Workgroup: STIR Working Group
Internet-Draft:
draft-ietf-stir-identity-header-errors-
handling-07
Published: 7 November 2022
Intended Status: Standards Track
Expires: 11 May 2023
Authors: C. Wendt
Somos Inc.

Identity Header Errors Handling for STIR

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 field 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 11 May 2023.

Table of Contents

1. Introduction

The STIR framework as described in [RFC7340] is an authentication framework for asserting a telephone number or URI based identity using a digital signature and certificate based framework as described in [RFC8225] and [RFC8226] respectively. [RFC8224] describes the use of the STIR framework in the SIP protocol [RFC3261] and defines both the authentication service that creates a PASSporT, defined in [RFC8225], and delivers it in an Identity header field and the verification service that correspondingly verifies the PASSporT and embedded originating identity.

This document is concerned with errors in validating PASSporTs and Identity header fields and how they are communicated in special cases and defines a solution to help address the potential issue of multiple Identity header fields and the plurality of potential verification errors. Additionally, it addresses the issue of the current 4xx error response and that when there is a verification error, the call is terminated. In some deployments, it may be the case that the policy for handling errors dictates that calls should continue even if there is a verification error. In many cases of, for example, inadvertent or operational errors that do not represent

any identity falsification type of attempt, the policy of continuing the call even though the identity is not verified, may be the preferred policy. In these cases, the authentication service should still be notified of the error so that corrective action can be taken to fix any issues. This specification will discuss the use of the Reason header field in subsequent provisional (1xx) responses in order to deliver the error back to the authentication service or other SIP path network equipment responsible for error handling.

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 defines the method of adding an identifier so that the authentication service can uniquely 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 document defines a new Reason header field [RFC3326] protocol "STIR" for STIR applications using SIP as defined in [RFC8224]. The use of "STIR" as a reason header field protocol with the [RFC8224] defined error cause codes allows the use of multiple Reason header fields defined in [RFC3326] and updated in [I-D.ietf-sipcore-multiple-reasons]. Any provisional SIP Response message or final response message, with the exception of a 100 (Trying), MAY contain one or more Reason header fields with a STIR related cause code defined in [RFC8224] or future specifications. The use of multiple Reason header field is discussed in more detail later in the document.

4. Use of provisional response 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 occured, including 4XX errors described in [RFC8224] Section 6.2.2, then the verification service MUST 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 MUST 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 field MUST 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 PASSporT identifier, "ppi", parameter containing the PASSporT string as an identifier for the identity header and corresponding PASSporT that generated the error to the Reason header field. The "ppi" parameter for the Reason header field is RECOMMENDED in particular for cases that a SIP INVITE contains multiple Identity header fields. As implied and defined in [RFC8224], error codes associated with STIR targeted at authentication services that produced a specific identity header field represent a single error occurring with the verification and processing of that identity header field. Therefore the association of a "ppi" parameter with a Reason header field using "STIR" protocol MUST only identify a single cause code in the context of a call dialog defined in [RFC8224] or in future documents defining STIR related errors. The PASSporT can be included in full form or in compact form, where only the signature of the PASSporT is included with two periods as a prefix as defined in [RFC8225] Section 7 to identify the reported Identity header field with an error. Compact form is the recommended form as full form may include information that could have privacy or security implications in some call scenarios as discussed in Section 9.

Example Reason header field with full form PASSporT:

```
Reason: STIR ;cause=436 ;text="Bad Identity Info" ;ppi= \
"eyJhbGciOiJFUzI1NiIsInR5cCI6InBhc3Nwb3J0IiwieDV1I \
joiaHR0cHM6Ly9jZXJ0LmV4YW1wbGUub3JnL3Bhc3Nwb3J0LmNlciJ9.eyJ \
kZXN0Ijp7InVyaSI6WyJzaXA6YWxpY2VAZXhhbXBsZS5jb20iXX0sImlhdC \
I6IjE0NDMyMDgzNDUiLCJvcmlnIjp7InRuIjoiMTIxNTU1NTEyMTIifX0.r \
q3pjT1hoRwakEGjHCnWSwUnshd0-zJ6F1VOgFWSjHBr8Qjpjlk-cpFYpFYs \
ojNCpTzO3QfPOlckGaS6hEck7w"
```

Example Reason header field with compact form PASSporT:

```
Reason: STIR ;cause=436 ;text="Bad Identity Info" ;ppi= \
"..rq3pjT1akEGjHCnWSwUnshd0-zJ6F1VOgFWSjHBr8Qjpjlk-cpFYpFYs \
ojNCpTzO3QfPOlckGaS6hEck7w"
```

6. Handling multiple verification errors

If there are multiple Identity header field verification errors being reported the verification service MUST include a corresponding number of Reason header fields per error. These Reason header fields should include a "ppi" parameters including the 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.ietf-sipcore-multiple-reasons] allowing multiple Reason header fields with the same protocol value, for this specification "STIR" should be used for any STIR error defined in [RFC8224] or future specifications.

Example Reason header fields for two identity info errors:

```
Reason: STIR ;cause=436 ;text="Bad Identity Info" ;ppi=     \
"..rq3pjT1hoRwakEGjHCnWSwUnshd0-zJ6F1VOgFWSjHBr8Qjpjlk-cpFY \
pFYsojNCpTzO3QfPOlckGaS6hEck7w"

Reason: STIR ;cause=438 ; text="Invalid Identity Header" ;ppi=  \
"..rJ6F1VOgFWSjHBr8Qjpjlk-cpFYpFYsq3pjT1hoRwakEGjHCnWSwUnsh \
d0-zckGaS6hEck7wojNCpTzO3QfPOl"
```

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-parameters as follows:

Protocol Value	Protocol Cause	Reference
STIR	STIR Error code	RFC 8224

This document also requests the definition of a new header field parameter name to be registered by IANA into the Header Field Parameters and Parameter Values sub-registry under https://www.iana.org/assignments/sip-parameters as follows:

Header Field	Parameter Name	Predefined Values	Reference
Reason	ppi	No	RFC THIS

9. Security Considerations

This specification discusses the use of a PASSporT as an identifier for cases where there are multiple identity header field errors occuring 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 upstream 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. While this specification allows for both full and compact form of the PASSporT to be used as the error identifier, use of the compact form is RECOMMENDED to avoid the potential exposure of call information contained in the full form of the PASSporT.

10. References

10.1. Normative References

[I-D.ietf-sipcore-multiple-reasons] Sparks, R., "Multiple SIP Reason Header Field Values", Work in Progress, Internet-Draft, draft-ietf-sipcore-multiple-reasons-01, 23 August 2022, <https://www.ietf.org/archive/id/draft-ietf-sipcore-multiple-reasons-01.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>.

[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>.

[RFC8225] Wendt, C. and J. Peterson, "PASSporT: Personal Assertion Token", RFC 8225, DOI 10.17487/RFC8225, February 2018, <https://www.rfc-editor.org/info/rfc8225>.

[RFC8226] Peterson, J. and S. Turner, "Secure Telephone Identity Credentials: Certificates", RFC 8226, DOI 10.17487/RFC8226, February 2018, <https://www.rfc-editor.org/info/rfc8226>.

10.2. Informative References

[RFC7340] Peterson, J., Schulzrinne, H., and H. Tschofenig, "Secure Telephone Identity Problem Statement and Requirements", RFC 7340, DOI 10.17487/RFC7340, September 2014, <https://www.rfc-editor.org/info/rfc7340>.

Appendix A. Acknowledgements

The author would like to thank David Hancock for help to identify these error scenarios and additionally Jon Peterson, Roman Shpount, Robert Sparks, Christer Holmberg and others in the STIR working group for their helpful feedback and discussion.

Author's Address

Chris Wendt
Somos Inc.

Email: chris-ietf@chriswendt.net