Network Working Group
Internet-Draft
Updates: 8226 (if approved)
Intended status: Standards Track
Expires: 25 July 2021

R. Housley
Vigil Security

21 January 2021

Enhanced JWT Claim Constraints for STIR Certificates
draft-housley-stir-enhance-rfc8226-00

Abstract

RFC 8226 provides a certificate extension to constrain the JWT claims that can be included in the PASSporT as defined in RFC 8225. If the signer includes a JWT claim outside the constraint boundaries, then the recipient will reject the entire PASSporT. This document defines additional ways that the JWT claims can be constrained.

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 25 July 2021.

Table of Contents

1. Introduction

The use of certificates [RFC5280] in establishing authority over telephone numbers is described in [RFC8226].

Section 8 of [RFC8226] provides a certificate extension to constrain the JWT claims that can be included in the PASSporT [RFC8225]. If the signer includes a JWT claim outside the constraint boundaries, then the recipient will reject the entire PASSporT.

This document defines an enhanced JWTClaimConstraints certificate extension, which provides all of the capabilities available in the original certificate extension as well as some additional ways to constrain the allowable JWT claims.

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. Enhanced JWT Claim Constraints Syntax

Certificate subjects are limited to specific values for PASSporT claims with the Enhanced JWT Claim Constraints certificate extension; issuers permit all claims by omitting the Enhanced JWT Claim Constraints certificate extension from the extension field of the certificate [RFC5280]. The certificate extension is non-critical, applicable only to end-entity certificates, and defined with ASN.1 [X.680]. The syntax of the JWT claims in a PASSporT is specified in [RFC8225].

The Enhanced JWT Claim Constraints certificate extension is optional, but when present, it constrains the JWT claims that authentication services may include in the PASSporT objects they sign. Constraints are applied by certificate issuers and enforced by recipients when validating PASSporT claims as follows:

1. mustInclude indicates JWT claims that MUST appear in the PASSporT in addition to the iat, orig, and dest claims. The baseline PASSporT claims ("iat", "orig", and "dest") are considered to be permitted by default, and these claims SHOULD NOT be part of the mustInclude list. If mustInclude is absent, the iat, orig, and dest claims MUST appear in the PASSporT.

2. permittedValues indicates that if the claim name is present, the claim MUST contain one of the listed values.

3. mustExclude indicates JWT claims that MUST NOT appear in the PASSporT. in addition to the iat, orig, and dest claims. The baseline PASSporT claims ("iat", "orig", and "dest") are considered to be permitted by default, and these claims MUST NOT be part of the mustExclude list.

4. excludedValues indicates that if the claim name is present, the claim MUST NOT contain any of the listed values.

The Enhanced JWT Claim Constraints certificate extension is identified by the following object identifier (OID):

```
id-pe-eJWTClaimConstraints OBJECT IDENTIFIER ::= { id-pe TBD1 }
```

The Enhanced JWT Claim Constraints certificate extension has the following syntax:

```
EnhancedJWTClaimConstraints ::= SEQUENCE {
  mustInclude [0] JWTClaimNames OPTIONAL,
    -- The listed claim names MUST appear in the PASSporT
    -- in addition to iat, orig, and dest. If absent, iat, orig,
    -- and dest MUST appear in the PASSporT.
  permittedValues [1] JWTClaimValuesList OPTIONAL,
    -- If the claim name is present, the claim MUST contain one
    -- of the listed values.
  mustExclude [2] JWTClaimNames OPTIONAL,
    -- The listed claim names MUST NOT appear in the PASSporT.
  excludedValues [3] JWTClaimValuesList OPTIONAL }
    -- If the claim name is present, the claim MUST NOT contain
    -- any of the listed values.
```

```
( WITH COMPONENTS { ..., mustInclude PRESENT } |
  WITH COMPONENTS { ..., permittedValues PRESENT } |
  WITH COMPONENTS { ..., mustExclude PRESENT } |
  WITH COMPONENTS { ..., excludedValues PRESENT } )

JWTClaimValuesList ::= SEQUENCE SIZE (1..MAX) OF JWTClaimValues

JWTClaimValues ::= SEQUENCE {
  claim JWTClaimName,
  values SEQUENCE SIZE (1..MAX) OF UTF8String }

JWTClaimNames ::= SEQUENCE SIZE (1..MAX) OF JWTClaimName

JWTClaimName ::= IA5String
```

4. Examples

Consider two examples with a PASSporT claim called "confidence" with values "low", "medium", and "high":

* If a CA issues to an authentication service certificate that includes an Enhanced JWT Claim Constraints certificate extension that contains the mustInclude JWTClaimName "confidence", then an authentication service is required to include the "confidence" claim in all PASSporTs it generates and signs; a verification service will treat as invalid any PASSporT it receives with a PASSporT claim that does not include the "confidence" claim.

* If a CA issues to an authentication service certificate that includes an Enhanced JWT Claim Constraints certificate extension that contains the permittedValues JWTClaimName "confidence" and a permitted "high" value, then a recipient authentication service will treat as invalid any PASSporT it receives with a PASSporT "confidence" claim with a value other than "high". However, a recipient authentication service will not treat as invalid a PASSporT it receives without a PASSporT "confidence" claim at all.

* If a CA issues to an authentication service certificate that includes an Enhanced JWT Claim Constraints certificate extension that contains the mustExclude JWTClaimName "confidence", then a recipient authentication service will treat as invalid any PASSporT it receives with a PASSporT "confidence" claim regardless of the claim value.

* If a CA issues to an authentication service certificate that includes an Enhanced JWT Claim Constraints certificate extension that contains the excludedValues JWTClaimName "confidence" and a permitted "low" value, then a recipient authentication service

will treat as invalid any PASSporT it receives with a PASSporT "confidence" claim with a value of "low". However, a recipient authentication service will not treat as invalid a PASSporT it receives without a PASSporT "confidence" claim at all.

5. IANA Considerations

This document makes use of object identifiers for the Enhanced JWT Claim Constraints certificate extension defined in Section 3 and the ASN.1 module identifier defined in Appendix A. Therefore, IANA is asked to made the following assignments within the SMI Numbers Registry.

For the Enhanced JWT Claim Constraints certificate extension in the "SMI Security for PKIX Certificate Extension" (1.3.6.1.5.5.7.1) registry:

TBD1 id-pe-eJWTClaimConstraints

For the ASN.1 module identifier in the "SMI Security for PKIX Module Identifier" (1.3.6.1.5.5.7.0) registry:

TBD2 id-mod-eJWTClaimConstraints-2021

6. Security Considerations

For further information on certificate security and practices, see [RFC5280], especially the Security Considerations section.

The Enhanced JWT Claim Constraints certificate extension can be used by certificate issuers to provide limits on the acceptable PASSporT that will be accepted by recipient verification services. Enforcement of these limits depends upon proper implementation by the recipient verification services. The digital signature on the PASSportT data structure will be valid even if the limits are violated.

7. Acknowledgements

Many thanks to Chris Wendt for his insight into the need for the for the Enhanced JWT Claim Constraints certificate extension.

8. References

8.1. 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>.

[RFC5280] Cooper, D., Santesson, S., Farrell, S., Boeyen, S., Housley, R., and W. Polk, "Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile", RFC 5280, DOI 10.17487/RFC5280, May 2008, <https://www.rfc-editor.org/info/rfc5280>.

[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>.

[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>.

[X.680] International Telecommunication Union, "Information Technology - Abstract Syntax Notation One (ASN.1): Specification of basic notation", ISO/IEC 8824-1, August 2021.

8.2. Informative References

[RFC5912] Hoffman, P. and J. Schaad, "New ASN.1 Modules for the Public Key Infrastructure Using X.509 (PKIX)", RFC 5912, DOI 10.17487/RFC5912, June 2010, <https://www.rfc-editor.org/info/rfc5912>.

Appendix A. ASN.1 Module

This appendix provides the ASN.1 [X.680] definitions for the Enhanced JWT Claim Constraints certificate extension. The module defined in this appendix are compatible with the ASN.1 specifications published in 2015.

This ASN.1 module imports ASN.1 from [RFC5912].

```
<CODE BEGINS>
EnhancedJWTClaimConstraints-2021
  { iso(1) identified-organization(3) dod(6) internet(1)
    security(5) mechanisms(5) pkix(7) id-mod(0)
    id-mod-eJWTClaimConstraints-2021(TBD2) }

DEFINITIONS EXPLICIT TAGS ::= BEGIN

IMPORTS

id-pe
FROM PKIX1Explicit-2009  -- From RFC 5912
  { iso(1) identified-organization(3) dod(6) internet(1)
    security(5) mechanisms(5) pkix(7) id-mod(0)
    id-mod-pkix1-explicit-02(51) }

EXTENSION
FROM PKIX-CommonTypes-2009  -- From RFC 5912
  { iso(1) identified-organization(3) dod(6) internet(1)
    security(5) mechanisms(5) pkix(7) id-mod(0)
    id-mod-pkixCommon-02(57) } ;

-- Enhanced JWT Claim Constraints Certificate Extension

ext-eJWTClaimConstraints EXTENSION ::= {
  SYNTAX EnhancedJWTClaimConstraints
  IDENTIFIED BY id-pe-JWTClaimConstraints }

id-pe-eJWTClaimConstraints OBJECT IDENTIFIER ::= { id-pe TBD1 }

EnhancedJWTClaimConstraints ::= SEQUENCE {
  mustInclude [0] JWTClaimNames OPTIONAL,
    -- The listed claim names MUST appear in the PASSporT
    -- in addition to iat, orig, and dest.  If absent, iat, orig,
    -- and dest MUST appear in the PASSporT.
  permittedValues [1] JWTClaimValuesList OPTIONAL,
    -- If the claim name is present, the claim MUST contain one
    -- of the listed values.
  mustExclude [2] JWTClaimNames OPTIONAL,
    -- The listed claim names MUST NOT appear in the PASSporT.
  excludedValues [3] JWTClaimValuesList OPTIONAL }
    -- If the claim name is present, the claim MUST NOT contain
    -- any of the listed values.
( WITH COMPONENTS { ..., mustInclude PRESENT } |
  WITH COMPONENTS { ..., permittedValues PRESENT } |
  WITH COMPONENTS { ..., mustExclude PRESENT } |
  WITH COMPONENTS { ..., excludedValues PRESENT } )
```

```
   JWTClaimValuesList ::= SEQUENCE SIZE (1..MAX) OF JWTClaimValues

   JWTClaimValues ::= SEQUENCE {
     claim JWTClaimName,
     values SEQUENCE SIZE (1..MAX) OF UTF8String }

   JWTClaimNames ::= SEQUENCE SIZE (1..MAX) OF JWTClaimName

   JWTClaimName ::= IA5String

   END
   <CODE ENDS>
```

Author's Address

Russ Housley
Vigil Security, LLC
516 Dranesville Road
Herndon, VA, 20170
United States of America

Email: housley@vigilsec.com