Enhance RFC 8226 JWT Constraints

draft-ietf-stir-enhance-rfc8226-00

Russ Housley

STIR WG

IETF 110

RFC 8226 JWT Constraints

The RFC 8226 syntax could mandate the inclusion of particular claims, but it could not mandate that particular claims cannot be included.

The RFC 8226 syntax could mandate particular claim values, but it could not mandate that particular claim values cannot be included.

```
JWTClaimConstraints ::= SEQUENCE {
   mustInclude [0] JWTClaimNames OPTIONAL,
      -- The listed claim names MUST appear in the PASSporT in addition to iat, orig, dest
      -- If absent, iat, orig, dest MUST appear in the PASSporT
   permittedValues [1] JWTClaimPermittedValuesList OPTIONAL }
      -- If the claim name is present, the claim MUST contain one of the listed values
    ( WITH COMPONENTS { ..., mustInclude PRESENT } |
      WITH COMPONENTS { ..., permittedValues PRESENT } )
```

Enhanced JWT Constraints (1 of 2)

```
EnhancedJWTClaimConstraints ::= SEQUENCE {
  mustInclude [0] JWTClaimNames OPTIONAL,
    -- The listed claim names MUST appear in the PASSporT in addition to iat, orig, dest
    -- If absent, iat, orig, dest MUST appear in the PASSporT
  permittedValues [1] JWTClaimPermittedValuesList 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
   -- The listed claim names MUST NOT contain iat, orig, dest
  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 } )
```

Enhanced JWT Constraints (2 of 2)

```
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
```

Example

```
  0  89: 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'
       :     } }
 66  22:   [3] {
 68  20:     SEQUENCE {
 70  18:       SEQUENCE {
 72   9:         IA5String 'assurance'
 83   5:         SEQUENCE {
 85   3:           UTF8String 'low'
       :   } } } } }
```

The "confidence" claim must be present in the PASSporT

The "confidence" claim must have a value of "high" or "medium"

The "priority" claim must not be present in the PASSporT

The "assurance" claim, if present in the PASSporT, must not have a value of "low"

Way Forward

- There are no outstanding comments
- Ready for STIR WG Last Call?
- Obviously, Robert will make all consensus calls