

SIPCORE Working Group  
Internet-Draft  
Intended status: Standards Track  
Expires: November 26, 2016

C. Holmberg  
Ericsson  
J. Jiang  
China Mobile  
May 25, 2016

**Via header field parameter to indicate received realm  
draft-holmberg-dispatch-received-realm-02.txt**

**Abstract**

This specification defines a new Session Initiation Protocol (SIP) Via header field parameter, "received-realm", which allows a SIP entity acting as an entry point to a transit network to indicate from which adjacent upstream network a SIP request is received, using a network realm value associated with the adjacent network.

**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 November 26, 2016.

**Copyright Notice**

Copyright (c) 2016 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 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

<a href="#">1.</a>	Introduction . . . . .	<a href="#">2</a>
<a href="#">1.1.</a>	General . . . . .	<a href="#">2</a>
<a href="#">1.2.</a>	Use-Case: Transit Network Application Services . . . . .	<a href="#">3</a>
<a href="#">1.3.</a>	Use-Case: Transit Network Routing . . . . .	<a href="#">3</a>
<a href="#">2.</a>	Applicability . . . . .	<a href="#">4</a>
<a href="#">3.</a>	Conventions . . . . .	<a href="#">4</a>
<a href="#">4.</a>	Definitions . . . . .	<a href="#">4</a>
<a href="#">5.</a>	Vie 'received-realm' header field parameter . . . . .	<a href="#">4</a>
<a href="#">5.1.</a>	General . . . . .	<a href="#">5</a>
<a href="#">5.2.</a>	Header . . . . .	<a href="#">5</a>
<a href="#">5.3.</a>	Payload claims . . . . .	<a href="#">5</a>
<a href="#">5.4.</a>	Syntax . . . . .	<a href="#">6</a>
<a href="#">5.4.1.</a>	General . . . . .	<a href="#">6</a>
<a href="#">5.4.2.</a>	ABNF . . . . .	<a href="#">6</a>
<a href="#">6.</a>	User Agent and Proxy behavior . . . . .	<a href="#">6</a>
<a href="#">6.1.</a>	General . . . . .	<a href="#">6</a>
<a href="#">6.2.</a>	Behavior of a SIP entity acting as a network entry point	7
<a href="#">6.3.</a>	Behavior of a SIP entity consuming the received-network value . . . . .	<a href="#">7</a>
<a href="#">7.</a>	Example . . . . .	<a href="#">7</a>
<a href="#">8.</a>	IANA Considerations . . . . .	<a href="#">8</a>
<a href="#">8.1.</a>	'received-realm' Via header field parameter . . . . .	<a href="#">8</a>
<a href="#">8.2.</a>	JSON Web Token Claims Registration . . . . .	<a href="#">8</a>
<a href="#">9.</a>	Security Considerations . . . . .	<a href="#">9</a>
<a href="#">10.</a>	Acknowledgements . . . . .	<a href="#">10</a>
<a href="#">11.</a>	Change Log . . . . .	<a href="#">10</a>
<a href="#">12.</a>	References . . . . .	<a href="#">11</a>
<a href="#">12.1.</a>	Normative References . . . . .	<a href="#">11</a>
<a href="#">12.2.</a>	Informative References . . . . .	<a href="#">11</a>
	Authors' Addresses . . . . .	<a href="#">11</a>

## [1.](#) Introduction

### [1.1.](#) General

When SIP sessions are established between networks belonging to different operators, or between interconnected networks belonging to the same operator (or enterprise), the SIP requests might traverse transit network.

Such transit networks might provide different kind of services. In order to do that, a transit network often needs to know to which



operator (or enterprise) the adjacent upstream network, from which the SIP session initiation request is received, belongs.

This specification defines a new Session Initiation Protocol (SIP) Via header field parameter, "received-realm", which allows a SIP entity acting as an entry point to a transit network to indicate from which adjacent upstream network a SIP request is received, using a network realm value associated with the adjacent network.

NOTE: As the adjacent network can be an enterprise network, an Inter Operator Identifier (IOI) cannot be used to identify the network, as IOIs are not defined for enterprise networks.

The following sections describe use-case where the information is needed.

### **1.2. Use-Case: Transit Network Application Services**

The 3rd Generation Partnership Project (3GPP) TS 23.228 specifies how an IP Multimedia Subsystem (IMS) network can be used to provide transit functionality. An operator can use its IMS network to provide transit functionality e.g. to non-IMS customers, to enterprise networks, and to other network operators.

The transit network operator can provide application services to the networks for which it is providing transit functionality. Transit application services are typically not provided per user basis, as the transit network does not have access to the user profiles of the networks for which the application services are provided. Instead, the application services are provided per served network.

When a SIP entity that provides application services (e.g. an Application Server) within a transit network receives a SIP request, in order to apply the correct services it needs to know the adjacent upstream network from which the SIP request is received.

### **1.3. Use-Case: Transit Network Routing**

A transit network operator normally interconnects to many different operators, including other transit network operators, and provides transit routing of SIP requests received from one operator network towards the destination. The destination can be within an operator network to which the transit network operator has a direct interconnect, or within an operator network that only can be reached via one or more interconnected transit operators.

For each customer, i.e. interconnected network operator for which, the transit network operator routes SIP requests towards the



requested destination a set of transit routing policies are defined. These policies are used to determine how a SIP request shall be routed towards the requested destination to meet the agreement the transit network operator has with its customer.

When a SIP entity that performs the transit routing functionality receives a SIP request, in order to apply the correct set of transit routing policies, it needs to know from which of its customers, i.e. adjacent upstream network, the SIP request is received.

## **2. Applicability**

The mechanism defined in this specification **MUST** only be used by SIP entities that are able to verify from which adjacent upstream network a SIP request is received.

The mechanism for verifying from which adjacent upstream network a SIP request is received is outside the scope of this specification.

## **3. Conventions**

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 [BCP 14](#), [RFC 2119](#) [[RFC2119](#)].

## **4. Definitions**

SIP entity: SIP User Agent (UA), or SIP proxy, as defined in [RFC 3261](#).

Adjacent upstream SIP network: The adjacent SIP network in the direction from which a SIP request is received.

Network entry point: A SIP entity on the border of network, which receives SIP requests from adjacent upstream networks.

Inter Operator Identifier (IOI): A globally unique identifier to correlate billing information generated within the IP Multimedia Subsystem (IMS).

JWT: JSON Web Token, as defined in [RFC 7519](#).

## **5. Vie 'received-realm' header field parameter**



### **5.1. General**

The Via 'received-realm' header field parameter value is represented as a JSON Web Token (JWT) [[RFC7519](#)]. The JWT payload contains SIP header field values, and the value representing the adjacent network.

The procedures for encoding the JWT and calculating the signature are defined in [[RFC7519](#)].

### **5.2. Header**

The following header parameters MUST be included in the JWT.

- o The "typ" parameter MUST have a "JWT" value.
- o The "alg" parameter MUST have the value of the algorithm used to calculate the JWT signature.

NOTE: Operators need to agree on the set of supported algorithms for calculating the JWT signature.

Example:

```
{
    "typ": "JWT",
    "alg": "HS256"
}
```

### **5.3. Payload claims**

The following payload claims MUST be included in the JWT.

- o The "adjacent\_network" claim has the value representing the adjacent network.
- o The "sip\_from\_tag" claim has the value of the From 'tag' header field parameter of the SIP message.
- o The "sip\_date" claim has the value of the Date header field in the SIP message.
- o The "sip\_callid" claim has have value of the Call-ID header field in the SIP message.
- o The "sip\_cseq\_num" claim has the numeric value of the CSeq header field in the SIP message.





- o the "sip\_via\_branch" claim has value of the Via branch header field parameter of the Via header field, in the SIP message, to which the received-realm header parameter is attached.

Example:

```
{
  "adjacent_network":"operator_1.com",
  "sip_from_tag":"1928301774",
  "sip_date":"Fri, 20 May 2016 06:41:47 GMT",
  "sip_callid":"a84b4c76e66710@pc33.atlanta.com",
  "sip_cseq_num":"314159",
  "sip_via_branch":"z9hG4bK776asdhds"
}
```

## **5.4. Syntax**

### **5.4.1. General**

This section describes the syntax extensions to the ABNF syntax defined in [\[RFC3261\]](#), by defining a new Via header field parameter, "received-realm". The ABNF defined in this specification is conformant to [RFC 5234](#) [\[RFC5234\]](#). "EQUAL", "LDQUOTE", "RDQUOTE" and "ALPHA" are defined in [\[RFC3261\]](#). "DIGIT" is defined in [\[RFC5234\]](#).

### **5.4.2. ABNF**

```
via-params      =/ received-realm
received-realm  = "received-realm" EQUAL jwt
jwt             = LDQUOTE header "." payload "." signature RDQUOTE
header          = *base64-char
payload         = *base64-char
signature       = *base64-char
base64-char     = ALPHA / DIGIT / "/" / "+"
```

## **6. User Agent and Proxy behavior**

### **6.1. General**

This section describes how a SIP entity, acting as an entry point to a network, uses the "received-realm" Via header field parameter.



### **6.2. Behavior of a SIP entity acting as a network entry point**

When a SIP entity, acting as a network entry point, forwards a SIP request, or initiates a SIP request on its own (e.g. a PSTN gateway), the SIP entity adds a Via header field to the SIP request, according to the procedures in [RFC 3261](#) [[RFC3261](#)]. In addition, if the SIP entity is able to assert the adjacent upstream network, and if the SIP entity is aware of a network realm value defined for that network, the SIP entity can add a "received-realm" Via header field parameter, conveying the network realm value, to the Via header field added to the SIP request.

When the SIP entity adds a "received-realm" Via header field parameter to a SIP request, it MUST also calculate a Hash-based message authentication code (HMAC) [[RFC2104](#)] value from the parameter value, using a secret key which is shared between the SIP entity and any SIP entity which will use the parameter value. The HMAC is then added to the parameter.

When the receiver decodes the JWT, it MUST compare the JWT claims with the corresponding SIP header field information. If there is a mismatch, the receiver MUST discard the received-realm header field parameter.

### **6.3. Behavior of a SIP entity consuming the received-network value**

When a SIP entity receives a Via 'received-network' header field parameter, and intends to perform actions based on the header field parameter value, it MUST first check whether the values of the JWT claims representing SIP header field values match the associated SIP header field values within the SIP request. If the values of the JWT claims representing SIP header field values do not match the values of the associated SIP header field values the SIP entity MUST discard the adjacent network information present in the JWT. The SIP entity MAY take also take additional actions (e.g. rejecting the SIP request) based on local policy.

## **7. Example**



```

Operator 1      T_EP                                T_AS

- INVITE ----->
  Via: IP_UA
    - INVITE ----->
      Via: IP_TEP; received-realm="eyJhbG.eyJpc3.03f329"
        Via: IP_UA; received=IP_UA

    <- 200 OK -----
      Via: IP_TEP; received-realm="eyJhbG.eyJpc3.03f329"
        Via: IP_UA; received=IP_UA

<- 200 OK-----
  Via: IP_UA; received=IP_UA

```

## 8. IANA Considerations

### 8.1. 'received-realm' Via header field parameter

This specification defines a new Via header field parameter called received-realm in the "Header Field Parameters and Parameter Values" sub-registry as per the registry created by [\[RFC3968\]](#). The syntax is defined in [Section 5.4](#). The required information is:

Header Field	Parameter Name	Predefined Values	Reference
-----	-----	-----	-----
Via	received-realm	No	RFCXXXX

### 8.2. JSON Web Token Claims Registration

This specification defines new JSON Web Token claims in the "JSON Web Token Claims" sub-registry as per the registry created by [\[RFC7519\]](#).

- o Claim Name: "adjacent\_network"
- o Claim Description: Adjacent network from where a SIP request is received
- o Change Controller: IESG
- o Specification Document(s): RFC XXXX
- o Claim Name: "sip\_from\_tag"
- o Claim Description: SIP From tag header field parameter value



- o Change Controller: IESG
- o Specification Document(s): RFC XXXX, [RFC 3261](#)
- o Claim Name: "sip\_date"
- o Claim Description: SIP Date header field value
- o Change Controller: IESG
- o Specification Document(s): RFC XXXX, [RFC 3261](#)
- o Claim Name: "sip\_callid"
- o Claim Description: SIP Call-Id header field value
- o Change Controller: IESG
- o Specification Document(s): RFC XXXX, [RFC 3261](#)
- o Claim Name: "sip\_cseq\_num"
- o Claim Description: SIP CSeq numeric header field parameter value
- o Change Controller: IESG
- o Specification Document(s): RFC XXXX, [RFC 3261](#)
- o Claim Name: "sip\_via\_branch"
- o Claim Description: SIP Via branch header field parameter value
- o Change Controller: IESG
- o Specification Document(s): RFC XXXX, [RFC 3261](#)

## **9. Security Considerations**

As the received-realm Via header field parameter can be used to trigger applications, it is important to ensure that the parameter has not been added to the SIP message by an unauthorized SIP entity.

The operator MUST change the key on a frequent basis. The operator also needs to take great care in ensuring that the key used to calculate the JWT signature value is only known by the network entry point adding the received-realm Via header field parameter to a SIP message and the entities that use the parameter value.





A SIP entity MUST NOT use the adjacent network information if the values of the JWT claims representing SIP header field values do not match the values of the associated SIP header field values.

A SIP entity MUST use different key values for each parameter value that it recognizes and use to trigger actions.

## **10. Acknowledgements**

Thanks to Adam Roach and Richard Barnes for providing comments and feedback on the document.

## **11. Change Log**

[RFC EDITOR NOTE: Please remove this section when publishing]

Changes from [draft-holmberg-dispatch-received-realm-01](#)

- o Define received-realm parameter value as a JSON Web Token (JWT).

Changes from [draft-holmberg-dispatch-received-realm-00](#)

- o New version due to expiration of previous version.

Changes from [draft-holmberg-received-realm-04](#)

- o Changed IETF WG from sipcore to dispatch.
- o HMAC value added to the parameter.

Changes from [draft-holmberg-received-realm-03](#)

- o New version due to expiration.

Changes from [draft-holmberg-received-realm-02](#)

- o New version due to expiration.

Changes from [draft-holmberg-received-realm-01](#)

- o New version due to expiration.

Changes from [draft-holmberg-received-realm-00](#)

- o New version due to expiration.



## **12. References**

### **12.1. Normative References**

- [RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", [BCP 14](#), [RFC 2119](#), DOI 10.17487/RFC2119, March 1997, <<http://www.rfc-editor.org/info/rfc2119>>.
- [RFC3261] Rosenberg, J., Schulzrinne, H., Camarillo, G., Johnston, A., Peterson, J., Sparks, R., Handley, M., and E. Schooler, "SIP: Session Initiation Protocol", [RFC 3261](#), DOI 10.17487/RFC3261, June 2002, <<http://www.rfc-editor.org/info/rfc3261>>.
- [RFC5234] Crocker, D., Ed. and P. Overell, "Augmented BNF for Syntax Specifications: ABNF", STD 68, [RFC 5234](#), DOI 10.17487/RFC5234, January 2008, <<http://www.rfc-editor.org/info/rfc5234>>.
- [RFC7519] Jones, M., Bradley, J., and N. Sakimura, "JSON Web Token (JWT)", [RFC 7519](#), DOI 10.17487/RFC7519, May 2015, <<http://www.rfc-editor.org/info/rfc7519>>.

### **12.2. Informative References**

- [RFC2104] Krawczyk, H., Bellare, M., and R. Canetti, "HMAC: Keyed-Hashing for Message Authentication", [RFC 2104](#), DOI 10.17487/RFC2104, February 1997, <<http://www.rfc-editor.org/info/rfc2104>>.
- [RFC3968] Camarillo, G., "The Internet Assigned Number Authority (IANA) Header Field Parameter Registry for the Session Initiation Protocol (SIP)", [BCP 98](#), [RFC 3968](#), DOI 10.17487/RFC3968, December 2004, <<http://www.rfc-editor.org/info/rfc3968>>.

#### Authors' Addresses

Christer Holmberg  
Ericsson  
Hirsalantie 11  
Jorvas 02420  
Finland

Email: [christer.holmberg@ericsson.com](mailto:christer.holmberg@ericsson.com)



Yi Jiang  
China Mobile  
No.32 Xuanwumen West Street  
Beijing Xicheng District 100053  
P.R. China

Email: [jiangyi@chinamobile.com](mailto:jiangyi@chinamobile.com)