

Network Working Group
Internet-Draft
Intended status: Informational
Expires: April 30, 2015

G. Chen
China Mobile
D. Zhang
Huawei
T. Reddy
Cisco
October 27, 2014

(U)SIM based PCP Authentication
[draft-chen-pcp-authentication-sim-01](#)

Abstract

With (U)SIM support, PCP authentication could leverage the credentials stored in (U)SIM. The document details PCP authentication considerations based on (U)SIM support. The authentication procedures in EAP and GBA framework have been specifically elaborated. In order to complete the process, new code and option are also proposed.

Status of This Memo

This Internet-Draft is submitted in full conformance with the provisions of [BCP 78](#) and [BCP 79](#).

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF). Note that other groups may also distribute working documents as Internet-Drafts. The list of current Internet-Drafts is at <http://datatracker.ietf.org/drafts/current/>.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

This Internet-Draft will expire on April 30, 2015.

Copyright Notice

Copyright (c) 2014 IETF Trust and the persons identified as the document authors. All rights reserved.

This document is subject to [BCP 78](#) and the IETF Trust's Legal Provisions Relating to IETF Documents (<http://trustee.ietf.org/license-info>) in effect on the date of publication of this document. Please review these documents carefully, as they describe your rights and restrictions with respect

Internet-Draft

pcp-auth-sim

October 2014

to this document. Code Components extracted from this document must include Simplified BSD License text as described in Section 4.e of the Trust Legal Provisions and are provided without warranty as described in the Simplified BSD License.

Table of Contents

1.	Introduction	2
2.	PCP Authentication with (U)SIM	2
2.1.	EAP Framework	3
2.2.	GBA Framework	4
3.	Proposal	6
4.	Security Considerations	7
5.	IANA Considerations	7
6.	References	7
6.1.	Normative References	7
6.2.	Informative References	8
	Authors' Addresses	8

[1.](#) Introduction

Mobile network is experiencing the significant traffic changes over the past few years. With Long Term Evolution (LTE) advance, plenty of data services have been appeared to be major traffic on the network. The Port Control Protocol[RFC6887] could facilitate data paths through NAT/Firewell and optimize data traffic behavior. It's obvious a 3rd Generation Partnership Project (3GPP) network can benefit from the use of the PCP service.

[[I-D.chen-pcp-mobile-deployment](#)] has enumerated several considerations in a mobile environment. Subscribers take advantage of (U)SIM to provide the security guarantee. Hence, PCP clients could also leverage the credential to perform authentication.

This document describes the uses of (U)SIM specific authentication which is compatible with [[I-D.ietf-pcp-authentication](#)]. A new option is proposed to assist the completion of process.

[2.](#) PCP Authentication with (U)SIM

A permanent key is stored on the (U)SIM card and in AAA nodes (e.g. HLR/HSS) in the mobile network. The key has been to pass through the authentication. Afterwards, derived keys are generated for chipering and integrity protection of user-plan and control plane traffic. The

use of (U)SIM to PCP authentication is applicable to WLAN access and 3GPP access cases. The following demonstrates the scenarios with different frameworks.

2.1. EAP Framework

With the support of (U)SIM cards, UEs could take the credentials from (U)SIM cards and perform EAP-SIM[RFC4186]/EAP-AKA[RFC4187]/EAP-AKA'[RFC5448] get through the authentication. The network has been shown as the below.

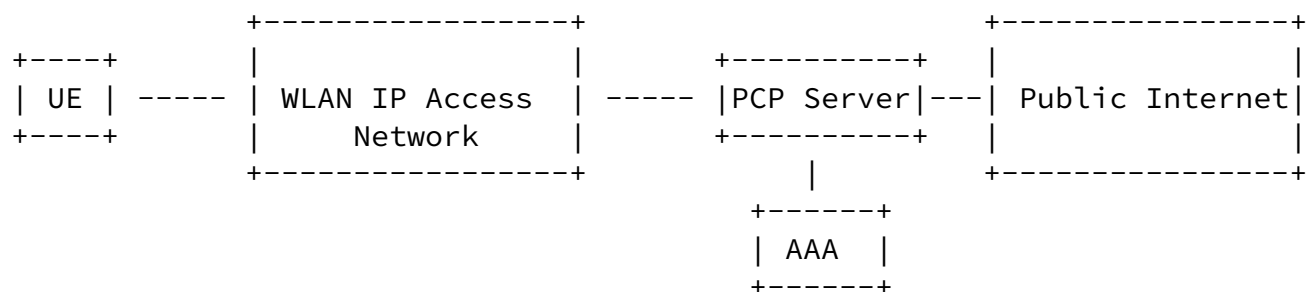


Figure1: WLAN Access with EAP Support

The process of authentication in the EAP framework is compliant with [I-D.ietf-pcp-authentication]. In addition, the PCP server takes the authenticator role and operates as pass-through behavior. It forwards EAP packets received from the PCP client and destined to the backend authentication server (i.e., AAA server); packets received from the AAA server destined to the PCP client are forwarded to it. PCP server is required to have interconnection with AAA server over RADIUS[RFC5580] or DIAMETER[RFC6733] protocol. The Figure 2 shows an example with EAP-AKA/EAP-AKA' process.

Internet-Draft

pcp-auth-sim

October 2014

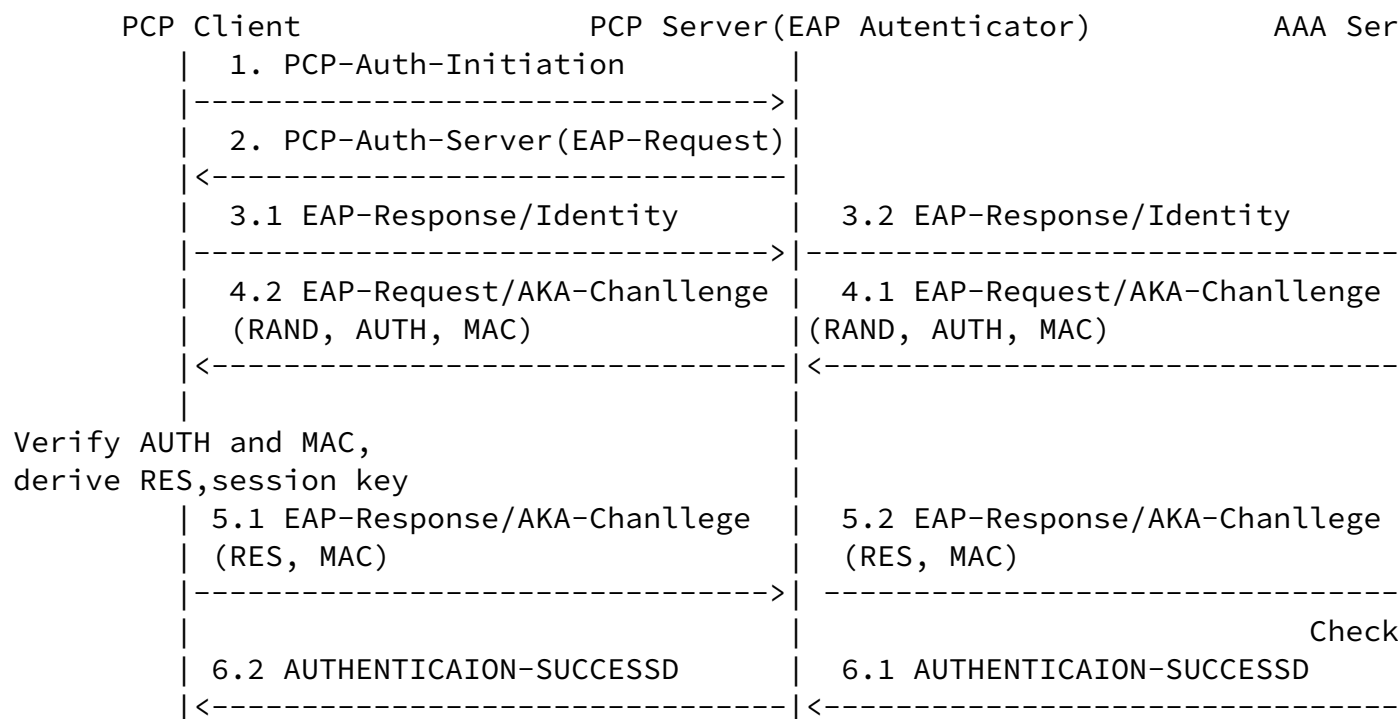


Figure2: PCP authentication with EAP-AKA/EAP-AKA'

The EAP framework could be used to support authentication of WLAN users with (U)SIM. Direct WLAN or WLAN interworking with 3GPP networks can adopt this method.

2.2. GBA Framework

[TS33.220] has specified Generic Bootstrapping Architecture (GBA) to

offer bootstrap authentication and key agreement for application security. This architecture has been already used to support the authentication of 3GPP access users to service platform with 3GPP AKA mechanism, for example Ut interface authentication in IMS network. GBA has merits of flexibility so the service platforms could benefit from the adoption and do not have to introduce additional process and new credentials. Therefore, it's desirable to accomodate the PCP authentication in such framework. Figure 3 shows the network with GBA.

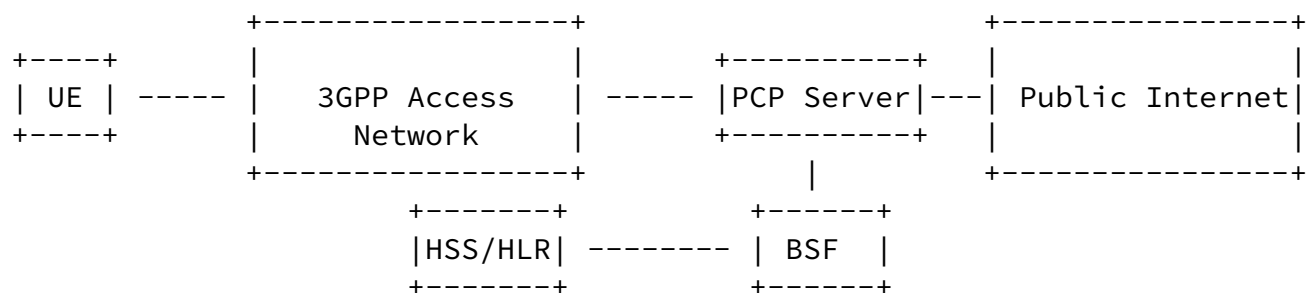


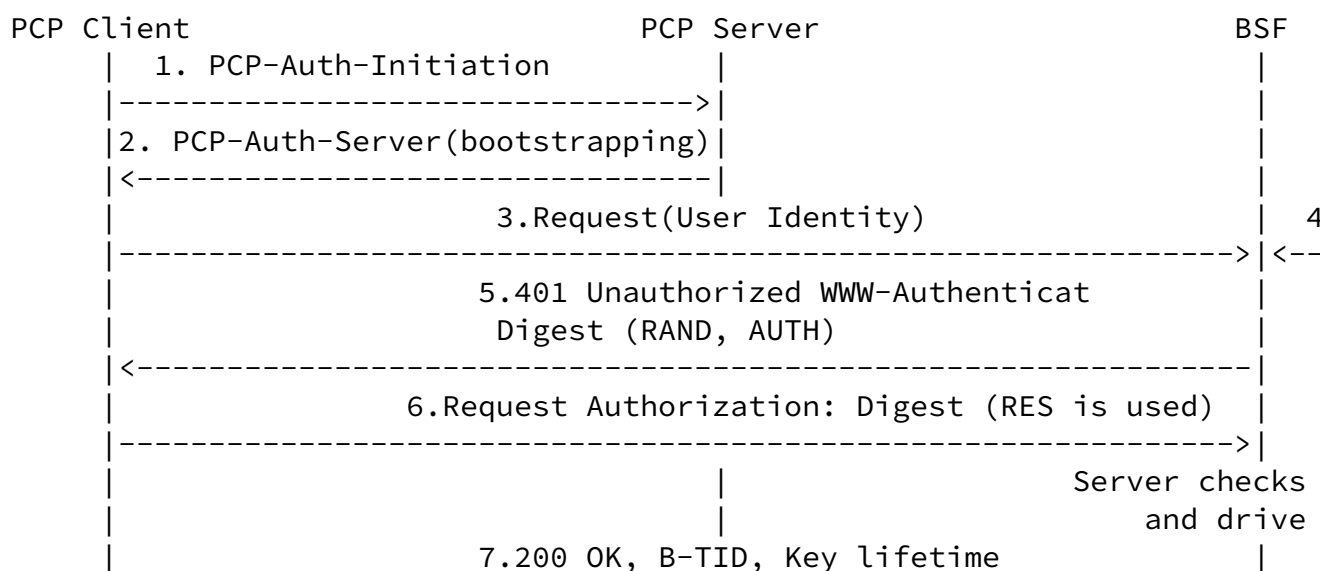
Figure3: 3GPP Access with GBA Support

A Bootstrapping Server Function (BSF) and the UE mutually authenticate using the AKA protocol, and agree on session keys that are afterwards applied between UE and a PCP Server. The set of all user security material is stored in the Home Subscriber System (HSS).

Once BSF requires the security material for a user, HSS identity the specific material by matching UE identity(e.g. MSISDN or IMSI) and reponse BSF with Authentication Vector (AV, AV = RAND||AUTN||XRES||CK||IK). Afterwards, HTTP AKA[RFC3310] is taken place between UE and BSF. As a sequence, both the UE and the BSF shall use the Ks to derive the key material Ks, whichi is used for

securing the path between PCP server and UE. BSF also generates a Bootstrapping Transaction Identifier (B-TID) as an index in order to facilitate the conversation between PCP Server and BSF.

After the bootstrapping has been completed, the authentication of messages will be exchanged between the UE and a PCP server based on those session keys generated during the mutual authentication between UE and BSF. Figure4 shows the process.



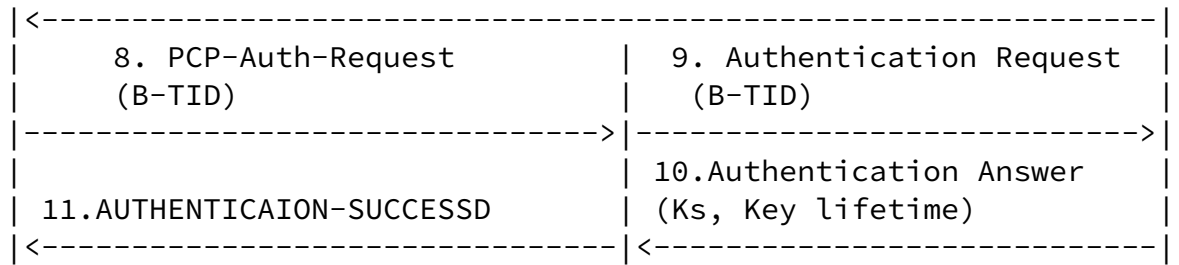


Figure4: PCP authentication in GBA

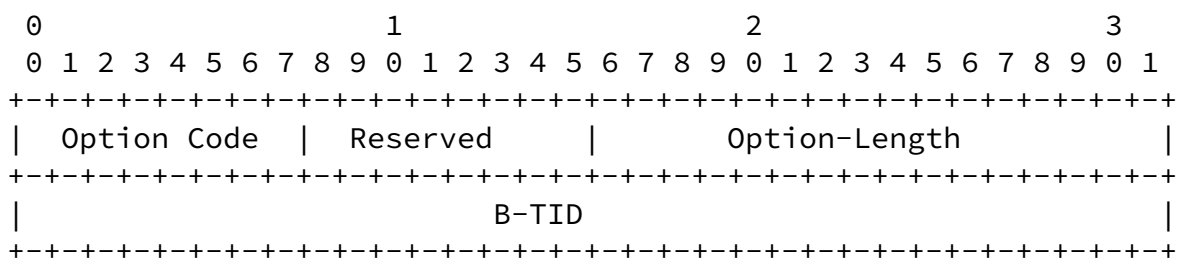
3. Proposal

In order to fullfill the process of PCP authentication in GBA, one result code is required and company with [\[I-D.ietf-pcp-authentication\]](#).

TBD BOOTSTRAPPING-INITIATION

The code is applied to above step 2 in Figure4.

B-TID option is also proposed to perform step 8 in Figure 4.



Option Code: it's to identify the B-TID use.

Option-Length: The length of the B-TID Option (in octet), including the 4 octet fixed header and the variable length of the B-TID message.

B-TID: According to ,The B-TID value shall be also generated in format of Network Access Identi (NAI) by taking the base64 encoded [\[RFC3548\]](#), RAND value , and the BSF server name, i.e. base64encode(RAND)@BSF_servers_domain_name.

[4.](#) Security Considerations

TBD

[5.](#) IANA Considerations

TBD

[6.](#) References

[6.1.](#) Normative References

- [RFC3310] Niemi, A., Arkko, J., and V. Torvinen, "Hypertext Transfer Protocol (HTTP) Digest Authentication Using Authentication and Key Agreement (AKA)", [RFC 3310](#), September 2002.
- [RFC4186] Haverinen, H. and J. Salowey, "Extensible Authentication Protocol Method for Global System for Mobile Communications (GSM) Subscriber Identity Modules (EAP-SIM)", [RFC 4186](#), January 2006.
- [RFC4187] Arkko, J. and H. Haverinen, "Extensible Authentication Protocol Method for 3rd Generation Authentication and Key Agreement (EAP-AKA)", [RFC 4187](#), January 2006.
- [RFC5448] Arkko, J., Lehtovirta, V., and P. Eronen, "Improved Extensible Authentication Protocol Method for 3rd Generation Authentication and Key Agreement (EAP-AKA')", [RFC 5448](#), May 2009.
- [RFC5580] Tschofenig, H., Adrangi, F., Jones, M., Lior, A., and B. Aboba, "Carrying Location Objects in RADIUS and Diameter", [RFC 5580](#), August 2009.
- [RFC6733] Fajardo, V., Arkko, J., Loughney, J., and G. Zorn, "Diameter Base Protocol", [RFC 6733](#), October 2012.

- [RFC6887] Wing, D., Cheshire, S., Boucadair, M., Penno, R., and P.

Selkirk, "Port Control Protocol (PCP)", [RFC 6887](#), April 2013.

[TS33.220]

"Generic Authentication Architecture (GAA); Generic Bootstrapping Architecture (GBA)", 10.1.0 3GPP TS 33.220, March 2012.

[6.2](#). Informative References

[I-D.chen-pcp-mobile-deployment]

Chen, G., Cao, Z., Boucadair, M., Ales, V., and L. Thiebaut, "Analysis of Port Control Protocol in Mobile Network", [draft-chen-pcp-mobile-deployment-04](#) (work in progress), July 2013.

[I-D.ietf-pcp-authentication]

Wasserman, M., Hartman, S., Zhang, D., and T. Reddy, "Port Control Protocol (PCP) Authentication Mechanism", [draft-ietf-pcp-authentication-06](#) (work in progress), October 2014.

[RFC3548] Josefsson, S., "The Base16, Base32, and Base64 Data Encodings", [RFC 3548](#), July 2003.

Authors' Addresses

Gang Chen
China Mobile
53A,Xibianmennei Ave.,
Xuanwu District,
Beijing 100053
China

Email: phdgang@gmail.com

Dacheng Zhang
Huawei
Beijing
China

Email: zhangdacheng@huawei.com

Tirumaleswar Reddy
Cisco Systems, Inc.
Cessna Business Park, Varthur Hobli
Sarjapur Marathalli Outer Ring Road
Bangalore, Karnataka 560103
India

Email: tiredy@cisco.com

