Rich Call Data PASSporT extension
draft-ietf-stir-passport-rcd-05

STIR Working Group
IETF106
Overview of update

• Based on very good input of virtual meeting new draft includes

  • Text on usage, specifically 3 modes

    • Basic signing with direct content

    • A MUST for signing with integrity claim digest when there is any URLs as part of RCD

    • A mechanism for explicitly limiting the integrity digest to the certificate for PASSporT signers that are non-authoritative over approving the content of the RCD specifically

• For call-info specific integration it was agreed to define more specific call-info usage so a new draft, draft-wendt-sipcore-call-info-rcd-00 was submitted that specifically will define a new call-info purpose of “jcard”.

• Compact form support was added as well based on reconstructing “rcd” claim from call-info headers and display-name parameter.

• Support for other call-info tokens was removed.
Example of “rcd" PASSporT with “nam”

Protected Header
{
    "alg":"ES256",
    "typ":"passport",
    "ppt":"rcd",
    "x5u":"https://biloxi.example.org/biloxi.cer"
}

Payload
{
    "orig":{"tn":"12025551000"},
    "dest":{"tn":"12025551001"},
    "iat":1443208345,
    "rcd":{"nam":"James Bond"}
}
Example of “rcd” PASSporT with “nam”

Protected Header
{
  "alg":"ES256",
  "typ":"passport",
  "ppt":"rcd",
  "x5u":"https://biloxi.example.org/biloxi.cer"
}

Payload
{
  "orig":{"tn":"12025551000"},
  "dest":{"tn":"12155551001"},
  "iat":1443208345,
  "rcd":{"nam":"James Bond",
      "jcd":{"vcard":{"version":{},"text":"4.0"},
             "fn",{},"text", "James Bond"},
             "n",{},"text",{"Bond","James","",","","Mr."}],
             "adr",{"type":"work"},"text",
             ["",","","3100 Massachusetts Avenue NW","Washington","DC","20008","USA"]},
            ["email",{},"text","007@mi6-hq.com"],
            ["tel",{"type":{"voice","text","cell"},"pref":"1"},"uri",
             "tel:+1-202-555-1000"],
            ["tel",{"type":{"fax"}},"uri","tel:+1-202-555-1001"],
            ["bday",{},"date","19241116"],
            ["logo",{},"uri",
}
Integrity claim

• Provides both a direct and indirect set of mechanisms for verification/approval/policy enforcement of the contents of the rich call data

• “rcdi” - a digest of a canonical form of the “rcd” claim in its entirety, including concatenation of the contents of the URLs.

• Can use JWTConstraints to enforce use of “rcdi” claim and a specific digest value
Integrity claim

• Construction:
  • Pick algorithm for digest
  • Create canonicalized “rcd”
    • lexicographic order of keys
    • white space removal
    • concatenate the base64 encoded content of the resources pointed to by URLs in order of their appearance in re-ordered keys
  • create digest of resulting string
Example of "rcd" PASSporT with "nam", "jcl" and "rcdi"

Protected Header
{
  "alg":"ES256",
  "typ":"passport",
  "ppt":"rcd",
  "x5u":"https://biloxi.example.org/biloxi.cer"
}

Payload
{
  "orig":{"tn":"12025551000"},
  "dest":{"tn":"12155551001"},
  "iat":1443208345,
  "rcd":{"nam":"James Bond","jcl":"https://example.org/james_bond.json"},
  "rcdi":"sha256-H8BRh8j48O9oYatfu5AZzq6A9R6dQZngK7T62em8MUt1FLm52t+eX6xO"
}
Example of ‘rcdi’ claim construction

Example "rcd" claim with URL:
"rcd": { "nam": "James Bond",
        "jcl": "https://example.org/james_bond.json"
    }

Example "rcd" input digest string:
{"nam":"James Bond","jcl":"https://example.org/james_bond.json"};
    ONG##*NCCCDJK123...KLJASlkJlkjsadlf2e3

Example "rcdi" claim:
"rcdi":"sha256-u5AZzq6A9RINQZngK7T62em8M"
JWT Constraints

- In order to enforce the contents of the “rcd” in delegated and other indirect flows STIR certs including JWT Constraints can be used in the STIR certificate

- JWT Constraints would be as follows:
  - a "mustInclude" for the "rcd" claim
  - a "permittedValues" equal to the created "rcdi" claim value string.
Example - with Constraints

Enterprise → TNSP KMS
TN Credentials → RCD digest
RCD - logo/name

TNSP KMS → Call Center
RCD signed → identity header

Call Center - sign call → OSP
RCD identity

OSP → TSP
SHAKEN identity

TSP → STI-CA
Cert w/ constraints