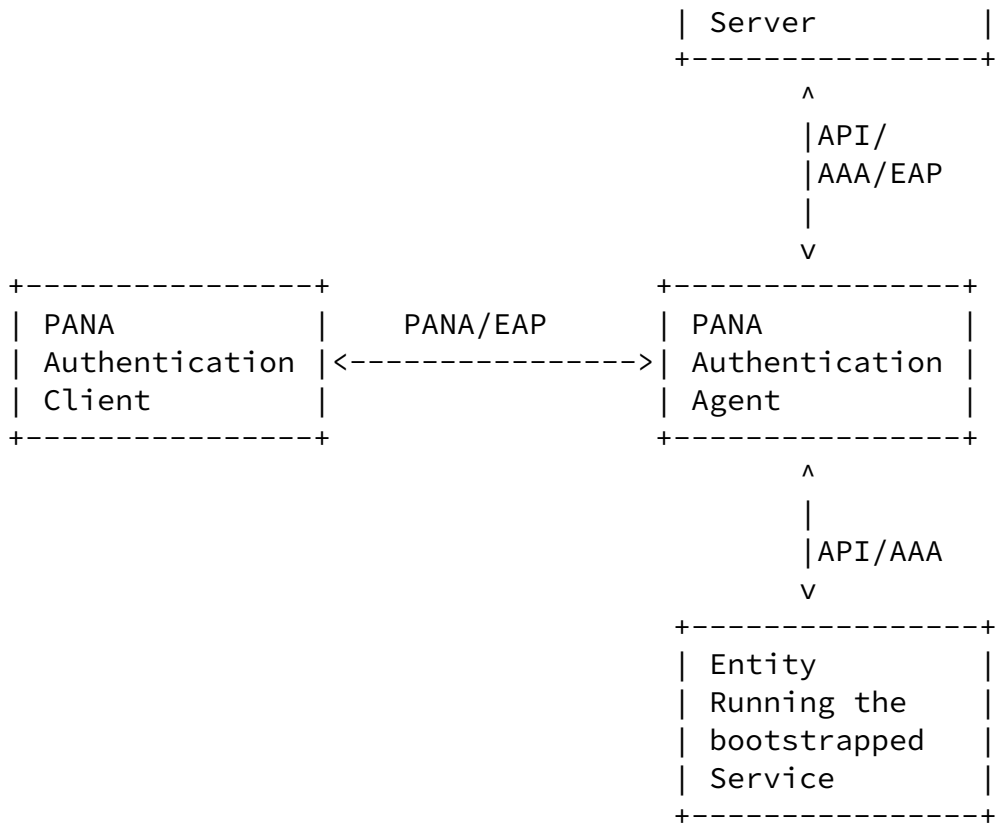


Figure 6: SAML Artifact transport in PANA

To create a feasible solution, it is necessary that the SAML artifact can be carried in a AAA protocol (e.g., DIAMETER or RADIUS) between the AAA server and the PAA and is then finally delivered from the PAA to the PaC by using PANA. According to the PANA specification [1] the PANA-FirstAuth-End-Request (PFER) (if both NAP and ISP authentication is carried out) and/or Pana-Binding-Request (PBR) message can transport new AVPs. Confidentiality protection must be provided for this purpose. Authorization information could be carried by defining new AVPs to be transported inside these messages. Note that the new attributes or AVPs to carry SAML in DIAMETER (or RADIUS) also need to be defined.

6. Binding Authorization Information to Credentials

SAML introduces the concept of a holder-of-the-key assertion to bind the assertions (authorization information) to a cryptographic key. See Section 5.1 of [2]

A number of credentials can be used with the KeyInfo element of the Holder-of-the-Key assertion as described in Section 4.4 of [8], such as:

- KeyName element, which is a string containing an identifier to a key.
- KeyValue element, which contains the public key
- RetrievalMethod element, which is a reference to a key
- The X509Data element even contains one or more identifiers of keys, X.509 certificates, certificate identifiers or a revocation list.
- PGPData element that is used to convey information related to PGP public key pairs
- SPKIData element carries information related to SPKI public key pairs, certificates and other SPKI data.
- MgmtData element can contain a string value used to convey in-band key distribution or agreement data

These concept allows the SAML assertion to be associated with the bootstrapped credentials. For example, binding a public key to a SAML assertion might also be a helpful when the public / private key pair is also bootstrapped based using EAP and uses a pseudonym to allow user identity confidentiality. In this case, this approach would provide credential based authorization. This would then allow subsequent application layer protocols interactions to be secured while authorization information can be attached and provided via SAML.

Binding a Kerberos Granting Ticket or a Kerberos Service Ticket to a SAML assertion is also possible but a Kerberos ticket does not have a unique identifier, such as a SerialNumber provided by X.509 certificates. One possible approach is to attach the same unique and randomly chosen identifier to both, the KeyName element and to the authorization-data field of the encrypted part of the Kerberos ticket.

Furthermore, it is possible to bind the SAML assertion to the AAA-key. This binding, therefore, associates the network authentication and authorization protocol run to the assertion. Each time the user needs to re-authenticate, the assertion can be presented to grant access to the network (and also allowing the both entities to generate a new AAA-key). Such a procedure might be helpful when handovers within different access routers in the access network is desired (intra-domain mobility) or even with inter-domain mobility.

7. Security Considerations

The security of the proposed mechanism relies on the selected EAP method, on SAML and on the bootstrapping mechanism. A security analysis of different EAP methods is outside the scope of this document. It is assumed that the bootstrapping mechanism (possibly involving AAA key distribution mechanisms) and the selected EAP method is secure.

This section discusses a number of selected security threats and their countermeasures.

7.1 Stolen Assertion

Threat:

If an eavesdropper can eavesdrop the SAML Assertion and construct a service request, then the eavesdropper could be able to impersonate the user at other entities.

Countermeasures:

By providing adequate confidentiality, eavesdropping of a SAML assertion can be avoided.

7.2 MitM Attack

Threat:

Since the SAML assertion is presented to a service when authorization is desired, a malicious service provider could impersonate the user at some other entities. These entities would

believe that the adversary has the rights indicated in the assertion.

Countermeasures:

If the adversary is a not-participating in the SIP signaling itself (i.e., it is not a SIP proxy or a SIP UA), this threat can be eliminated by employing inherent SIP security mechanisms , such as TLS. However, if this entity is part of the communication itself then reference integrity needs to be provided. Assertions with tight restrictions (e.g., validity of the assertion) can also limit the possible damage.

7.3 Forged Assertion

Threat:

A malicious user could forge or alter a SAML assertion in order to communicate with other entities.

Countermeasures:

To avoid this kind of attack, the entities must assure that proper mechanisms for protecting the SAML assertion needs to be in place. It is recommended to protect the assertion using a digital signature. Note that the current proposal uses Artifacts in most places (EAP methods or PANA) and makes it therefore difficult for an adversary to be able to mount such an attack.

7.4 Replay Attack

Threat:

An adversary who is able to gain access to an Assertion or an Artifcat might be able to attach this token to a resource request to gain special privileges.

Countermeasures:

The Artifact must be encrypted when the user obtains it. It also needs to be transmitted encrypted when it is used for authorization. To make it even more difficult for an adversary to reuse the Artifact it is possible to associate credentials (either symmetric or asymmetric keying material) with the Assertion. An adversary can then only impersonate the legitimate user if he knows the Artifact or Assertion and the corresponding credentials.

7.5 Privacy

Threat:

An adversary might be able to eavesdrop both the EAP communication and the usage of SAML Artifacts and Assertions. This information might reveal user identities and usage patterns.

Countermeasures:

EAP methods provide mechanisms to hide the true user identity. This is, however, useless if a SAML Assertion again reveals the

true user identity. Since the Assertion is possibly only exchanged using DIAMETER an adversary needs to be located at a AAA client or server. The Artifcat itself does not reveal user specific information since it is only a pointer to the Assertion. Only legitimate entities are allowed to fetch the Assertion using an Artifact. Furthermore, SAML does not mandate the inclusion of a user identity in the Assertion.

8. Acknowledgments

We would like to thank Goeman Stefan and Rainer Falk for sharing their thoughts with us. Furthermore, we would like to thank the authors of [29] on trait-based authorization for SIP (namely Jon Peterson, James Polk, Douglas Sicker and Marcus Tegnander) for their discussions on the usage of SAML for IETF protocols.

The authors are working in two EU funded projects, namely Ambient Networks and DAIDALOS.

Parts of this document are a byproduct of the Ambient Networks

Project, partially funded by the European Commission under its Sixth Framework Programme. It is provided "as is" and without any express or implied warranties, including, without limitation, the implied warranties of fitness for a particular purpose. The views and conclusions contained herein are those of the authors and should not be interpreted as necessarily representing the official policies or endorsements, either expressed or implied, of the Ambient Networks Project or the European Commission.

The work described in this document is partially based on results of IST FP6 Integrated Project DAIDALOS. DAIDALOS receives research funding from the European Community's Sixth Framework Programme. Apart from this, the European Commission has no responsibility for the content of this paper. The information in this document is provided as is and no guarantee or warranty is given that the information is fit for any particular purpose. The user thereof uses the information at its sole risk and liability. The views and conclusions contained herein are those of the authors and should not be interpreted as necessarily representing the official policies or endorsements, either expressed or implied, of Daidalos Project or the European Commission.

9. References

9.1 Normative References

[1] Forsberg, D., "Protocol for Carrying Authentication for Network

Access (PANA)", draft-ietf-pana-pana-09 (work in progress), July 2005.

[2] Maler, E., Philpott, R., and P. Mishra, "Bindings and Profiles for the OASIS Security Assertion Markup Language (SAML) V1.1", September 2003.

[3] Maler, E., Philpott, R., and P. Mishra, "Assertions and Protocol for the OASIS Security Assertion Markup Language (SAML) V1.1", September 2003.

[4] Blunk, L., "Extensible Authentication Protocol (EAP)", draft-ietf-eap-rfc2284bis-09 (work in progress), February 2004.

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

[6] Calhoun, P., Loughney, J., Guttman, E., Zorn, G., and J. Arkko, "Diameter Base Protocol", RFC 3588, September 2003.

[7] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", March 1997.

[8] Eastlake, D., Reagle, J., and D. Solo, "XML-Signature Syntax and Processing, W3C Recommendation (available at http://www.w3.org/TR/xmldsig-core/)", February 2002.

9.2 Informative References

[9] Tschofenig, H. and D. Kroeselberg, "Next Steps for ENROLL", draft-tschofenig-enroll-next-steps-00 (work in progress), October 2004.

[10] Pritikin, M., "Trusted Transitive Introduction Model", draft-pritikin-ttimodel-01 (work in progress), July 2004.

[11] Patel, A., "Problem Statement for bootstrapping Mobile IPv6", draft-ietf-mip6-bootstrap-ps-03 (work in progress), July 2005.

[12] Jee, J., "Diameter Mobile IPv6 Bootstrapping Application using PANA", draft-jee-mip6-bootstrap-pana-00 (work in progress), October 2004.

[13] Giaretta, G., "MIPv6 Authorization and Configuration based on EAP", draft-giaretta-mip6-authorization-eap-02 (work in progress), October 2004.

[14] Kempf, J., "Bootstrapping Mobile IPv6", draft-chakrabarti-mip6-bmip-01 (work in progress), February 2005.

[15] Tschofenig, H., Bournelle, J., and S. Thiruvengadam, "Bootstrapping Mobile IPv6 using PANA", draft-tschofenig-mip6-bootstrapping-pana-00 (work in progress), October 2004.

[16] Leung, K., "Authentication Protocol for Mobile IPv6", draft-ietf-mip6-auth-protocol-04 (work in progress), February 2005.

[17] Droms, R. and W. Arbaugh, "Authentication for DHCP Messages", RFC 3118, June 2001.

[18] Yegin, A., Tschofenig, H., and D. Forsberg, "Bootstrapping RFC3118 Delayed DHCP Authentication Using EAP-based Network Access Authentication", draft-yegin-eap-boot-rfc3118-01 (work in progress), January 2005.

[19] Tschofenig, H., "Bootstrapping RFC3118 Delayed authentication using PANA", draft-tschofenig-pana-bootstrap-rfc3118-01 (work in progress), October 2003.

[20] Tschofenig, H., "Bootstrapping Kerberos", draft-tschofenig-pana-bootstrap-kerberos-00 (work in progress), July 2004.

[21] Mahy, R., "An Extensible Authentication Protocol (EAP) Enrollment Method", draft-mahy-eap-enrollment-00 (work in progress), July 2005.

[22] Cam-Winget, N., "Dynamic Provisioning using EAP-FAST", draft-cam-winget-eap-fast-provisioning-00 (work in progress), July 2005.

[23] Aboba, B., "Extensible Authentication Protocol (EAP) Key Management Framework", draft-ietf-eap-keying-06 (work in progress), April 2005.

[24] Maler, E. and J. Hughes, "Technical Overview of the OASIS Security Assertion Markup Language (SAML) V1.1", March 2004.

[25] Ellison, C., Frantz, B., Lampson, B., Rivest, R., Thomas, B., and T. Ylonen, "SPKI Certificate Theory", RFC 2693, September 1999.

[26] Farrell, S. and R. Housley, "An Internet Attribute Certificate Profile for Authorization", RFC 3281, April 2002.

[27] Kaufman, C., "Internet Key Exchange (IKEv2) Protocol", draft-ietf-ipsec-ikev2-17 (work in progress), October 2004.

[28] Bournelle, J., "Bootstrapping Mobile IPv6 using PANA", draft-bournelle-pana-mip6-00 (work in progress), December 2004.

[29] Peterson, J., "Trait-based Authorization Requirements for the Session Initiation Protocol (SIP)", draft-ietf-sipping-trait-authz-01 (work in progress), February 2005.

[30] Alfano, F., "Diameter Quality of Service Application", draft-alfano-aaa-qosprot-02 (work in progress), February 2005.

[31] Bosch, S., Karagiannis, G., and A. McDonald, "NSLP for Quality-of-Service signaling", draft-ietf-nsis-qos-nslp-06 (work in progress), February 2005.

[32] Tschofenig, H., "Using SAML for SIP", draft-tschofenig-sip-saml-03 (work in progress), July 2005.

[33] Aboba, B. and J. Wood, "Authentication, Authorization and Accounting (AAA) Transport Profile", RFC 3539, June 2003.

[34] Mattila, L., Koskinen, J., Stura, M., Loughney, J., and H. Hakala, "Diameter Credit-control Application", draft-ietf-aaa-diameter-cc-06 (work in progress), August 2004.

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

[36] Bersani, F., "The EAP-PSK Protocol: a Pre-Shared Key EAP Method", draft-bersani-eap-psk-07 (work in progress),

February 2005.

[37] Tschofenig, H., "EAP IKEv2 Method (EAP-IKEv2)", draft-tschofenig-eap-ikev2-06 (work in progress), May 2005.

[38] Aboba, B. and D. Simon, "PPP EAP TLS Authentication Protocol",

RFC 2716, October 1999.

[39] Aboba, B. and P. Calhoun, "RADIUS (Remote Authentication Dial In User Service) Support For Extensible Authentication Protocol (EAP)", RFC 3579, September 2003.

[40] Eronen, P., Hiller, T., and G. Zorn, "Diameter Extensible Authentication Protocol (EAP) Application", draft-ietf-aaa-eap-10 (work in progress), November 2004.

Authors' Addresses

Hannes Tschofenig
Siemens
Otto-Hahn-Ring 6
Munich, Bavaria 81739
Germany

Email: Hannes.Tschofenig@siemens.com

Gerardo Giaretta
Telecom Italia Lab
via G. Reiss Romoli, 274
TORINO, 10148
Italy

Email: gerardo.giaretta@tilab.com

Antonio F. Gomez-Skarmeta
University of Murcia
Campus de Espinardo s/n
Murcia, E-30100

Spain

Email: skarmeta@dif.um.es

James Polk
Cisco
2200 East President George Bush Turnpike
Richardson, Texas 75082
US

Email: jmpolk@cisco.com

Intellectual Property Statement

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.

Disclaimer of Validity

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 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 WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.

Copyright Statement

Copyright (C) The Internet Society (2005). 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.

Acknowledgment

Funding for the RFC Editor function is currently provided by the Internet Society.