



French MQ User Group - MQ octobre 2026

Advanced Message Security

Luc-Michel Demey
Demey Consulting
LMD@Demey-Consulting.fr

Ce document a été préparé à partir de différentes sources d'information publiquement disponibles.
Tous les efforts ont été faits pour rendre ce document complet et exact. Demey Consulting décline par avance toute responsabilité quant aux erreurs et omissions présentes dans ce support. Seuls les documents de référence IBM font foi quant aux capacités et au paramétrage des produits cités.

Version 1.04 – Octobre 2026

Limitation de responsabilité :

Tous les efforts ont été faits pour rendre ce support de cours complet et exact. Demey Consulting décline par avance toute responsabilité quant aux erreurs et omissions présentes dans ce support. Seuls les documents de référence IBM font foi quant aux capacités et au paramétrage des produits cités.

IBM, WebSphere, MQSeries sont des marques déposées de International Business Machines.



Copyright 2001-2026 - Demey Consulting – 72, avenue du Général de Gaulle
94170 Le Perreux sur Marne
lmd@demey-consulting.fr

Tous droits réservés.

Toute reproduction, partielle ou totale de ce document par quelque procédé que ce soit, faite sans consentement écrit de Demey Consulting est illicite.



Protection des données

- Contexte réglementaire :
 - RGPD
 - PCI/DSS (Visa / Mastercard / ...)
 - CSP (Customer Security Program – Swift)
- Protection des données :
 - In transit (Transfert sur le réseau)
 - At rest (Stockage : fichiers, BdD, ...)





Application aux messages MQ

- In transit :
 - Transfert via des canaux **DQM**, **SVRCONN**, **Cluster**
 - Solution : **TLS**
- At rest :
 - Messages en attente de traitement dans des files
 - Messages en attente de transfert dans une XmitQ
 - Messages tombés en DLQ





Sécurité des messages MQ - 1

- OAM (setmqaut, AUTHREC, ...)
- Chiffrement des canaux (TLS)
- CHLAUTH, CONNAUTH, ...



Sécurité des messages MQ - 2

- Pas de protection du contenu des files de messages
- Pas de confidentialité de bout en bout
- Un compte avec les « bons » droits (*) peut :
 - Visualiser les messages
 - Ajouter des messages
 - Retirer des messages
 - Réinjecter un message modifié

() groupe mqm/QMQM/QMQMADM, groupe Administrateurs, *ALLOBJ, droits explicites)*





Sécurité des messages MQ - 3

- Les besoins :
 - **Chiffrer les messages « at rest »**
 - S'assurer que seuls les expéditeurs autorisés posent des messages
 - S'assurer que seul le destinataire du message pourra le lire
 - Permettre aux destinataires de s'assurer de l'identité de l'émetteur
- De manière transparente pour les applications existantes





La solution IBM : AMS (Advanced Message Security)

- Fonctionne avec des « **intercepteurs** » au niveau du MQI
 - Valide les identités avec des **certificats**
 - Plusieurs niveaux de protection
 - Protection définie au niveau de chaque file
 - Liste des expéditeurs et des destinataires autorisés
-
- **Nécessite MQ Advanced**



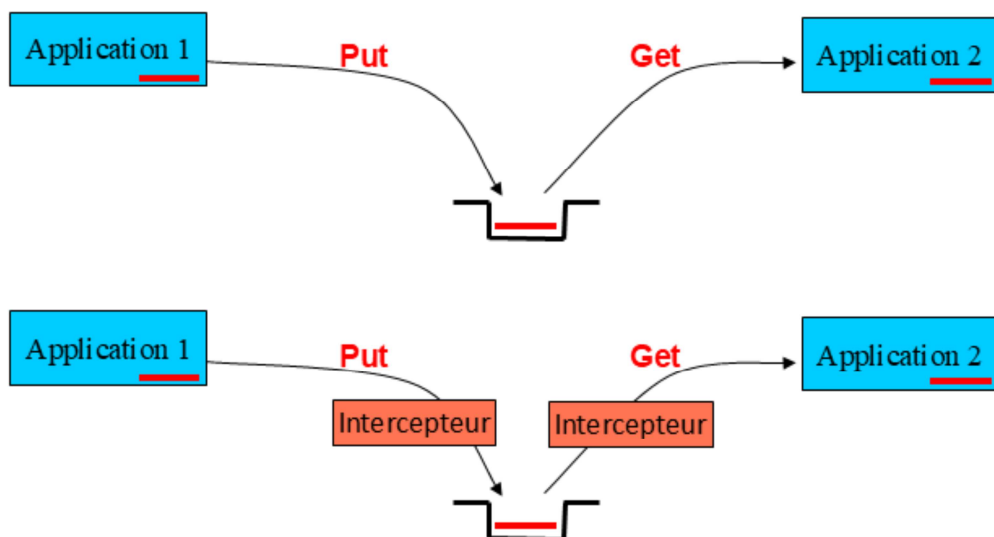


Niveaux de protection

- **Confidentiality** : les messages sont chiffrés par l'émetteur
- **Integrity** : les messages sont signés par l'émetteur
- **Privacy** : les messages sont signés et chiffrés par l'émetteur
- **None** : ni chiffrement, ni signature



Intercepteurs MQI



- Les opérations de Put et Get passent par un « intercepteur »
- Cet intercepteur chiffre ou déchiffre la partie data du message en fonction de la configuration
- Aucune modification applicative nécessaire



Comment ça marche ?

Côté expéditeur :

1. Génération d'une clé de session
2. Chiffrement de la partie data avec cette clé
3. Chiffrement de la clé de session avec la clé publique du destinataire
4. Ajout de la clé chiffrée au message
5. Envoi du message

Côté destinataire :

1. Lecture du message
2. Déchiffrement de la clé de session avec la clé privée du destinataire
3. Déchiffrement de la partie data avec cette clé de session

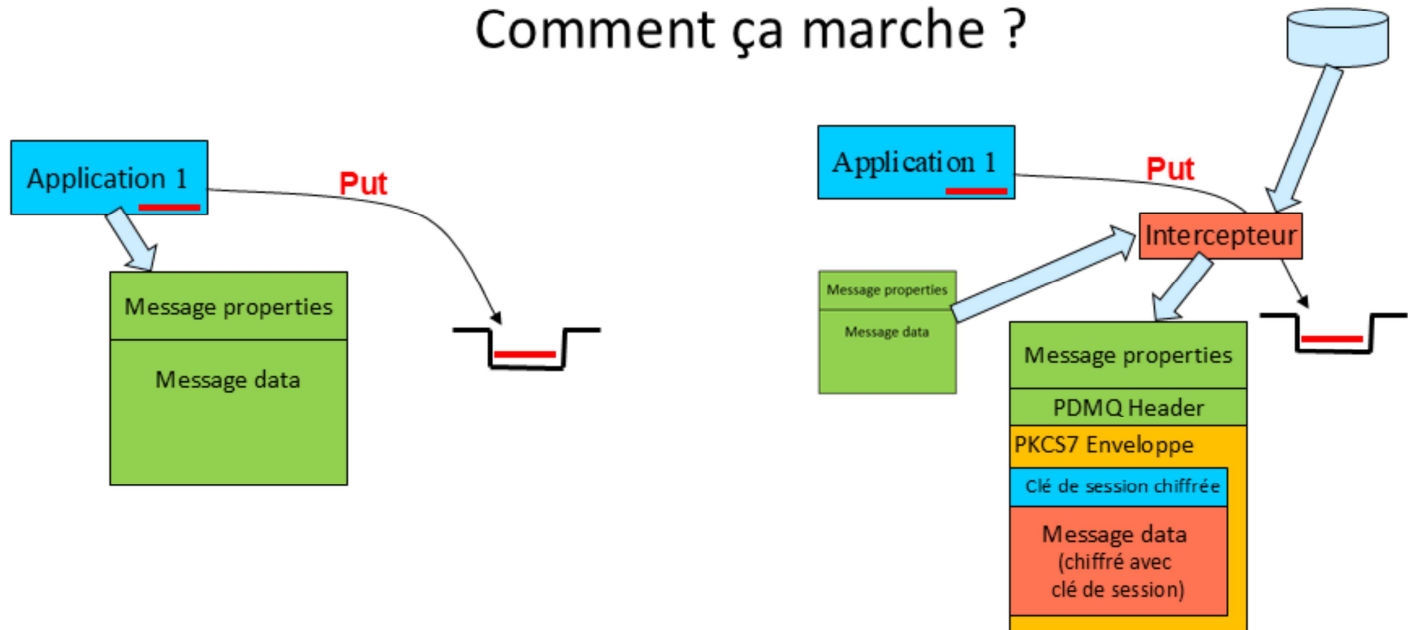


Détail des opérations dans le cas du chiffrement (sans signature).

Si signature, le message est signé par l'expéditeur avec sa clé privée, et le destinataire vérifie cette signature avec la clé publique de l'expéditeur



Comment ça marche ?



L'application dépose un message MQ classique (properties + data)

L'intercepteur génère une clé de session, et l'utilise pour chiffrer la partie data du message

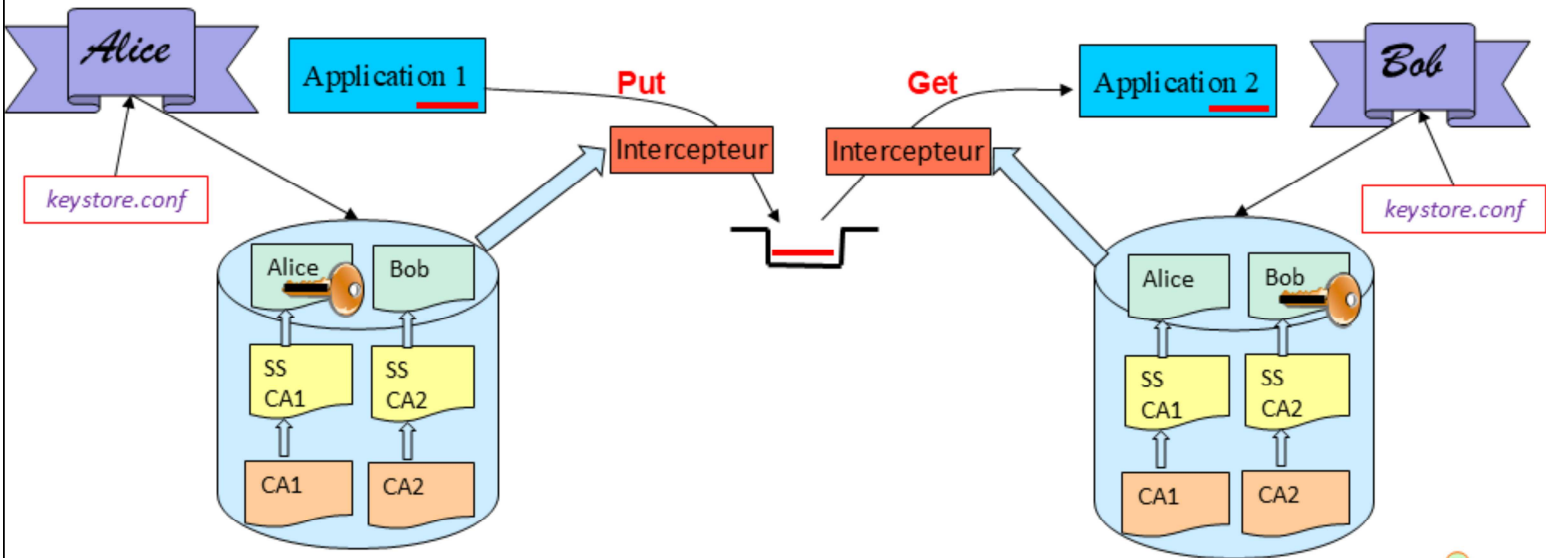
Puis il chiffre cette clé avec le certificat du destinataire et l'insère dans le message.

S'il y a plusieurs destinataires, il chiffre la clé autant de fois qu'il y a de destinataires, avec les certificats correspondants.

Pour limiter l'impact sur les performances, la clé de session peut être ré-utilisée x fois.



Utilisation des certificats



Le magasin d'Alice contient son certificat avec sa clé privée, ainsi que la chaîne de certification.

Le magasin de Bob contient son certificat avec sa clé privée, ainsi que la chaîne de certification.

Pour pouvoir chiffrer la clé de session, Alice a besoin du certificat de Bob (sans sa clé privée, avec la chaîne de certification).

Le CN du certificat doit correspondre à l'utilisateur qui fait le get ou le put.



Magasin de certificats

- Formats cms, jks, jceks ou JCERACFKS (z/OS)
- Contient le certificat et la clé privée du compte qui dépose ou consomme les messages
 - Lien par le label contenu dans le [keystore.conf](#)
- Contient le certificat (sans clé privée) du ou des destinataires des messages déposés
- Contient les chaines de certification



keystore.conf

- Fichier texte, permet de spécifier :
 - Le nom du magasin
 - Le label du certificat
 - Le mot de passe ...
- Par défaut :
 - \$HOME/.mqs/keystore.conf
 - %HOMEDRIVE%%HOMEPATH%\mqs\keystore.conf
- MQS_KEYSTORE_CONF
 - export MQS_KEYSTORE_CONF=path/filename
 - set MQS_KEYSTORE_CONF=path\filename

```
cms.keystore = path/mag_alice  
cms.certificate = Alice
```





Activation de la protection pour une file

- Utilisation de POLICIES
- Objets MQ
- Commandes :
 - SET POLICY (DISPLAY POLICY) en MQSC
 - setmqspl (dspmqspl) en CLI (Windows, Linux, z/OS)
 - SETMQMSPL (DSPMQMSPL) en CLI IBM i
- La POLICY porte le même nom que la file à protéger



Paramètres de protection

- Algorithme de signature (**MD5**, **SHA1**, SHA256, SHA384, SHA512, ...)
- Algorithme de chiffrement (**RC2**, **DES**, **3DES**, AES128, AES256 , ...)
- CN du ou des destinataires
- CN du ou des émetteurs
- Nombre de réutilisations de la clé de session (1 à 9999999)
- Comportement si message non protégé





MCA Interception

- Cas d'un lien entre environnement AMS et environnement non AMS
- Le chiffrement du message est effectué à l'arrivée sur le système AMS
- Pour les liens MQ client :
 - Activation AMS côté client ou MCA Interception
- Pour les liens DQM :
 - z/OS uniquement
 - SoD pour distribué

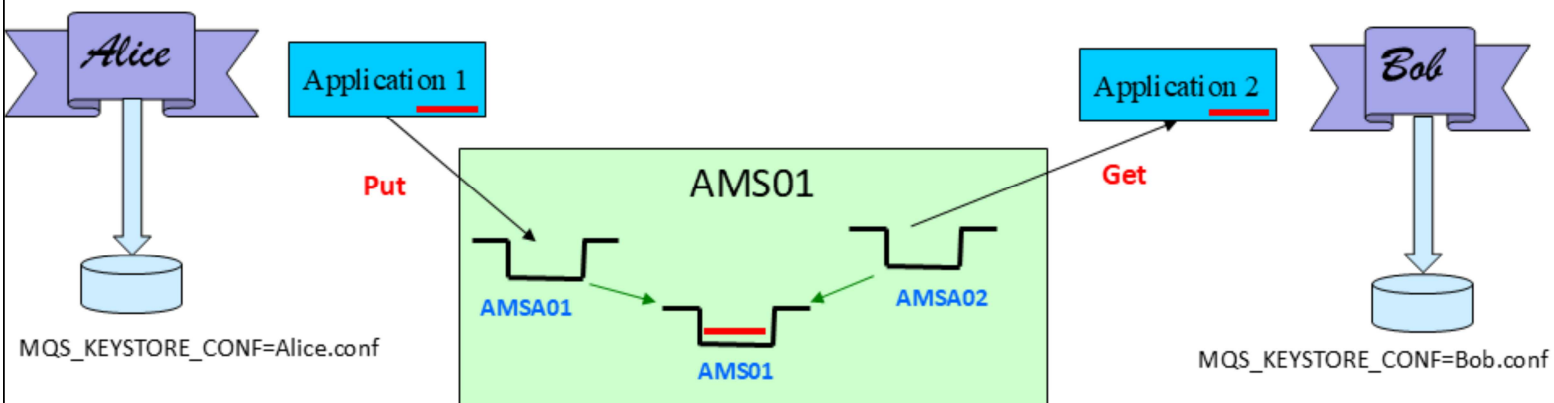




Exemple pratique



Environnement





Configuration keystore.conf

Alice

```
set MQS_KEystore_CONF=...\mags\Alice.conf
```

Fichier Alice.conf

```
cms.keystore = path/mag_alice
```

```
cms.certificate = Alice
```

```
runmqakm -cert -list -db mag_alice.kdb
```

Certificats détectés

* par défaut, - personnel, ! sécurisé, # secret key

```
! "CA DC 01"
```

```
! Bob
```

```
- Alice
```

Bob

```
set MQS_KEystore_CONF=...\mags\Bob.conf
```

Fichier Bob.conf

```
cms.keystore = path/mag_bob
```

```
cms.certificate = Bob
```

```
runmqakm -cert -list -db mag_bob.kdb
```

Certificats détectés

* par défaut, - personnel, ! sécurisé, # secret key

```
! "CA DC 01"
```

```
! Alice
```

```
- Bob
```





Protection de la file AMSA01

```
SET POLICY(AMSA01) SIGNALG(SHA256) ENCALG(AES256) RECIPI('CN=bob,OU=Tests AMS,O=Demey Consulting,L=Paris,C=FR') SIGNER('CN=alice,OU=Tests AMS,O=Demey Consulting,L=Paris,C=FR') ACTION(REPLACE)
```

AMQ9084I: Règle IBM MQ Advanced Message Security définie.

```
DISPLAY POLICY(AMSA01)
```

AMQ9086I: Affichez les détails de la règle IBM MQ Advanced Message Security.

```
POLICY(AMSA01)
```

```
SIGNALG(SHA256)
```

```
ENCALG(AES256)
```

```
SIGNER(CN=alice,OU=Tests AMS,O=Demey Consulting,L=Paris,C=FR)
```

```
RECIPI(CN=bob,OU=Tests AMS,O=Demey Consulting,L=Paris,C=FR)
```



Protection de la file AMSA02

```
SET POLICY(AMSA02) SIGNALG(SHA256) ENCALG(AES256) RECIPI('CN=bob,OU=Tests AMS,O=Demey Consulting,L=Paris,C=FR') SIGNER('CN=alice,OU=Tests AMS,O=Demey Consulting,L=Paris,C=FR') ACTION(REPLACE)
```

AMQ9084I: Règle IBM MQ Advanced Message Security définie.

```
DISPLAY POLICY(AMSA02)
```

AMQ9086I: Affichez les détails de la règle IBM MQ Advanced Message Security.

```
POLICY(AMSA02)
```

```
SIGNALG(SHA256)
```

```
ENCALG(AES256)
```

```
SIGNER(CN=alice,OU=Tests AMS,O=Demey Consulting,L=Paris,C=FR)
```

```
RECIPI(CN=bob,OU=Tests AMS,O=Demey Consulting,L=Paris,C=FR)
```



Introduction AMS

Gestion via MQ Explorer

MQ Explorer - Contenu X

Règles de sécurité

Nom de la règle	Algorithme
AMSA01	Néant
AMSA02	Néant

Informations générales

Nom de la règle : AMSA01

Tolérance

☒ Appliquer cette règle à tous les messages
Les messages conformes à cette règle sont remis. Les messages non conformes à la règle ne sont pas remis

☐ Tolérer les messages non conformes à cette règle
Tous les messages sont remis

Signature

Algorithme de signature des messages : Néant

☐ Accepter les messages signés provenant d'un émetteur

☒ Accepter uniquement les messages signés provenant des émetteurs de messages listés ci-dessous

Noms distinctifs des émetteurs de messages autorisés :

CN=alice,O=Demey Consulting,C=FR

Ajouter Supprimer

Chiffrement

Algorithme de chiffrement des messages : AES128

☐ Pas de réutilisation de clé

☐ Réutilisation de clé illimitée

☒ Réutilisation de clé personnalisée

Nombre de réutilisations de clé : 10

Les messages sont uniquement lisibles s'ils sont chiffrés pour l'un des destinataires de message autorisés spécifiés ci-dessous.

Noms distinctifs des destinataires de messages autorisés :

CN=bob,O=Demey Consulting,C=FR

Ajouter Supprimer

© Demey Consulting, 2001-2026 French MQ User Group Octobre 202



Introduction AMS



Test de dépôt

```
set MQS_KEYSTORE_CONF=... \mags\Alice.conf
amqspout AMSA01 AMS01
Sample AMQSPUT0 start
target queue is AMSA01
aaa
bbb

Sample AMQSPUT0 end
```

Afficheur de messages

Nom du gestionnaire de files d'attente : AMS01

Nom de file d'attente : AMS01

Position	Date/heure d'insertion	ID utilisateur	Nom de l'application d'insertion
1	2 oct. 2026, 18:57:41	alice	J:\MQ100\bin64\amqspout.exe
2	2 oct. 2026, 18:57:43	alice	J:\MQ100\bin64\amqspout.exe

Message 1 - Propriétés

Informations générales

Rapport

Contexte

ID

Segmentation

Données

Données

Longueur totale: 678

Longueur des données: 678

Format:

CCSID: 850

Codage: 546

Données de message: PDMQO

Octets des données de message:

30 00 70 00 00 00	PDMQO...p...p...
30 00 16 02 00 00	'...R.....
30 00 00 00 00 00	MQSTR
33 41 30 31 20 20	AMSA01
30 20 20 20 20 20	
30 20 20 20 20 20	
30 00 10 00 00 00	
17 00 01 07 03 A0	[0E... *âHâ...â]
11 02 01 AA 30 02	[E..0E. ...1E..0E]
17 31 08 30 09 06	[*...0U10Uc10 -]
30 0C 06 03 55 04	[U...FR1.0...U.]
30 10 06 03 55 04	[...Paris1.0...U.]
34 43 31 0E 30 0C	[.. PKI OF DC1.0..]
12 61 31 28 30 29	[..U[..Infra1+0)]
31 16 1C 70 68 69	[. *âHâ... .pki]
30 70 63 6F 6F 73	[nf10dem...rnr]

Fermer



AMS : Impacts

- Licence MQ Advanced (\$\$\$)
- Consommation CPU (en fonction de la protection et de la réutilisation de la clé de session)
- Gestion des certificats et des magasins
- Latence (opérations cryptographiques)
- Taille des messages : original + 1280 + (200 x nd de destinataires)
- Quelques options non supportées (PubSub, channel exit, ...)
- Pas de support pour les canaux AMQP et MQTT





La formation avec Demey Consulting



- Un organisme de formation déclaré et « Datadocké »
- Un catalogue de modules sur WebSphere Application Server et IBM MQ
- Plus de 50 modules MQ disponibles (1500 slides)
- Des supports de cours totalement francisés et au dernier niveau technique (MQ version 10.0.1)
- Des travaux pratiques sur Windows, Linux et IBM i avec les corrigés
- Des filières prédéfinies de 2 à 5 jours, ou à la carte.

<https://demey-consulting.fr/formationMQ>