

Network Working Group
Internet-Draft
Updates: [8226](#) (if approved)
Intended status: Standards Track
Expires: 17 October 2021

R. Housley
Vigil Security
15 April 2021

Enhanced JWT Claim Constraints for STIR Certificates
draft-ietf-stir-enhance-rfc8226-02

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 an additional way 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 17 October 2021.

Copyright Notice

Copyright (c) 2021 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. 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

1.	Introduction	2
2.	Terminology	2
3.	Enhanced JWT Claim Constraints Syntax	3
4.	Usage Examples	4
5.	Certificate Extension Example	5
6.	IANA Considerations	6
7.	Security Considerations	7
8.	Acknowledgements	8
9.	References	8
9.1.	Normative References	8
9.2.	Informative References	8
Appendix A.	ASN.1 Module	9
	Author's Address	10

[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 an additional way to constrain the allowable JWT claims. That is, the enhanced extension can provide a list of claims that are not allowed to be included in the PASSporT.

[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

The Enhanced JWT Claim Constraints certificate extension limits the PASSport claims and the claim values that can successfully validated by the certificate that contains the extension. Certificate 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 required by [RFC8225], 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 exactly match one of the listed values.
3. `mustExclude` indicates JWT claims that MUST NOT appear in the PASSport. The baseline PASSport claims ("`iat`", "`orig`", and "`dest`") are always permitted, and these claims MUST NOT be part of the `mustExclude` list.

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 }
( WITH COMPONENTS { ..., mustInclude PRESENT } |
  WITH COMPONENTS { ..., permittedValues PRESENT } |
  WITH COMPONENTS { ..., mustExclude 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. Usage Examples

Consider these usage examples with a PASSporT claim called "confidence" with values "low", "medium", and "high". These examples illustrate the constraints that are imposed by mustInclude, permittedValues, and mustExclude:

- * 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 without a "confidence" PASSporT 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 verification service will treat as invalid any PASSporT it receives with a PASSporT "confidence" claim with a value other than "high". However, a verification 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 verification service will treat as invalid any PASSporT it receives with a PASSporT "confidence" claim regardless of the claim value.

5. Certificate Extension Example

A certificate containing an example of the EnhancedJWTClaimConstraints certificate extension is provided in Figure 1. The certificate is provided in the format described in [RFC7468]. The example of the EnhancedJWTClaimConstraints extension from the certificate is shown in Figure 2. The example imposes four constraints:

1. The "confidence" claim must be present in the PASSporT.
2. The "confidence" claim must have a value of "high" or "medium".
3. The "priority" claim must not be present in the PASSporT.

NOTE: This certificate in Figure 1 will need to be corrected once IANA assigns the object identifier for the certificate extension.

```
-----BEGIN CERTIFICATE-----
MIICqjCCAlCgAwIBAgIUH7Zd3rQ5Asv0lzLnzUHhrVhDSlowCgYIKoZIzj0EAwIw
KTElMAkGA1UEBhMCVVMxGjAYBgNVBAMMEUJPR1VTIFNIQUtFTiBST09UMB4XDTIx
MDQxNTEyMTg1NlloXDTIyMDQxNTEyMTg1NlowbDELMAkGA1UEBhMCVVMxCzAJBgNV
BAGMA1ZBMRAwDgYDVQQHDAdlZXJuZG9uMR4wHAYDVQQKDBVDb2d1cyBFeGFtcGxl
IFRlbGVjb20xDTALBgNVBASMBFZvSVAXDzANBgNVBAMMB1NIQUtFTjBZMBMGByqG
SM49AgEGCCqGSM49AwEHA0IABNR6C6nBWRA/fXTglV03aXkXy8hx9oBttVLhsTZ1
IYVRBao40ZhVf/Xv1a3xLsZ6KfdhuylSeAKuCoSbVGojYDGjggERMIIBDTAMBgNV
HRMBAf8EAjAAMA4GA1UdDwEB/wQEAwIHgDAdBgNVHQ4EFgQUd1G3dxHyZKL/FZfS
PI7rpuueRbswHwYDVROjBBgwFoAULToKtrQeFrwwyXpMj1qu3TQEeoEwQgYJYIZI
AYb4QgENBDUWM1RoaxMgY2Vydg1maWNhdGUgY2Fubm90IGJlIHRYdXN0ZWQgZm9y
IGFueSBwdXJwb3NlLjAwBggrBgEFBQcBGgQKMAigBhYEMTIzNDBRBgsrBgEFBQcB
l4+jcARCECgDjAMFgpjb25maWRlbnNlloSAwHjAcFgpjb25maWRlbnNlMA4MBGhp
Z2gMBm1lZG11baIMMAowCHByaw9yaXR5MAoGCCqGSM49BAMCA0gAMEUCIQC1AR9y
WWHoUWH3KZ0UIvBamATHQvjJCyKWuHQIyR6LSAIGWhuf+di772aGlWhMpv5uSua5
ljiGsKx+dMEIE2uU978=
-----END CERTIFICATE-----
```

Figure 1. Example Certificate.


```

0  64: SEQUENCE {
2  14:   [0] {
4  12:     SEQUENCE {
6  10:       IA5String 'confidence'
      :     }
      :   }
18 32:   [1] {
20 30:     SEQUENCE {
22 28:       SEQUENCE {
24 10:         IA5String 'confidence'
36 14:         SEQUENCE {
38  4:           UTF8String 'high'
44  6:           UTF8String 'medium'
      :         }
      :       }
      :     }
      :   }
52 12:   [2] {
54 10:     SEQUENCE {
56  8:       IA5String 'priority'
      :     }
      :   }
      : }

```

Figure 2. Example EnhancedJWTClaimConstraints extension.

6. 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 make 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

7. 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 PASSports that will be accepted by verification services. Enforcement of these limits depends upon proper implementation by the verification services. The digital signature on the PASSportT data structure will be valid even if the limits are violated.

Use of the Enhanced JWT Claim Constraints certificate extension permittedValues constraint is most useful when the claim definition allows a specified set of values. In this way, all of the values that are not listed in the JWTClaimValuesList are prohibited in a valid PASSportT.

Certificate issuers must take care when imposing constraints on the PASSport claims and the claim values that can successfully validated; some combinations can prevent any PASSport from being successfully validated by the certificate. For example, an entry in mustInclude and an entry in mustExclude for the same claim will prevent successful validation on any PASSport.

Certificate issuers must take care when imposing constraints on the PASSport claims and the claim values that can successfully validated; some combinations can prevent any PASSport from being successfully validated by the certificate. For example, an entry in mustInclude and an entry in mustExclude for the same claim will prevent successful validation on any PASSport.

Certificate issuers should not include an entry in mustExclude for the "rcdi" claim for a certificate that will be used with the PASSport Extension for Rich Call Data defined in [\[I-D.ietf-stir-passport-rcd\]](#). Excluding this claim would prevent the integrity protection mechanism from working properly.

Certificate issuers must take care when performing certificate renewal [\[RFC4949\]](#) to include exactly the same Enhanced JWT Claim Constraints certificate extension in the new certificate as the old one. Renewal usually takes place before the old certificate expires, so there is a period of time where both the new certificate and the old certificate are valid. If different constraints appear in the two certificates with the same public key, some PASSports might be valid when one certificate is used and invalid when the other one is used.

8. Acknowledgements

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

Thanks to Ben Campbell for the thoughtful review and comments. The document is much better as a result of the comments.

9. References

9.1. 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>>.
- [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>>.
- [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.

9.2. Informative References

[I-D.ietf-stir-passport-rcd]

Peterson, J. and C. Wendt, "PASSport Extension for Rich Call Data", Work in Progress, Internet-Draft, [draft-ietf-stir-passport-rcd-09](http://www.ietf.org/internet-drafts/draft-ietf-stir-passport-rcd-09), 18 November 2020, <<http://www.ietf.org/internet-drafts/draft-ietf-stir-passport-rcd-09.txt>>.

[RFC4949] Shirey, R., "Internet Security Glossary, Version 2", FYI 36, [RFC 4949](http://www.rfc-editor.org/info/rfc4949), DOI 10.17487/RFC4949, August 2007, <<https://www.rfc-editor.org/info/rfc4949>>.

[RFC7468] Josefsson, S. and S. Leonard, "Textual Encodings of PKIX, PKCS, and CMS Structures", [RFC 7468](http://www.rfc-editor.org/info/rfc7468), DOI 10.17487/RFC7468, April 2015, <<https://www.rfc-editor.org/info/rfc7468>>.

[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-eJWTClaimConstraints }  
  
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.  
( WITH COMPONENTS { ..., mustInclude PRESENT } |  
  WITH COMPONENTS { ..., permittedValues PRESENT } |  
  WITH COMPONENTS { ..., mustExclude 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

