PASSporT-02

STIR Working Group
interim call - May 2016
Chris Wendt

Overview

- Few additions and changes
  - new ES256 example token
  - update to ‘mky’ format
  - change to text on ‘alg’ rules and other proposals from list

ES256 example

ES256 example - signature size 87 characters

```
eyJ0eXAiOiJwYXNzcG9ydCIsImFsZyI6IkVTMjU2IiwieDV1IjoiaHR0cHM6Ly9j
ZXJ0LmV4YW1wbGUub3JnL3Bhc3Nwb3J0LmNydCJ9
.
eyJpYXQiOiIxNDQzMjA4MzQ1Iiwib3RuIjoiMTIxNTU1NTEyMTIiLCJkdXJpIjoi
c2lwOmFsaWNlQGV4YW1wbGUuY29tIn0
.
KK89q2RFY-BkKQQhiB0z6-fIaFUy6NDyUboKXOix9XnYLxTCjdw1UHjCbw4CefeK
wH_t7W-bnGlZz4pI-rMjfQ
```

RS256 example - signature size 684 characters

```
eyJ0eXAiOiJwYXNzcG9ydCIsImFsZyI6IlJTMjU2IiwieDV1IjoiaHR0cHM6Ly9j
ZXJ0LmV4YW1wbGUub3JnL3Bhc3Nwb3J0LmNydCJ9
.
eyJpYXQiOiIxNDQzMjA4MzQ1Iiwib3RuIjoiMTIxNTU1NTEyMTIiLCJkdXJpIjoi
c2lwOmFsaWNlQGV4YW1wbGUuY29tIn0
.
AaeXRqm7kHnkZu2j6cQmDCiomZRiaE55bYWhFgnX8xMqpBFq96M0xgMM5OLa9_LM
rkuKv2ivK5GZz8OlFrmAirucRlAh8YdUkj5Cr5xPRr-gg9acD9jqJUnQ-ZxpL1yq
-FFVLhvpbsE5NMPHXUp5lpt62rD-S0NlhwHNCeMqZHxt6T5BmZBXITEd1PRRij_6
FhE3wxWEhZMthWJuEbcPpRMZDu-R7lTNddn62nUKjn3s00R3gm25Dto5Z0dzfQpA
ysJvnbc1QRimfsYqJPUFc57lnglVLf4WrpeZCc8-LcoXeSr_dseDgsrmg2EuHmn5
h1nTOmLgF16ZHm121ZVjiXz2sMFvs9RaIxw0AFkM7rnV56OxAFCRuzMNldiEVf8p
lRZVvqZ4BfVQlCNXNyyVgPOUtNr3ta6yD2H0oANQvvHtwjuSwB9Kruj4Wsu5N7Ik
i4MBs6SWJDmcUV-NW_AHYLaao-IvFVe4oCkJNjsqwwXuLv1TO2sDHdc5sQO5zm21
019PPxw1udHVtywsRVNKLo0RzE0TqYUF7XclCDur7MMOx9SnStV2PFIM7Jejyn9x
54RtJEjOnchaSalfIFr_UXqXgVmRZVTzLDQIlcmHjlhhLnCnNx3sYsAANen8Y8jt
fgJ2ewjGotB4Lq8VYe1FacBKKk0VyCfImXba0u1hB8Q
```

PASSporT “mky" fingerprint

- For an SDP offer that includes the following fingerprint values,

```
a=fingerprint:sha-256 02:1A:CC:54:27:AB:EB:9C:53:3F:3E:4B:65:2E:7D:46:3F:
54:42:CD:54:F1:7A:03:A2:7D:F9:B0:7F:46:19:B2

a=fingerprint:sha-256 4A:AD:B9:B1:3F:82:18:3B:54:02:12:DF:3E:5D:49:6B:
19:E5:7C:AB:3E:4B:65:2E:7D:46:3F:54:42:CD:54:F1
```

- the PASSporT Payload object would be:

```
{
   “iat”:”1443208345",
   "otn":"12155551212",
   "duri":"sip:alice@example.com",
   “mky”:"[{
      "algorithm":"sha-256",
      "digest":"02:1A:CC:54:27:AB:EB:9C:53:3F:3E:4B:65:2E:7D:46:3F:54:
         42:CD:54:F1:7A:03:A2:7D:F9:B0:7F:46:19:B2"
   },
   {
      "algorithm":"sha-256",
      "digest":"4A:AD:B9:B1:3F:82:18:3B:54:02:12:DF:3E:5D:49:6B:19:E5:7C:AB:
         3E:4B:65:2E:7D:46:3F:54:42:CD:54:F1"
   }]"
}
```

Proposals from list

In Section 3.1, please say that the PASSporT signature will be ECDSA with curve P-256 and the SHA-256 one-way hash function.

In Section 3.1, “.crt” is used as a file extension. RFC 2585 says that “.cer” should be used in this case. Is there any problem making that change?

In section 3.1.2, I think the WG has decide to support on ES256. Please remove RS256.

In Section 3.2.2.2, there was a discussion about dropping the colon characters just to make the PASSportT token smaller. Is there a reason that was not done?