# Retour expérimentation CHLAUTH sur zOS.





SILCA PRODUCTION INFORMATIQUE

# 1- S’intègre dans un projet Groupe.

- **Recommandations de IG.**
- **Demandes fortes de nos clients, de sécuriser les connections inbounds.**
- **Apports V7/V8 de WMQ intéressants à mettre en œuvre.**
- **Disponibles sur zOS et distribués.**
- **S’additionne à l’infrastructure de sécurité mise en place.**

# 2- Installation des *AUTH et paramétrages.

## Rendre Disponible les AUTHINFO du QMGR de SILCA.

- DEFINE AUTHINFO(SILCA.IDPWOS) AUTHTYPE(IDPWOS) QSGDISP(QMGR) ADOPTCTX(NO) CHCKCLNT(OPTIONAL) CHCKLOCL(OPTIONAL)

- ALTER QMGR CHLAUTH(ENABLED) CONNAUTH(SILCA.IDPWOS)

## Paramètre CHCKCLNT & CHCKLOCL.

**NONE** Switches off checking.

**OPTIONAL** Ensure User ID and password are provided by an application, they are a valid pair, but that it is not mandatory to provide them.

**REQUIRED** Requires that all applications provide a valid user ID and password.

**REQDADM** Privileged users must supply a valid user ID and password, but non-privileged users are treated as with the OPTIONAL setting. See also the following note. (This setting is not allowed on z/OS systems.)

## Paramètre Adaptcnx

**ADOPTCTX(YES)** All authorization checks for an application are made with the same user ID that you authenticated by password, by selecting to adopt the context as the application context for the rest of the life of the connection. (utilisation de bout en bout du userid de connexion (connexion et ressource)

**ADOPTCTX(NO**) An application provides a user ID and password for the purposes of authenticating them at connection time, but then continues by using the user ID that the application is running under for future authorization checks. (utilisation du userid Password pour authentification mais accès aux ressources avec un compte prédéfinie et différents

## Reslevel positionné sous External Securité « Racf ».

**RESLEVEL profiles :** Control the number of userids that are subject to authorization for any resources accessed through a connection.

# 3- Les Options retenues.

## Définir la queue qui accueille les règles CHLAUTH.

- SYSTEM.CHLAUTH.DATA.QUEUE

## Définir les CHLAUTH par défaut.

```
SET CHLAUTH( '*' ) +
      TYPE( BLOCKUSER ) +
      USERLIST( '*MQADMIN' ) +
      DESCR( 'Default rule to disallow privileged users' )

SET CHLAUTH( 'SYSTEM.*' ) +
      TYPE( ADDRESSMAP ) +
      ADDRESS( '*' ) +
      USERSRC( NOACCESS ) +
      DESCR( 'Default rule to disable all SYSTEM channels' )

SET CHLAUTH( 'SYSTEM.ADMIN.SVRCONN' ) +
      TYPE( ADDRESSMAP ) +
      ADDRESS( '*' ) +
      USERSRC( CHANNEL ) +
      DESCR( 'Default rule to allow MQ Explorer access' )
```

## AUTHINFO.

- Paramètre CHCKCLNT & CHCKLOCL à « Optional »
- Paramètre Adaptcnx à « No ».

# 3- Les Options retenues.

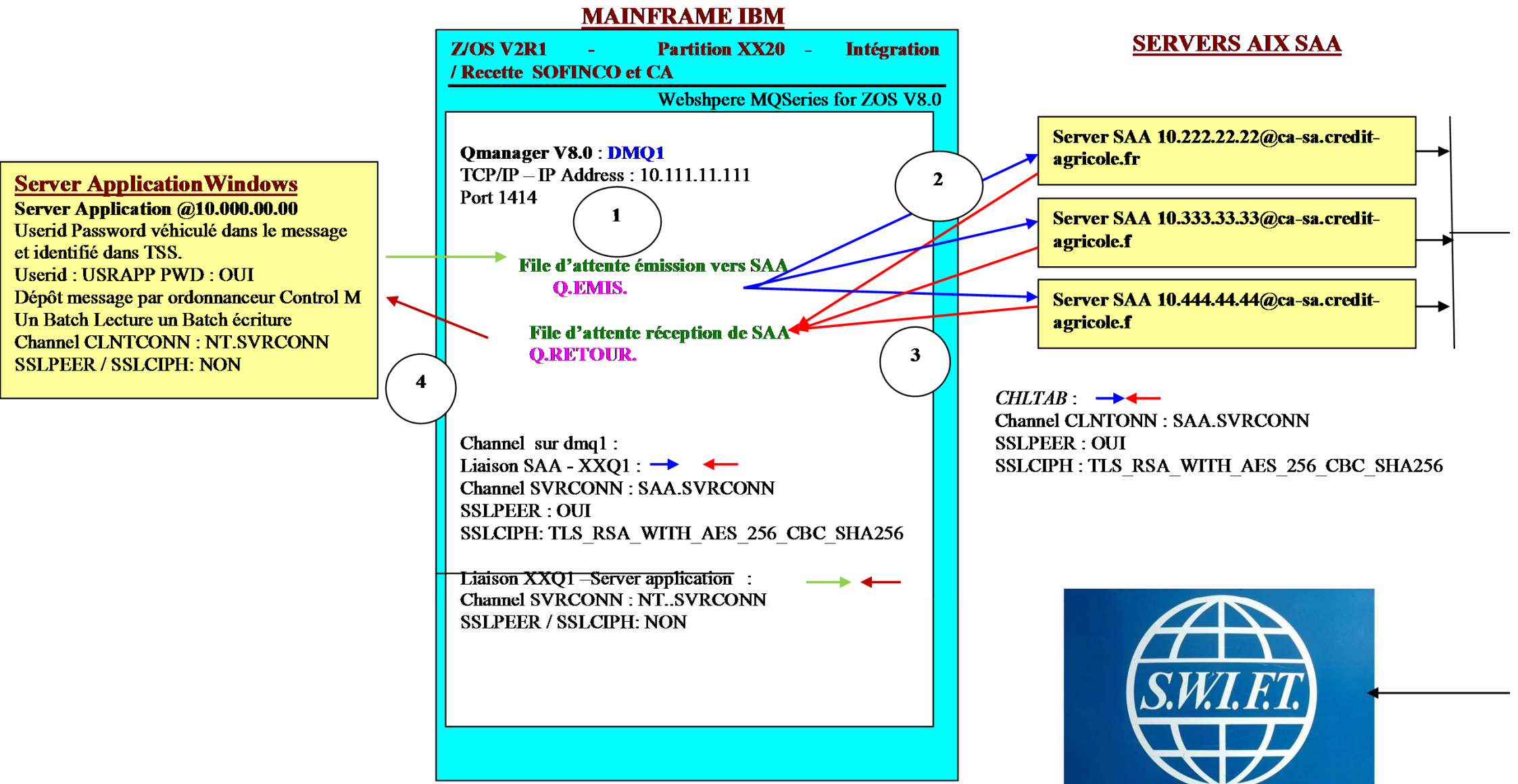
- **CHLAUTH sécurisation pas à pas.**
  - SET CHLAUTH('*') TYPE(ADDRESSMAP) ADDRESS('*') USERSRC(NOACCESS) DESCR(‘Sécurisation avec en douceur') WARN(YES).
  - ALTER QMGR CHLEV(EXCEPTION).
  - Monitoring de la SYSTEM.ADMIN.CHANNEL.EVENT MQRC_CHANNEL_BLOCKED_WARNING

**<.....QMD2.....>**
**<.....1X.XXX.XX.3.....>**
**<.....Ý.....>**
**<...XX.XXXX.SVRCONN...>**
**<.....R.....iSERIALN>**
**<UMBER=33:44:55:66:77:88:F>**
**<B:A1:BB:F3:FF:AA:BB:CC:DD>**
**<:EE:FF:A1,CN=MONCN01_LOLO>**
**<T_HOMOLOGA,OU=CA>**
**<,O=CM,L=Paris,ST=IDF,C=F>**
**<RANCE.....&.....>**
**<...CN=AC Interne de Laurent>**
**<ur,OU=0004 77777777,O=EU>**
**<,C=FR.....>**
**<.....mqm.....è.>**
**<.....amqsputc.....>**

# 3- Les Options retenues.

- **CHLAUTH USERMAP si possible.**
  - SET CHLAUTH(NT.SVRCONN) TYPE(USERMAP)
  - ADDRESS('10.000.000.000') CHCKCLNT(REQUIRED)
  - CLNTUSER('USRLEND')
  - DESCR('connexion only from dbdc server and lend user')
  - MCAUSER('ANOTHER') USERSRC(MAP)
    - Le MCAUSER du channel reste reseigné:
      - **MCA user ID . . . . . : {@€-|D&F$**
- **TYPE(SSLPEERMAP).**
    - SSLCERTI OU SSLPEER (pas encore statué ☹)
- **TYPE(BLOCKADDR)**
  - Pas utilisé ou de façon temporaire.

# 4- Choix d'une application.



# 4- Connexion entre Server application et Mainframe.

- **Server Application.**
  - Identifier.
    - le compte / Password à véhiculer (en accord avec le nommage cible).
    - @Ip du Server source.
    - les éléments de connexion cible.
      - **NT.SVRCONN / 10.111.11.11 / 1414**

:

# 4- Connexion entre Server application et Mainframe.

- **Server Mainframe.**
  - Déclarer
    - le Userid du CLNTUSER et son Password (pas expiration) dans l'External Sécurity (TSS).
    - le Userid du MCAUSER (chlauth) (pas expiration) dans l'External Sécurity (TSS).
      - Autoriser le Userid aux Queues (Lecture / écriture).
  - Définir CHLAUTH.
      - Aucun connexion sur ce canal

```
SET CHLAUTH(NT.SVRCONN) TYPE(ADDRESSMAP) +
ADDRESS('*') +
DESCR('block all connexions with channel') +
USERSRC(NOACCESS)
```

# 4- Connexion entre Server application et Mainframe.

## Server Mainframe (2).

- Définir CHLAUTH.
  - Validation de la Chlauth via une autre adresse mais même Userid / Password.

**SET CHLAUTH(NT.SVRCONN)  TYPE(USERMAP) ADDRESS('10.444.44.44') +**
**CHCKCLNT(REQUIRED)  CLNTUSER('USRLEND') MCAUSER('ANOTHER') +**
**DESCR('Validate Rules and access with user / parwword') USERSRC(MAP).**

java MQPut DMQ1 LOLO.EMIS.QUEUE NT.SVRCONN 10.000.00.000 1414
**USRLEND PASSWORD1.**
MQJE001: Completion Code '2', Reason '2035'.
A WebSphere MQ Error occured : Completion Code 2 Reason Code 2035
com.ibm.mq.MQException: MQJE001: Completion Code '2', Reason '2035'.

  - Création de la Chlauth applicative.

**SET CHLAUTH(NT.SVRCONN) TYPE(USERMAP) ADDRESS(10.000.00.00)**
**CHCKCLNT(REQUIRED) CLNTUSER(USRLEND) +**
**DESCR('Rule Application for Project LEND') +**
**MCAUSER(ANOTHER) USERSRC(MAP)**

# 4- Connexion entre Server application et Mainframe.

## Server Mainframe (3).

- Définir CHLAUTH.
  - Contrôle Channel utilise la Chlauth souhaitée.

**DIS CHLAUTH (NT.SVRCONN) ADDRESS('10.000.00.000') CLNTUSER('USRLEND') +**
**MCAUSER('ANOTHER') MATCH(RUNCHECK)**

**CSQN205I COUNT= 3, RETURN=00000000, REASON=00000000**
**CSQM454I DMQ1**

**CHLAUTH(NT.SVRCONN) TYPE(USERMAP) ADDRESS(10.000.00.000)**
**CHCKCLNT(REQUIRED) CLNTUSER( USRLEND ) MCAUSER(ANOTHER)**
**USERSRC(MAP)**

# 4- Connexion entre Server SAA et Mainframe

- **Server Application.**
  - Installer Certificat IBM MQ.
    - AC + Certificat Userid Applicatif.
  - Identifier le CN du certificat Cible.
  - Créer une entrée CCDT.

**DEFINE CHANNEL(SAA.SVRCONN) DESCR( ) TRPTYPE(TCP)**
**CONNAME('10.111.11.11(1414)') QMNAME(DMQ1)**
**SSLCIPH(TLS_RSA_WITH_AES_256_CBC_SHA256)**
**SSLPEER(CN=lolo20.mq.calolo.local,OU=11,OU=Laurent,OU=PKI Prive,O=Banque Europenne,C=FR)**
**SHARECNV(10)** :

# 4- Connexion entre Server SAA et Mainframe

## Server Mainframe (Solution 1).

- Installer (si pas déjà fait)
  - AC + Certificat Queue Manager.
- Identifier le CN du Certificat Userid Applicatif cible.
- Definir le Channel SVRCONN.

```
DEFINE CHANNEL(SAA.SVRCONN) CHLTYPE(SVRCONN)
QSGDISP(QMGR) TRPTYPE(TCP) DESCR('APPLICATION LEND en provenance de
SAA HOMOLOGATION') DISCINT(6000)
SSLCIPH(TLS_RSA_WITH_AES_256_CBC_SHA256)
SSLPEER('CN=SERVER_SWIFT.HOMOLO,OU=FR,OU=EU,O=BK,L=Paris,ST=IDF,C=Fr
ance') HBINT(300)
```

- Définir CHLAUTH.

```
SET CHLAUTH(SAA.SVRCONN) TYPE(SSLPEERMAP) SSLCERTI(CN=*)
SSLPEER(CN=*) USERSRC(NOACCESS).
SET CHLAUTH(SAA.SVRCONN) TYPE(SSLPEERMAP)
MCAUSER(USRSAA) CHCKCLNT(ASQMGR)
SSLPEER(CN=*,OU=FR,OU=EU,O=BK,L=Paris,ST=IDF,C=FRANCE)
```

# 4- Connexion entre Server SAA et Mainframe

## Server Mainframe (Solution 2).

- Installer (si pas déjà fait)
  - AC + Certificat Userid Applicatif.
  - Identifier le Issuer du Certificat Userid Applicatif.

    Issuer's distinguished name CN=AUTORITY GROUP.OU=ABDC.OU=PKI PRIVE.O=Credit Agricole.C=EU

- Créer Channel SVRCONN.

  **DEFINE CHANNEL(SAA.SVRCONN) CHLTYPE(SVRCONN)**

  **QSGDISP(QMGR) TRPTYPE(TCP) DESCR('APPLICATION LEND en provenance de SAA HOMOLOGATION')**

  **SSLCIPH(TLS_RSA_WITH_AES_256_CBC_SHA256) MCAUSER( )**

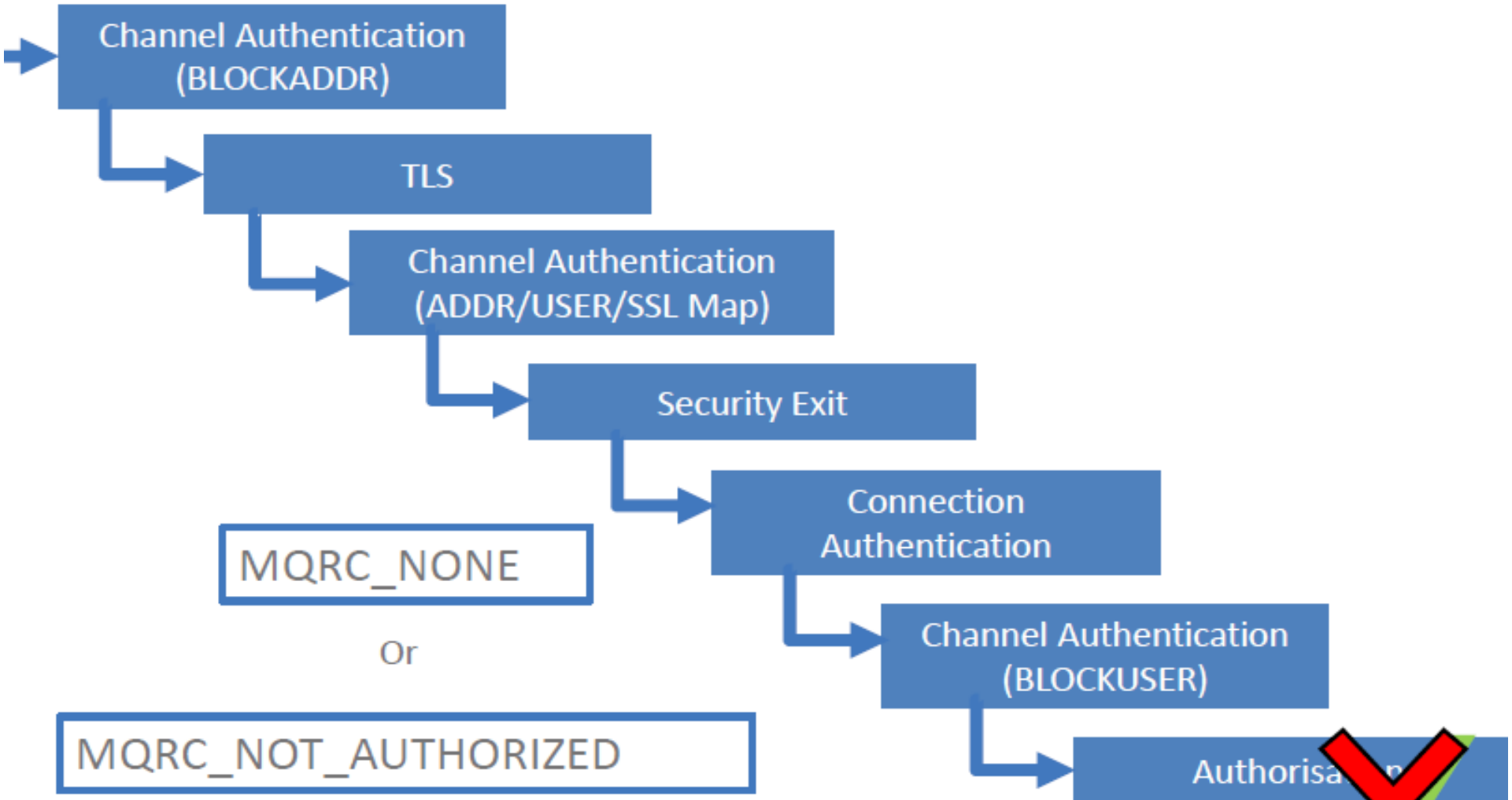
  **SSLPEER(CN=SERVER_SWIFT.HOMOLO,OU=EU,O=BK,L=Paris,ST=IDF,C=FRANCE**

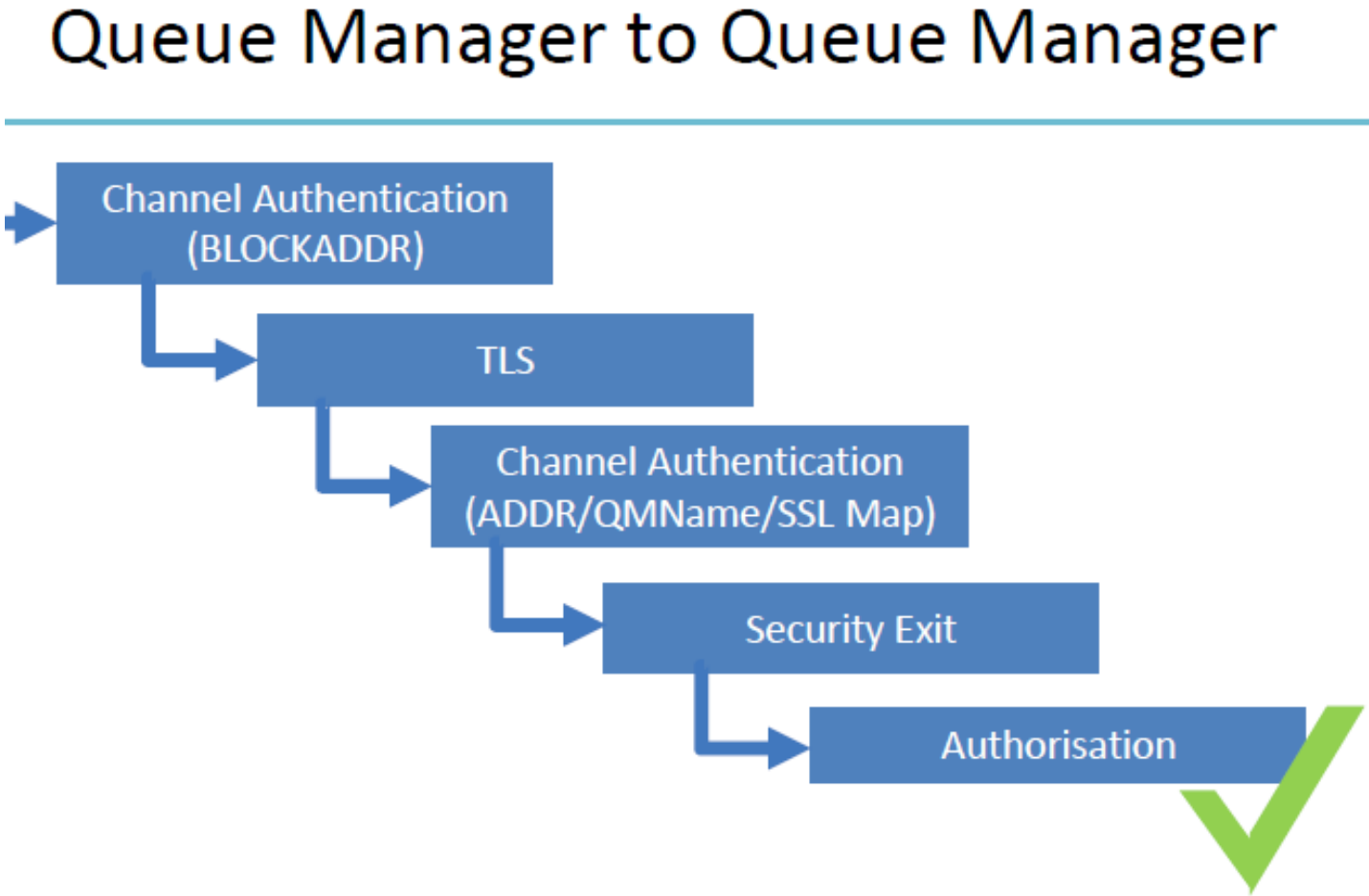
- Définir CHLAUTH.

  **SET CHLAUTH(SAA.SVRCONN) TYPE(SSLPEEMAP) SSLPEER('CN=*')-**
  **SSLCERTI('CN=*') USERSRC(NOACCESS)** *(SSLPEER obligatoire)*

  **SET CHLAUTH(SAA.SVRCONN) TYPE(SSLPEERMAP)**
  **MCAUSER(USRSAA) CHCKCLNT(ASQMGR) SSLCERTI('CN=AUTORITY GROUP.OU=ABDC.OU=PKI PRIVE.O=Credit Agricole.C=EU')** SSLPEER('CN=*')

# 5- Ibm Cloud Technical University 2016.




Queue Manager to Queue Manager
Channel Authentication (BLOCKADDR)
TLS
Channel Authentication (ADDR/QMName/SSL Map)
Security Exit
Authorisation

# 5- Conclusion.

- **nombreuses documentations disponibles sur la sécurité.**
  - Morag, T.Rob, Robert Parker, Mike Cregger
- **Beaucoup de tests et lectures effectués.**
- **Reste énormément à faire.**
- **On est confiant ……..**

# QUESTIONS ?