Security_4_Plugfest – Prototype Objects

Author: Oliver Pfaff, Siemens AG, CT RTC ITS

Introduction

This documents captures prototype objects for the security-enabling of the Nice F2F Plugfest. These prototypes do focus on sampling the data objects on application-level data.

ES256 Tokens

By default ES256 is used as AS token signature algorithm. This section describes their acquisition.

C Registration at AM

Registration Request

URL: https://ec2-54-154-59-218.eu-west-1.compute.amazonaws.com/iam-services/0.1/oidc/am/register

```
{
      "client_name": "testClient0123456789",
      "grant_types": [ "client_credentials"]
}
```

No Authorization header is needed. Do alter the value of the “client_name” member when making an own registration.

Registration Response

```
{
  "client_id": "0c5f83a7-cf08-4f48-8337-bfc65ea149ff",
```

```
  "client_secret": "AOpOrI2SdPi90SbAeMFiLFUtqWPi0Mure-
bwZffLTDvUB756eYczDgo9bAUPJQNRVSyvP11Oby30gGF6wm6JnMw",
  "client_secret_expires_at": 0,
  "client_id_issued_at": 1451293402,
  "registration_access_token":
"eyJraWQiOiJQbHVnRmVzdE5pY2UiLCJhbGciOiJFUzI1NiJ9.eyJhdWQiOiIwNzQwZWNh
Yy00ZTAyLTRmZTYtOWI5MC1kZjE4ZjUzZDFhNTMiLCJpc3MiOiJodHRwczpcL1wvYW0uY2
9tcGFueS1zLmNvbTo4NDQzXC9pYW0tc2VydmljZXNcLzAuMVwvb2lkY1wvYW1cLyIsImlh
dCI6MTQ1MTI5MzQwMiwianRpIjoiNDk2NDFkZmYtZTFjMy00MjI0LTljMjItNDI3YmY5MW
JmYTdhIn0.XTZjjnuzGUxQPIOiLuayY-
gCf7XP7Xkf1fMxmxCp821enwwpzcidLA59hxrGk723Geq1fHV3HDIwwrXIsYGoXg",
  "registration_client_uri": "https://am.company-s.com:8443/iam-
services/0.1/oidc/am/register/0740ecac-4e02-4fe6-9b90-df18f53d1a53",
  "redirect_uris": [],
  "client_name": "testClient0123456789",
  "contacts": [],
  "token_endpoint_auth_method": "client_secret_basic",
  "scope": "address phone email profile iot",
  "grant_types": [
    "client_credentials"
  ],
  "response_types": [],
  "default_acr_values": [],
  "post_logout_redirect_uris": [],
  "request_uris": []
}
```


Only the values of members “client_id” and “client_secret” are needed in the following

AM/AS Token Acquisition from AM

Token Request

URL: https://ec2-54-154-59-218.eu-west-1.compute.amazonaws.com/iam-services/0.1/oidc/am/token

```
grant_type=client_credentials
```

An Authorization header is needed. It shall reflect the client credentials (values of “client_id” and “client_secret”) obtained before. Multiple token acquisition exchanges may be done per C (at AM) registration i.e. there is no need to repeat the C (at AM) registration per token acquisition.

Token Response


```
{
  "access_token":
"eyJhbGciOiJFUzI1NiJ9.eyJhdWQiOiIwYzVmODNhNy1jZjA4LTRmNDgtODMzNy1iZmM2
NWVhMTQ5ZmYiLCJzdWIiOiIwYzVmODNhNy1jZjA4LTRmNDgtODMzNy1iZmM2NWVhMTQ5Zm
YiLCJpc3MiOiJodHRwczpcL1wvYW0uY29tcGFueS1zLmNvbTo4NDQzXC9pYW0tc2Vydmlj
ZXNcLzAuMVwvb2lkY1wvYW1cLyIsInR5cCI6Im9yZzp3Mzp3b3Q6and0OmFtOmFzLXdyYX
A6bWluIiwiYXNfdG9rZW4iOiJleUpoYkdjaU9pSkZVekkxTmlKOS5leUpoZFdRaU9pSk9h
V05sVUd4MVoyWmxjM1JTVXlJc0luTjFZaUk2SWpCak5XWTRNMkUzTFdObU1EZ3ROR1kwT0
MwNE16TTNMV0ptWXpZMVpXRXhORGxtWmlJc0ltbHpjeUk2SWs1cFkyVlFiSFZuWm1WemRF
```

```
RlRJaXdpZEhsd0lqb2liM0puT25jek9uZHZkRHBxZDNRNllYTTZiV2x1SWl3aWFuUnBJam
9pTTJJMFptRTJZVFl0WldGa01pMDBabVV4TFRrd1lXSXRORGt6WmpKaU5USTJNREF5SW4w
LnI4MnFYc1NYQnppWjRUWXVfRzREZ1VFSnNPQ0dXbXBaVW5CVkNoQnhUdEM4TWowTnltai
1ialN1NWdLUDVSb0FaQWNZWVRYdGloVEtKbGJwS29ia19nIiwianRpIjoiODY3NWZhMmYt
N2NmNS00MWQ1LTk5ZTgtNzczYjZkMzQyYTU0In0.YulWVPVeDY5i5FtkS0x7SxKUg5dpD2
JoJ38iEKrJPFm1jsFBWwmjLY7vcLssW4XVykWsRQAmd6_5Vl9gL4p1-Q",
  "token_type": "Bearer",
  "expires_in": 3599
}
```


This response object provides the AM token as the value of the “access_token” member (see above). The AM token contains the AS token as the value of the “as_token” member. A prototype is:

eyJhbGciOiJFUzI1NiJ9.eyJhdWQiOiJOaWNlUGx1Z2Zlc3RSUyIsInN1YiI6IjBjNWY4M2E3LWN
mMDgtNGY0OC04MzM3LWJmYzY1ZWExNDlmZiIsImlzcyI6Ik5pY2VQbHVnZmVzdEFTIiwidHl
wIjoib3JnOnczOndvdDpqd3Q6YXM6bWluIiwianRpIjoiM2I0ZmE2YTYtZWFkMi00ZmUxLTkwYW
ItNDkzZjJiNTI2MDAyIn0.r82qXsSXBziZ4TYu_G4DgUEJsOCGWmpZUnBVChBxTtC8Mj0Nymj-
bjSu5gKP5RoAZAcYYTXtihTKJlbpKobk_g

Note that this is the so-called “minimal” AS token[1]. For simplicity reasons the “minimal” token comes with a minimal complexity (only the payload values “sub” and “jti” will vary per AS token instances).

HS256 Tokens

HS256 can be used as an alternative AS token signature algorithm. This requires to a RS registration (at AS) in addition to the exchanges prototyped above:

RS Registration at AS

Registration Request

URL: https://ec2-54-154-59-218.eu-west-1.compute.amazonaws.com/iam-services/0.1/oidc/as/register

```
{
      "client_name": "testServer0123456789",
      "grant_types": [ "client_credentials"],
      "id_token_signed_response_alg": "HS256"
}
```

No Authorization header is needed. Do alter the value of the “client_name” member when making an own registration.

Remark: the RS (at AS) registration can also be done with an “id_token_signed_response_alg” value of “ES256” or without “id_token_signed_response_alg” member. This establishes an RS

[1] Okay resp. intentional for getting started in a Plugfest. Do not use such token layout in production

(at AS) registration and corresponding rsId value (see token acquisition below) and allows to obtain so-called “normal” AS tokens as described below.

Registration Response


```
{
  "client_id": "2195f7cf-f64b-4147-bbdd-f0f545fae1d6",
  "client_secret":
"AKxubADLmSQzRDNZc5O5xOhbb65oPF1dg3n78GcC5rVVBZu3y3JpP0STbRU6Bs5HqNb1h
YmlX5GifJJULppa0U0",
  "client_secret_expires_at": 0,
  "client_id_issued_at": 1451296658,
  "registration_access_token":
"eyJraWQiOiJQbHVnRmVzdE5pY2UiLCJhbGciOiJFUzI1NiJ9.eyJhdWQiOiIyMTk1Zjdj
Zi1mNjRiLTQxNDctYmJkZC1mMGY1NDVmYWUxZDYiLCJpc3MiOiJodHRwczpcL1wvYXMuY2
9tcGFueS1zLmNvbTo5NDQzXC9pYW0tc2VydmljZXNcLzAuMVwvb2lkY1wvYXNcLyIsImlh
dCI6MTQ1MTI5NjY1OCwianRpIjoiYTlkYzY0NGUtZDFhOC00NDhkLTkyYjgtZTE3NjU4Zm
QxNTQ5In0.XIPUNy8t7YKBbC6x8gHb5oIHyZc_9WGLPjuwg4psMDJZjWXr6jihTHWzGn2Q
xK7VN3--d1zRVM9FxzKcZCT-9w",
  "registration_client_uri": "https://as.company-s.com:9443/iam-
services/0.1/oidc/as/register/2195f7cf-f64b-4147-bbdd-f0f545fae1d6",
  "redirect_uris": [],
  "client_name": "testServer0123456789",
  "contacts": [],
  "token_endpoint_auth_method": "client_secret_basic",
  "scope": "address phone email profile iot",
  "grant_types": [
    "client_credentials"
  ],
  "response_types": [],
  "id_token_signed_response_alg": "HS256",
  "default_acr_values": [],
  "post_logout_redirect_uris": [],
  "request_uris": []
}
```


Only the value of the member “client_id” is needed in the following. Note that this value describes the instance of the RS component at AS (not the C instance at AM).

C Registration at AM

Same as described above

AM/AS Token Acquisition from AM

Token Request

URL: https://ec2-54-154-59-218.eu-west-1.compute.amazonaws.com/iam-services/0.1/oidc/am/token

```
grant_type=client_credentials&rsId=2195f7cf-f64b-4147-bbdd-
f0f545fae1d6&rId=%2Ftrafficlight&mths=GET+POST
```

As before: an Authorization header is needed. It shall reflect the client credentials (values of “client_id” and “client_secret”) obtained before. Multiple token acquisition exchanges may be done per C (at AM) registration i.e. there is no need to repeat the C (at AM) registration per token acquisition.

New:

- The value of rsId shall be the identifier by which an RS is known at the AS. This is obtained as the value of the “client_id” member in the RS-at-AS registration response. Right now the supply of this RS identifier is OOB (interim approach: document in Plugfest Wiki)
- The value of rId shall be a relative path
- The value(s) of mths shall be a space-separated list of CoAP methods

Note: the AS component implements a liberal policy (allow-all) that will issue AS tokens for arbitrary values of rsId, rId and mths[2].

Token Response


```
{
 "access_token":
"eyJhbGciOiJFUzI1NiJ9.eyJhdWQiOiIwYzVmODNhNy1jZjA4LTRmNDgtODMzNy1iZmM2
NWVhMTQ5ZmYiLCJzdWIiOiIwYzVmODNhNy1jZjA4LTRmNDgtODMzNy1iZmM2NWVhMTQ5Zm
YiLCJpc3MiOiJodHRwczpcL1wvYW0uY29tcGFueS1zLmNvbTo4NDQzXC9pYW0tc2Vydmlj
ZXNcLzAuMVwvb2lkY1wvYW1cLyIsInR5cCI6Im9yZzp3Mzp3b3Q6and0OmFtOmFzLXdyYX
A6bWluIiwiZXhwIjoxNDUxMzAwNzA4LCJpYXQiOjE0NTEyOTcxMDksImFzX3Rva2VuIjoi
ZXlKaGJHY2lPaUpJVXpJMU5pSjkuZXlKaGRXUWlPaUl5TVRrMVpqZGpaaTFtTmpSaUxUUX
hORGN0WW1Ka1pDMW1NR1kxTkRWbVlXVXhaRFlpTENKemRXSWlPaUl3WXpWbU9ETmhOeTFq
WmpBNExUUm1ORGd0T0RNek55MWlabU0yTldWaE1UUTVabVlpTENKaFkya2lPbHQ3SW0xMG
FDSTZXeUpIUlZRaUxDSlFUMU5VSWwwc0luSmxjeUk2SWx3dmRISmhabVpwWTJ4cFoyaDBJ
bjFkTENKcGMzTWlPaUpvZEhSd2N6cGNMMXd2WVhNdVkyOXRjR0Z1ZVMxekxtTnZiVG81Tk
RRelhDOXBZVzB0YzJWeWRtbGpaWE5jTHpBdU1Wd3ZiMmxrWTF3dllYTmNMeUlzSW5SNWND
STZJbTl5WnpwM016cDNiM1E2YW5kME9tRnpPbU52WVhBNllXbG1JaXdpWlhod0lqb3hORF
V4TXpBd056QTVMQ0pwWVhRaU9qRTBOVEV5T1RjeE1Ea3NJbXAwYVNJNkltWXlZek5sT1RG
aExUQm1OV1l0TkRNNVpDMWhaakkzTFRRd1lUazFNR000WVdSbU5DSjkuazhIQ2tBbWhydU
I1NVh2UnVFbmJSc3BJQ1VDQ0dWSkxnSnM2UzJ4aWRMSSIsImp0aSI6ImQ1MDQyYWM0LWY0
YmYtNDg5ZC04YjQxLWE4MjQxMDQzNjQ1NyJ9.4OnUE3LjRrqBnz36SHlELYq3kVZ3iS30h
jSwtkNRaOXZjCzGlWc-QX4aRlc-oaCQK1zIVHfTGQ52z-U7jbZZnQ",
  "token_type": "Bearer",
  "expires_in": 3599,
  "scope": "address phone email profile iot"
}
```


This response object provides the AM token as the value of the “access_token” member (see above). The AM token contains the AS token as the value of the “as_token” member. A prototype is:


```
eyJhbGciOiJIUzI1NiJ9.eyJhdWQiOiIyMTk1ZjdjZi1mNjRiLTQxNDctYmJkZC1mMGY1N
DVmYWUxZDYiLCJzdWIiOiIwYzVmODNhNy1jZjA4LTRmNDgtODMzNy1iZmM2NWVhMTQ5ZmY
```


[2] Okay resp. intentional for getting started in a Plugfest. Do not use such token layout in production

iLCJhY2kiOlt7Im10aCI6WyJHRVQiLCJQT1NUIl0sInJlcyI6IlwvdHJhZmZpY2xpZ2h0I
n1dLCJpc3MiOiJodHRwczpcL1wvYXMuY29tcGFueS1zLmNvbTo5NDQzXC9pYW0tc2Vydml
jZXNcLzAuMVwvb2lkY1wvYXNcLyIsInR5cCI6Im9yZzp3Mzp3b3Q6and0OmFzOmNvYXA6Y
WlmIiwiZXhwIjoxNDUxMzAwNzA5LCJpYXQiOjE0NTEyOTcxMDksImp0aSI6ImYyYzNlOTF
hLTBmNWYtNDM5ZC1hZjI3LTQwYTk1MGM4YWRmNCJ9.k8HCkAmhruB55XvRuEnbRspICUCC
GVJLgJs6S2xidLI