Network Working Group
Request for Comments: 5002
Category: Informational

G. Camarillo
G. Blanco
Ericsson

August 2007

The Session Initiation Protocol (SIP) P-Profile-Key Private Header (P-Header)

Status of This Memo

Abstract

This document specifies the SIP P-Profile-Key P-header. This header field is used in the 3rd-Generation Partnership Project (3GPP) IMS (IP Multimedia Subsystem) to provide SIP registrars and SIP proxy servers with the key of the profile corresponding to the destination SIP URI of a particular SIP request.

Table of Contents

1. Introduction

The 3rd-Generation Partnership Project (3GPP) IMS (IP Multimedia Subsystem) uses SIP [RFC3261] as its main signalling protocol. (For more information on the IMS, a detailed description can be found in 3GPP TS 23.228 [3GPP.23.228] and 3GPP TS 24.229 [3GPP.24.229]). 3GPP has identified a set of requirements that can be met, according to the procedures in [RFC3427], by defining a new SIP P-header.

The remainder of this document is organized as follows. Section 3 describes the scenario considered by 3GPP and Section 4 discusses the requirements derived from this scenario. Section 5 defines the P-Profile-Key header field, which meets those requirements, and Section 6 discusses the applicability and scope of this new header field. Section 7 registers the P-Profile-Key header field with the IANA and Section 8 discusses the security properties of the environment where this header field is intended to be used.

2. Terminology

HSS: Home Subscriber Server.

I-CSCF: Interrogating - Call/Session Control Function.

Public Service Identity:
A SIP URI that refers to a service instead of a user.

S-CSCF: Serving - Call/Session Control Function.

Wildcarded Public Service Identity:
A set of Public Service Identities that match a regular expression and share the same profile.

3. Scenario

In the 3GPP IMS, there are scenarios where a set of proxies handling a request need to consult the same user database, as described in [RFC4457]. Those proxies typically use the destination SIP URI of the request as the key for their database queries. Nevertheless, when a proxy handles a Wildcarded Public Service Identity, the key to be used in its database query is not the destination SIP URI of the request, but a regular expression instead.

Public Service Identities are SIP URIs that refer to services instead of users. That is, they address a specific application in an Application Server. Wildcarded Public Service Identities are a set of Public Service Identities that match a regular expression and share the same profile. For example, the Public Service Identities

'sip:chatroom-12@example.com' and 'sip:chatroom-657@example.com' would match the Wildcarded Public Service Identity 'sip:chatroom-!.*!@example.com'. For a description of Wildcarded Public Service Identities, see 3GPP TS 23.003 [3GPP.23.003].

When a proxy queries the user database for a Public Service Identity for which there is no profile in the user database, the user database needs to find its matching Wildcarded Public Service Identity. For example, if the user database receives a query for 'sip:chatroom-657@example.com', the user database needs to go through all the Wildcarded Public Service Identity it has until it finds a matching one; in this case, 'sip:chatroom-!.*!@example.com'. The process to find a matching Wildcarded Public Service Identity can be computationally expensive, time consuming, or both.

When two proxies query the user database for the same Public Service Identity, which matches a Wildcarded Public Service Identity, the user database needs to perform the matching process twice. Having to perform that process twice can be avoided by having the first proxy obtain the Wildcarded Public Service Identity from the user database and transfer it, piggy-backed in the SIP message, to the second proxy. This way, the second proxy can query the user database using the Wildcarded Public Service Identity directly.

An alternative, but undesirable, solution would consist of having the user database store every Public Service Identity and its matching Wildcarded Public Service Identity. The scalability and manageability properties of this approach are considerably worse than those of the approach described earlier.

4. Requirements

This section lists the requirements derived from the previous scenario:

1. It is necessary to optimize the response time for session establishment in the 3GPP IMS.

2. It is necessary to keep the user database's size and maintenance manageable (e.g., storing individual Public Service Identities matching a Wildcarded Public Service Identity in the user database is not believed to be an acceptable solution).

5. P-Profile-Key Header Field Definition

This document defines the SIP P-Profile-Key P-header. The P-Profile-Key P-header contains the key to be used by a proxy to query the user database for a given profile.

The augmented Backus-Naur Form (BNF) [RFC4234] syntax of the P-Profile-Key header field is the following:

```
P-Profile-Key     = "P-Profile-Key" HCOLON (name-addr / addr-spec)
                     *( SEMI generic-param )
```

The format of HCOLON, name-addr, addr-spec, and generic-param are defined in [RFC3261]. The format of Wildcarded Public Service Identities is defined in 3GPP TS 23.003 [3GPP.23.003]. They take the form of Extended Regular Expressions (ERE) as defined in Chapter 9 of IEEE 1003.1-2004 Part 1 [IEEE.1003.1-2004].

The following is an example of a P-Profile-Key header field that contains a Wildcarded Public Service Identity:

```
P-Profile-Key: <sip:chatroom-!.*!@example.com>
```

6. Applicability

According to [RFC3427], P-headers have a limited applicability. Specifications of P-headers such as this RFC need to clearly document the useful scope of the proposal, and explain its limitations and why it is not suitable for the general use of SIP on the Internet.

The P-Profile-Key header field is intended to be used in 3GPP IMS networks. This header field carries the key of a service profile, that is stored in a user database referred to as HSS, between two proxies, which are referred to as I-CSCF and S-CSCF. The I-CSCF and the S-CSCF belong to the same administrative domain and share a common frame of reference to the user database. The I-CSCF inserts the P-Profile-Key header field into a SIP request and the S-CSCF removes it before routing the request further. (For a description of how an I-CSCF and an S-CSCF query the same user database for a single request, see [RFC4457].)

Typically, when SIP is used on the Internet, there are not multiple proxies with a trust relationship between them querying the same user database. Consequently, the P-Profile-Key header field does not seem useful in a general Internet environment.

7. IANA Considerations

This document defines a new SIP header field: P-Profile-Key. This header field has been registered by the IANA in the SIP Parameters registry under the Header Fields subregistry.

8. Security Considerations

The P-Profile-Key defined in this document is to be used in an environment where elements are trusted and where attackers are not supposed to have access to the protocol messages between those elements. Traffic protection between network elements is sometimes achieved by using IPsec and sometimes by physically protecting the network. In any case, the environment where the P-Profile-Key header field will be used ensures the integrity and the confidentiality of the contents of this header field. The P-Profile-Key header field MUST NOT be used in environments that do not have these characteristics.

The P-Profile-Key header field needs to be integrity protected to keep attackers from modifying its contents. An attacker able to modify the contents of this header field could make the network apply a different service than the one corresponding to the request carrying the P-Profile-Key header field.

The contents of the P-Profile-Key field need to be kept confidential. An attacker able to access the contents of this header field would obtain certain knowledge about the way services are structured in a given domain.

9. Acknowledgements

Alf Heidermark and Timo Forsman provided input to this document. Miguel Angel Garcia-Martin performed an expert review on this document on behalf of the SIPPING working group. Jon Peterson provided comments on this document.

10. References

10.1. Normative References

[RFC3261] Rosenberg, J., Schulzrinne, H., Camarillo, G., Johnston, A., Peterson, J., Sparks, R., Handley, M., and E. Schooler, "SIP: Session Initiation Protocol", RFC 3261, June 2002.

[RFC3427] Mankin, A., Bradner, S., Mahy, R., Willis, D., Ott, J., and B. Rosen, "Change Process for the Session Initiation Protocol (SIP)", BCP 67, RFC 3427, December 2002.

[RFC4234] Crocker, D. and P. Overell, "Augmented BNF for Syntax Specifications: ABNF", RFC 4234, October 2005.

[3GPP.23.003] 3GPP, "Numbering, addressing and identification", 3GPP TS 23.003 3.15.0, October 2006.

[IEEE.1003.1-2004] "Standard for information technology - portable operating system interface (POSIX). Base definitions", IEEE 1003.1-2004, 2004.

10.2. Informative References

[RFC4457] Camarillo, G. and G. Blanco, "The Session Initiation Protocol (SIP) P-User-Database Private-Header (P-Header)", RFC 4457, April 2006.

[3GPP.23.228] 3GPP, "IP Multimedia Subsystem (IMS); Stage 2", 3GPP TS 23.228 5.15.0, June 2006.

[3GPP.24.229] 3GPP, "Internet Protocol (IP) multimedia call control protocol based on Session Initiation Protocol (SIP) and Session Description Protocol (SDP); Stage 3", 3GPP TS 24.229 5.18.0, October 2006.

Authors' Addresses

Gonzalo Camarillo
Ericsson
Hirsalantie 11
Jorvas 02420
Finland

EMail: Gonzalo.Camarillo@ericsson.com

German Blanco
Ericsson
Via de los Poblados 13
Madrid 28033
Spain

EMail: German.Blanco@ericsson.com

Full Copyright Statement

Intellectual Property