Internet Engineering Task Force (IETF)
Request for Comments: 9410
Category: Standards Track
ISSN: 2070-1721

C. Wendt
Somos Inc.

July 2023

# Handling of Identity Header Errors for Secure Telephone Identity Revisited (STIR)

## Abstract

This document extends the current error-handling procedures for mapping of verification failure reasons to 4xx codes for Secure Telephone Identity Revisited (STIR) and the Authenticated Identity Management in the Session Initiation Protocol (SIP). It extends the ability to use the Reason header field as an option for conveying an error associated with an Identity header field 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. The handling of those situations is also defined.

## Status of This Memo

This is an Internet Standards Track document.

This document is a product of the Internet Engineering Task Force (IETF). It represents the consensus of the IETF community. It has received public review and has been approved for publication by the Internet Engineering Steering Group (IESG). Further information on Internet Standards is available in Section 2 of RFC 7841.

Information about the current status of this document, any errata, and how to provide feedback on it may be obtained at https://www.rfc-editor.org/info/rfc9410.



## 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 [RFC8225] and [RFC8226], respectively. [RFC8224] describes the use of the STIR framework in the SIP protocol [RFC3261]. It defines both a) the authentication service that creates a PASSporT [RFC8225] and delivers it in an Identity header field, and b) 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. This document also 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, i.e., the call is terminated when a verification error is present. 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. For example, in many cases of inadvertent or operational errors that do not represent any type of identity falsification attempt, the preferred policy may be to continue the call despite the unverified identity. 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.

To handle multiple Identity header fields where some in a call may be verified while others may not (i.e., they have errors), this document defines a method by which an identifier is added to the header 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 key words "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 error defined in [RFC8224] causes codes to allow the use of multiple Reason header fields as detailed in [RFC3326] and updated in [RFC9366]. 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 fields 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 occurred, including 4xx errors described in Section 6.2.2 of [RFC8224], the verification service MUST NOT send the 4xx as a response. Rather, it should include the error response code and reason phrase in a Reason header field in the next provisional or final response it sends 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. For a SIP INVITE containing multiple Identity header fields, the "ppi" parameter for the Reason header field is RECOMMENDED. As defined in [RFC8224], the STIR error codes used in responses are based on an error associated with a specific Identity header field representing a single error occurring with the verification and processing of that Identity header field. The association of a "ppi" parameter with a Reason header field [RFC3326] using the protocol value of "STIR" defined in this document MUST only identify a single cause code [RFC3326] in the context of a call dialog [RFC3261] corresponding only to the STIR-related error codes defined in [RFC8224] or future documents defining STIR-related error codes. The associated PASSporT object can be included either 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 Section 7 of [RFC8225], 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; this is discussed in Section 9.

Example Reason header field with a 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 a 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" parameter, 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 [RFC9366], 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). Then, it MUST remove the identified Reason header field to avoid the PASSporT information from going upstream to a User Agent Client (UAC) or User Agent Server (UAS) that may not be authorized to see claim information contained in the PASSporT for privacy or other reasons.

## 8. IANA Considerations

IANA has registered the following new protocol value (and associated protocol cause) in the "Reason Protocols" registry under <http://www.iana.org/assignments/sip-parameters>:

| Protocol Value | Protocol Cause | Reference |
|---|---|---|
| STIR | STIR Error code | [RFC8224] |

Table 1

IANA has also registered a new header field parameter name in the "Header Field Parameters and Parameter Values" registry under <https://www.iana.org/assignments/sip-parameters>:

| Header Field | Parameter Name | Predefined Values | Reference |
|---|---|---|---|
| Reason | ppi | No | RFC 9410 |

Table 2

## 9. Security Considerations

This specification discusses the use of a PASSporT as an identifier for cases where there are multiple identity header field 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 upstream beyond the

authentication service that originally signed the PASSporT(s) in the resulting error Reason header field. This specification states that the authentication service MUST remove the Reason header field with the PASSporT to protect the security (e.g., use of a 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 the 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


[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>.

[RFC9366] Sparks, R., "Multiple SIP Reason Header Field Values", RFC 9366, DOI 10.17487/RFC9366, March 2023, <https://www.rfc-editor.org/info/rfc9366>.


## 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>.


# Acknowledgements


The author would like to thank David Hancock for help identifying these error scenarios, as well as 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