IETF123 – Madrid
ACME

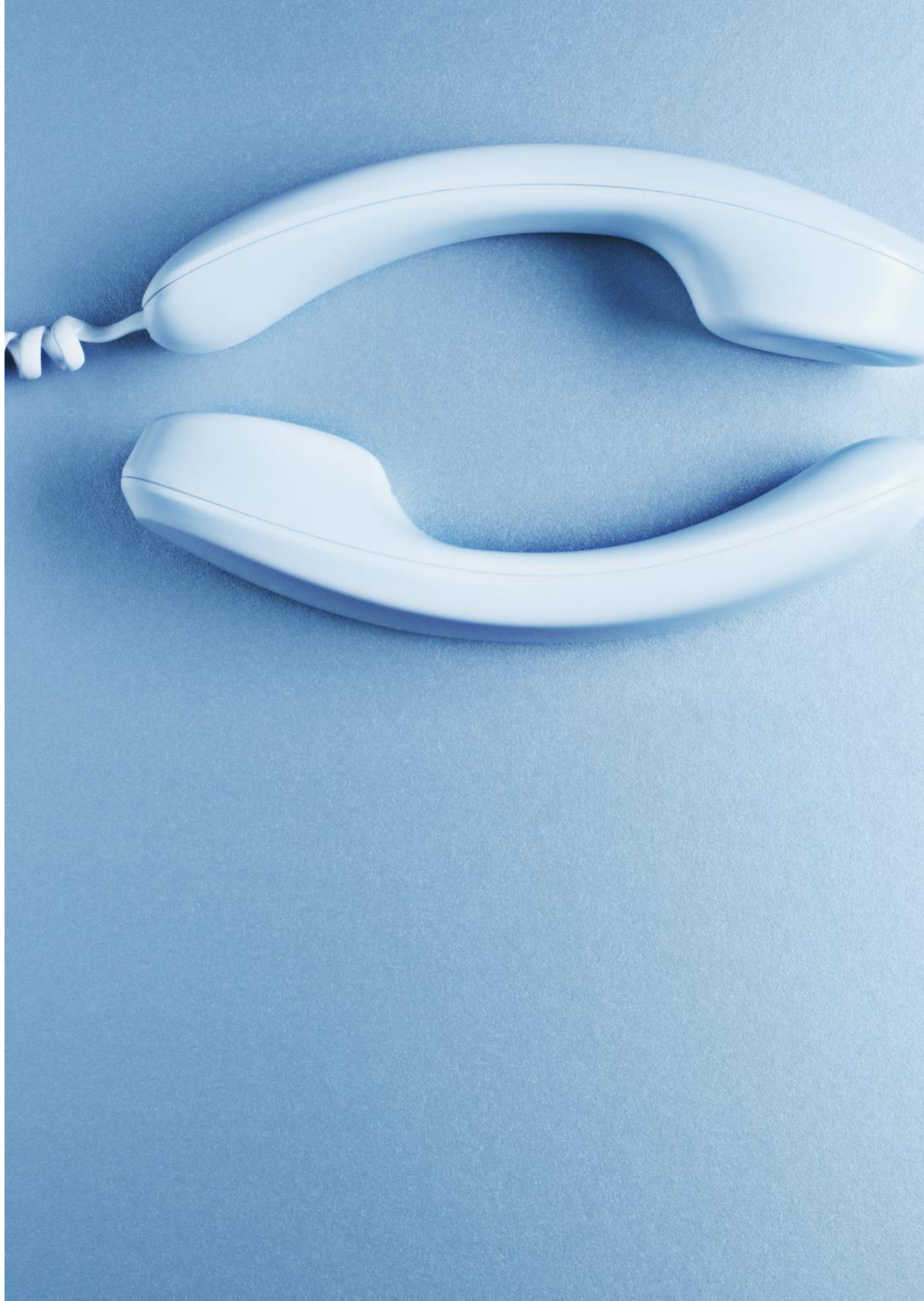
JWTClaimConstraints Authority Token Profile

draft-wendt-acme-authority-token-jwtclaimcon-03

Chris Wendt, David Hancock

Introduction to JWTClaimConstraints Authority Token Draft

- Defines an **Authority Token Profile** for ACME challenge validation specific to JWTClaimConstraints defined in STIR WG.
- Extends the existing Authority Token validation model [RFC9447] to include **JWTClaimConstraints** extension [RFC8226] and extended by **EnhancedJWTClaimConstraints** [RFC9118].



New ACME Challenge

- Defines new ACME Challenge Identifier Type: **JWTClaimConstraints**
- We have existing **TNAuthList Authority Token**
- Want to validate likely STIR cases where both **TNAuthList** and **JWTClaimConstraints** extensions are requested to be added to a certificate and the challenges are validated separately.
- New draft provides examples, want to validate our interpretation of the use of **multiple challenges** is correct

Examples – Authority Token

JWTClaimConstraints Authority Token

```
 {
     "protected": base64url({
       "typ":"JWT",
       "alg":"ES256",
       "x5u":"https://authority.example.org/cert"
     }),
     "payload": base64url({
       "iss":"https://authority.example.org",
       "exp":1640995200,
       "jti":"id6098364921",
       "atc":{"tktype":"JWTClaimConstraints",
         "tkvalue":"F83n2a...avn27DN3",
         "ca":false,
         "fingerprint":"SHA256 56:3E:CF:AE:83:CA:4D:15:B0:29:FF:1B:71:
          D3:BA:B9:19:81:F8:50:9B:DF:4A:D4:39:72:E2:B1:F0:B9:38:E3"}
     }),
     "signature": "9cbg5JO1Gf5YLjjz...SpkUfcdPai9uVYYQ"
   }
```

Examples – Authority Token Request

Body of the POST to the ”Authority” validating allowed JWTClaimConstraints extension

```
{
      "atc": {
        "tktype":"JWTClaimConstraints",
        "tkvalue":"F83n2a...avn27DN3",
        "ca":false,
        "fingerprint":"SHA256 56:3E:CF:AE:83:CA:4D:15:B0:29:FF:1B:71:D3
          :BA:B9:19:81:F8:50:9B:DF:4A:D4:39:72:E2:B1:F0:B9:38:E3"
      }
    }
```

And Response:

```
HTTP/1.1 200 OK
  Content-Type: application/json

  {"token": "DGyRejmCefe7v4N...vb29HhjjLPSggwiE"}
```

Examples – Basic Claim restrictions

```
SEQUENCE {
    mustExclude [2] {
      SEQUENCE {
        IA5String 'attest'
        IA5String 'origid'
        IA5String 'div'
        IA5String 'rph'
        IA5String 'sph'
        IA5String 'rcd'
        IA5String 'rcdi'
        IA5String 'crn'
        }
      }
    }
```

Examples – RCD Claim restrictions

```
SEQUENCE {
    permittedValues [1] {
      SEQUENCE {
        SEQUENCE {
          IA5String 'rcd'
          SEQUENCE {
            UTF8String '"nam": "James Bond"'
            }
          IA5String 'crn'
          SEQUENCE {
            UTF8String '"For your ears only"'
            }
          }
        }
      }
    mustExclude [2] {
      SEQUENCE {
        IA5String 'attest'
        IA5String 'origid'
        IA5String 'div'
        IA5String 'rph'
        IA5String 'sph'
        IA5String 'rcdi'
        }
      }
    }
```

Next Steps

- Seeking ACME WG review and adoption as a working item.
- Will also keep STIR working group in loop for SME input into STIR related details.