

Network Working Group
Internet-Draft
Intended status: Standards Track
Expires: 21 October 2022

C. Wendt
Somos Inc.
19 April 2022

Identity Header Error Handling
draft-ietf-stir-identity-header-errors-handling-01

Abstract

This document extends STIR and the Authenticated Identity Management in the Session Initiation Protocol (SIP) error handling procedures to include the mapping of verification failure reasons to STIR defined 4xx codes so the failure reason of an Identity header field can be conveyed to the upstream authentication service when local policy dictates that the call should continue in the presence of a verification failure. This document also defines procedures that enable a failure reason to be mapped to a specific Identity header for scenarios that use multiple Identity header fields where some may have errors and others may not and the handling of those situations is defined.

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 <https://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 21 October 2022.

Copyright Notice

Copyright (c) 2022 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 (<https://trustee.ietf.org/license-info>) in effect on the date of publication of this document.

Internet-Draft

Identity Errors

April 2022

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 Revised BSD License text as described in Section 4.e of the [Trust Legal Provisions](#) and are provided without warranty as described in the Revised BSD License.

Table of Contents

| | | |
|---------------------|--|-------------------|
| 1. | Introduction | 2 |
| 2. | Terminology | 3 |
| 3. | Reason header field protocol "STIR" | 3 |
| 4. | Use of provisional error responses to signal errors without terminating the call | 3 |
| 5. | Handling of a verification error when there are multiple Identity header fields | 3 |
| 6. | Handling multiple verification errors | 4 |
| 7. | Removal of the Reason header field by Authentication Service | 5 |
| 8. | IANA Considerations | 5 |
| 9. | Acknowledgements | 5 |
| 10. | Security Considerations | 6 |
| 11. | Normative References | 6 |
| | Author's Address | 7 |

[1.](#) Introduction

[RFC8224] in [Section 6.2.2](#) discusses future specifications for enhancement of how errors are communicated and the handling of multiple Identity header fields. This specification provides some additional mechanisms for solutions to address these problems.

In some deployments of STIR and specifically using SIP [[RFC3261](#)] as defined by [[RFC8224](#)], one issue with the current error handling, specifically with the use of the defined 4xx error responses, is that when an error occurs with the verification of the Identity header field or the PASSporT contained in the Identity header field and a 4xx response is returned, the call is then terminated. It may be the case that the policy for handling errors dictates that calls should continue even if there is a verification error, in the case of, for example inadvertent errors, however the authentication service should still be notified of the error so that corrective action can be taken. This specification will discuss the use of the Reason header field in subsequent provisional (1xx) responses in order to

accomplish this.

For the handling of multiple Identity header fields and the potential situation that some of the Identity header fields in a call may pass verification but others may have errors, this document provides a

mechanism to add an identifier so that the authentication service can identify which Identity header field is being referred to in the case of an error.

[2.](#) Terminology

The keywords "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "NOT RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in [BCP 14](#) [[RFC2119](#)] [[RFC8174](#)] when, and only when, they appear in all capitals, as shown here.

[3.](#) Reason header field protocol "STIR"

This specification defines a new Reason header field [[RFC3326](#)] protocol "STIR" for STIR applications using SIP as defined in [[RFC8224](#)]. This will differentiate current protocols, specifically "SIP" which is currently in wide industry usage, from the [[RFC8224](#)] defined error cause codes and the potential use of multiple Reason header fields defined in [[RFC3326](#)] and updated in [upcoming document TBD] allowing multiple Reason header fields with the same "STIR" protocol string. The use of multiple Reason header field is discussed in more detail later in the document.

[4.](#) Use of provisional error responses to signal errors without terminating the call

In cases where local policy dictates that a call should continue regardless of any verification errors that may have occurred, including 4XX errors described in [[RFC8224](#)] [Section 6.2.2](#), then the verification service SHOULD NOT send the 4XX as a response, but rather include the error response code and reason phrase in a Reason header field, defined in [[RFC3326](#)], in the next provisional or final responses sent to the authentication service.

Example Reason header field:

Reason: STIR ;cause=436 ;text="Bad Identity Info"

5. Handling of a verification error when there are multiple Identity header fields

In cases where a SIP message includes multiple Identity header fields and one of those Identity header fields has an error, the verification service SHOULD include the error response code and reason phrase associated with the error in a Reason header field, defined in [\[RFC3326\]](#), in the next provisional or final responses sent to the authentication service. The reason cause in the Reason header

Wendt

Expires 21 October 2022

[Page 3]

Internet-Draft

Identity Errors

April 2022

field SHOULD represent the error that occurred when verifying the contents of the Identity header field. The association of a Reason header field and error to a specific Identity header field is accomplished by adding a "ppt" parameter containing the PASSport that generated the error to the Reason header field. The "ppt" parameter for the Reason header field is optional, but RECOMMENDED, in particular for cases that a SIP INVITE contains multiple Identity header fields. The PASSport can be included in full form, or optionally in compact form, where only the signature of the PASSport is used to identify the reported Identity header field with an error.

Example Reason header field with full form PASSport:

```
Reason: STIR ;cause=436 ;text="Bad Identity Info" ;ppt= \
"eyJhbGciOiJIUzI1NiIsInR5cCI6ImlwIiwiaXNjaHR0cHM6Ly9jZXJ0LmV4YW1wbGUub3JnL3Bhc3Nwb3J0LmNlciJ9.eyJ\
kZXN0Ijpb7InVyaSI6WyJzaXA6YWxpY2VAZXhhbXBsZS5jb20iXX0sImVhdC\
I6IjE0NDMyMDgzNDUiLCJvcmlnIjpb7InRuIjoimTIxNTU1NTEyMTIifX0.r\
q3pjT1hoRwakEGjHCnWSwUnshd0-zJ6F1V0gFWSjHBr8Qjpjlk-cpFYpFYs\
ojNCpTz03QfP0lckGaS6hEck7w"
```

Example Reason header field with compact form PASSport: ~~~~~~

```
Reason: STIR ;cause=436 ;text="Bad Identity Info" ;ppt= \
"..rq3pjT1akEGjHCnWSwUnshd0-zJ6F1V0gFWSjHBr8Qjpjlk-cpFYpFYs\
ojNCpTz03QfP0lckGaS6hEck7w" ~~~~~~
```

6. Handling multiple verification errors

If there are multiple Identity header field verification errors being

reported the verification service SHOULD include corresponding Reason header fields with "ppt" parameters including full or compact form of the PASSporT with cause and text parameters identifying each error. As mentioned previously, the potential use of multiple Reason header fields defined in [\[RFC3326\]](#) is updated in [\[I-D.sparks-sipcore-multiple-reasons\]](#) allowing multiple Reason header fields with the same protocol value, for this specification being "STIR".

Example Reason header fields for two identity info errors:

```
Reason: STIR ;cause=436 ;text="Bad Identity Info" ;ppt= \
"eyJhbGciOiJFUzI1NiIsInR5cCI6InBhc3Nwb3J0IiwieDV1Ii \
joiaHR0cHM6Ly9jZXJ0LmV4YW1wbGUub3JnL3Bhc3Nwb3J0LmNlciJ9.eyJ \
kZXN0Ijp7InVyaSI6WyJzaXA6YWxpY2VAZXhhbXBsZS5jb20iXX0sImIhdC \
I6IjE0NDMyMDgzNDUiLCJvcmlnIjp7InRuIjoimTIxNTU1NTEyMTIifX0.r \
q3pjT1hoRwakEGjHCnWSwUnshd0-zJ6F1VOgFWSjHBr8Qjpjlk-cpFYpFYs \
ojNCpTz03QfP0lckGaS6hEck7w"
```

```
Reason: STIR ;cause=436 ; text="Bad Identity Info" ;ppt= \
"eyJhbGciOiJFUzI1NiIsInR5cCI6InBhc3Nwb3J0IiwieDV1Ii \
joiaHR0cHM6Ly9jZXJ0LmV4YW1wbGUub3JnL3Bhc3Nwb3J0LmNlciJ9.eyJ \
xpY2VAZXhhbXBsZS5jb20iXX0sImIhdCkZXN0Ijp7InVyaSI6WyJzaXA6YW \
p7InRuIjoimTIxNTU1NTEyMTIifX0I6IjE0NDMyMDgzNDUiLCJvcmlnIj.r \
J6F1VOgFWSjHBr8Qjpjlk-cpFYpFYsq3pjT1hoRwakEGjHCnWSwUnshd0-z \
ckGaS6hEck7wojNCpTz03QfP0l"
```

[7.](#) Removal of the Reason header field by Authentication Service

When an Authentication Service [\[RFC8224\]](#) receives the Reason header field with a PASSporT it generated as part of an Identity header field and the authentication of a call, it should first follow local policy to recognize and acknowledge the error (e.g. perform

operational actions like logging or alarming), but then MUST remove the identified Reason header field to avoid the PASSporT information from going upstream to a UAC or UAS that may not be authorized to see claim information contained in the PASSporT for privacy or other reasons.

8. IANA Considerations

This document requests the definition of a new protocol value (and associated protocol cause) to be registered by the IANA into the "Reason Protocols" sub-registry under <http://www.iana.org/assignments/sip-parameter> as follows:

| Protocol Value | Protocol Cause | Reference |
|----------------|----------------|--------------------------|
| ----- | ----- | ----- |
| STIR | Status code | RFC 8224 |

9. Acknowledgements

Would like to thank David Hancock for help to identify these error scenarios and Jon Peterson, Roman Shpount, Robert Sparks and STIR working group for helpful feedback and discussion.

10. Security Considerations

This specification discusses the use of a PASSporT as an identifier for cases where there is multiple identity header errors occurring as part of the Reason header field response. For some call scenarios (e.g. diversion based call flows) the signer of the PASSporT(s) may not be the first hop initiator of the call. In those cases, there may be some security or privacy concerns associated with PASSporT information that is passed beyond the authentication service that originally signed the PASSporT(s) in the resulting error Reason header field. This specification states the authentication service MUST remove the Reason header field with the PASSporT to protect the security (e.g. use of potentially still fresh PASSporT for replay attacks) and privacy of any potential information that could be passed beyond the authentication service response back in the

direction of the call initiator. This is just to reinforce this MUST as a security consideration that should be followed.

11. Normative References

- [I-D.sparks-sipcore-multiple-reasons]
Sparks, R., "Multiple SIP Reason Header Field Values",
Work in Progress, Internet-Draft, [draft-sparks-sipcore-multiple-reasons-00](https://www.ietf.org/archive/id/draft-sparks-sipcore-multiple-reasons-00), 12 November 2021,
<<https://www.ietf.org/archive/id/draft-sparks-sipcore-multiple-reasons-00.txt>>.
- [RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", [BCP 14](#), [RFC 2119](#),
DOI 10.17487/RFC2119, March 1997,
<<https://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,
<<https://www.rfc-editor.org/info/rfc3261>>.
- [RFC3326] Schulzrinne, H., Oran, D., and G. Camarillo, "The Reason Header Field for the Session Initiation Protocol (SIP)", [RFC 3326](#), DOI 10.17487/RFC3326, December 2002,
<<https://www.rfc-editor.org/info/rfc3326>>.
- [RFC8174] Leiba, B., "Ambiguity of Uppercase vs Lowercase in [RFC 2119](#) Key Words", [BCP 14](#), [RFC 8174](#), DOI 10.17487/RFC8174, May 2017, <<https://www.rfc-editor.org/info/rfc8174>>.

Wendt

Expires 21 October 2022

[Page 6]

Internet-Draft

Identity Errors

April 2022

- [RFC8224] Peterson, J., Jennings, C., Rescorla, E., and C. Wendt, "Authenticated Identity Management in the Session Initiation Protocol (SIP)", [RFC 8224](#),
DOI 10.17487/RFC8224, February 2018,
<<https://www.rfc-editor.org/info/rfc8224>>.

Author's Address

Chris Wendt
Somos Inc.
Email: chris-ietf@chriswendt.net