MQ 9.4 – AUTHENTICATION JWT

Un parcours pas si évident

2025-04-10

COMMENT ÇA MARCHE ?

L’application cliente s’authentifie auprès de son identity provider (Microsoft EntraID)

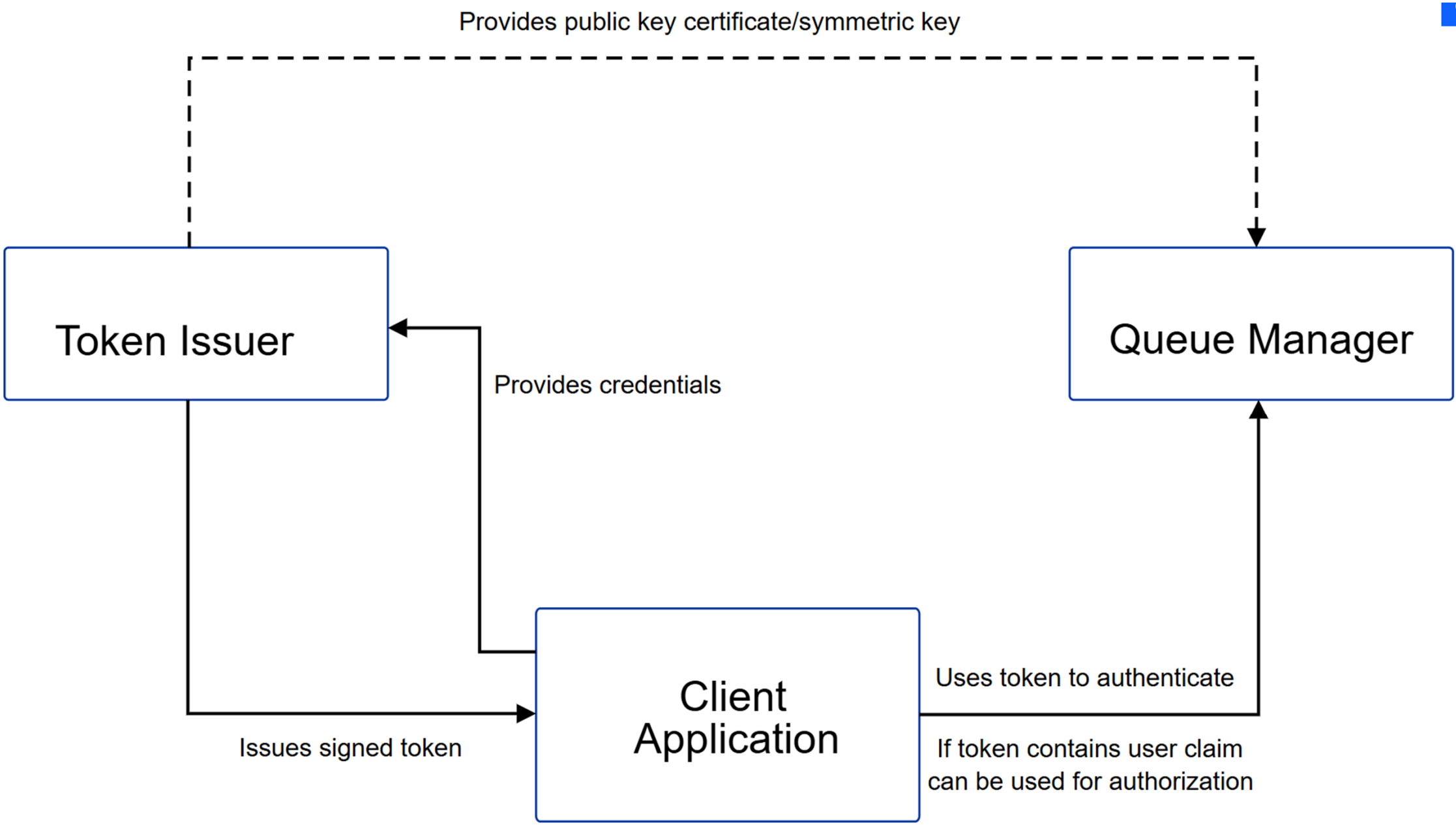
L’identity provider lui remet un token JWT à passer au QMGR

L’application effectue sa connexion au QMGR en envoyant son token en paramètre

Le QMGR (préalablement configuré correctement) vérifie la validité de ce token auprès de l’identity provider émetteur

Et si le token est validé, la connexion se poursuit normalement

AIRFRANCE KLM


Provides public key certificate/symmetric key
Token Issuer
Queue Manager
Provides credentials
Client Application
Uses token to authenticate
Issues signed token
If token contains user claim can be used for authorization

EN VRAI ÇA CHANGE QUOI ?

- On peut positionner le CHCKCLNT de son AUTHINFO à REQUIRED sans trop culpabiliser, c'est mieux pour la sécurité
- Les applications n'ont plus besoin d'envoyer le password (info sensible) de leur user à chaque connexion, c'est mieux pour la sécurité
- Le token a une durée de vie et devant être recyclé, c'est mieux pour la sécurité
- Ils sont délivrés et signés par un tiers, c'est mieux pour la sécurité
- Ils sont légers et simples à utiliser par les applications
- Conclusion : **Vous l'aurez compris, c'est mieux pour la sécurité**

AIRFRANCE KLM

CONFIGURATION DU QMGR

AVEC UN IDENTITY PROVIDER EXTERNE

- Déterminer l'adresse du EndPoint JWKS du provider
- Déterminer l'adresse de l'issuer
- Déterminer le username
  - ça dépend de l'utilisation (cf : diapo 6)


```
{
  "aud": "b0913877-8980-4617-8eee-622963e140f0",
  "iss": "https://login.microsoftonline.com/9b802d8b-
33fa-40fb-acb7-9ffdbd1919eb/v2.0",
  "iat": 1742825363,
  "nbf": 1742825363,
  "exp": 1742829263,
  "aio":
"k2RgYLiurPSTUzflkel05hyp7E/eOZrp/tWufjxPJJsdlGTztAE=",
  "azp": "eb61bcdb-1341-4e64-b1bf-39ccb0a3263b",
  "azpacr": "2",
  "oid": "835d1e2d-096f-4608-8ead-2ff20878f12c",
  "rh": "1.AREAiy2Am_oz-
0Cst5_9vRkZ63c4kbCAiRdGju5iKWPhQPARAAARAA.",
  "sub": "835d1e2d-096f-4608-8ead-2ff20878f12c",
  "tid": "9b802d8b-33fa-40fb-acb7-9ffdbd1919eb",
  "uti": "ZHpkvm-d80Wpp1gSG-cfAA",
  "ver": "2.0"
}
```


AIRFRANCE KLM

CONFIGURATION DU QMGR

SUITE

1. Créer un magasin de clé de type PKCS12 qui contient les certificats signataires du EndPoint JWKS du provider
    1. Car une connexion HTTPS est obligatoire

> **Important:** You should always provide JWKS information over TLS/HTTPS and you need this information to ensure that the queue manager can trust the connection.

2. Paramétrer le qm.ini

```
JWKS:
    Endpoint=https://myauthserver.example/jwks
    IssuerName=https://myauthserver.example/jwks
    UserClaim=MQUser
```

    1. Vérifier que la **SecurityPolicy** n'est pas positionnée explicitement à **group**

AIX Linux `SecurityPolicy=user|group|UserExternal|default`

> AIX V 9.4.0 Linux **Note:** From IBM MQ 9.4.0, if the AuthToken stanza is specified, the effective value of the **SecurityPolicy** attribute of the Service stanza is set to `UserExternal`. Token authentication is not available if **SecurityPolicy** is explicitly set to `Group` in the Service stanza. If **SecurityPolicy** is set to `Group`, remove the **SecurityPolicy** attribute from the Service stanza, then restart the queue manager. For more information, see AuthToken stanza of the qm.ini file.

JWT POUR FAIRE QUOI ?

De l'authentification simple

- A la manière d'un couple user/password classique qu'on mappe sur un MCAUSER via un CHLAUTH
- ADOPTCTX(NO) dans le CONNAUTH
- UserClaim optionnel dans le qm.ini

De l'autorisation en plus

- On utilise l'identité applicative encodée dans le token pour faire de la gestion de permission
- ADOPTCTX(YES) dans le CONNAUTH
- UserClaim obligatoire dans le qm.ini
- Limitation à 12 caractères pour le moment. Amené à changer prochainement

AIRFRANCE KLM

AIRFRANCE KLM

ÇA C'ÉTAIT LA THÉORIE

ça semble simple

AIRFRANCE KLM

EN PRATIQUE

c’est moins reposant

2 PMRs et 1 IDEA plus tard…

CONNEXION HTTPS VERS LE ENDPOINT

PMR N°1

Microsoft EntraID nous fournit une URL de EndPoint à ce format :	• https://login.microsoftonline.com/[...]
Le SNI est donc positionné à :	• login.microsoftonline.com
Or le DN renvoyé par le certificat est le suivant :	• CN=stamp2.login.microsoftonline.com,[…]
Le SNI apparaît uniquement dans les SAN du certificate	• MQ ignore les SANs et part en erreur : BAD CERTIFICATE
BUG dans la librairie TLS MQ	• Le PMR prendra plus d'1 mois
Heureusement, on avait trouvé un workaround avant…	

AIRFRANCE KLM

RECUPERATION DES CLES JWKS

PMR N°2

Les prérequis parlent :

- De la RFC 7519 : sur JWT (JSON Web Token)
- De la RFC 7515 : sur JWS (JSON Web Signature)

Mais aucune documentation ne fait mention :

- De la RFC 7517 : sur JWK (JSON Web Key)
  - Qui stipule au point 4.4 que le paramètre « alg » est optionnel
  - Contrairement à l'implémentation IBM MQ qui le rend obligatoire

Microsoft EntraID, utilise des clés sans « alg »

- 407 - Missing one or more of the required attributes in the retrieved JWKS payload. The required attributes are use, alg, kid, n, and e. Check that the JWKS payload contains one or more of the required attributes listed.

Le PMR prendra 15 jours

- Et un mail à Robert Parker

AIRFRANCE KLM

MQ LONG USER ID SUPPORT

IDEA

- Microsoft EntraID utilise des users de ce style 835d1e2d-096f-4608-8ead-2ff20878f12c
  - Ils font sensiblement plus de 12 caractères
  - Il est donc impossible de gérer les droits d'accès aux objets sur cette base
  - J'ai donc contacté Anthony Beardsmore pour lui faire un retour d'expérience

  - Nous attendons donc que quelque chose sorte des cartons d'Hursley

AIRFRANCE KLM

PLACE À LA DÉMO

JmsBrowser

- MQ 9.4.2.0 sur AKS