WebSphere. software

Guide MQ du 10/01/2006

La sécurité dans WebSphere MQ

Luc-Michel Demey

Demey® Consulting

lmd@demey-consulting.fr

Plan

- Terminologie & Objectifs
- Les messages MQ
- Inventaire de l'existant

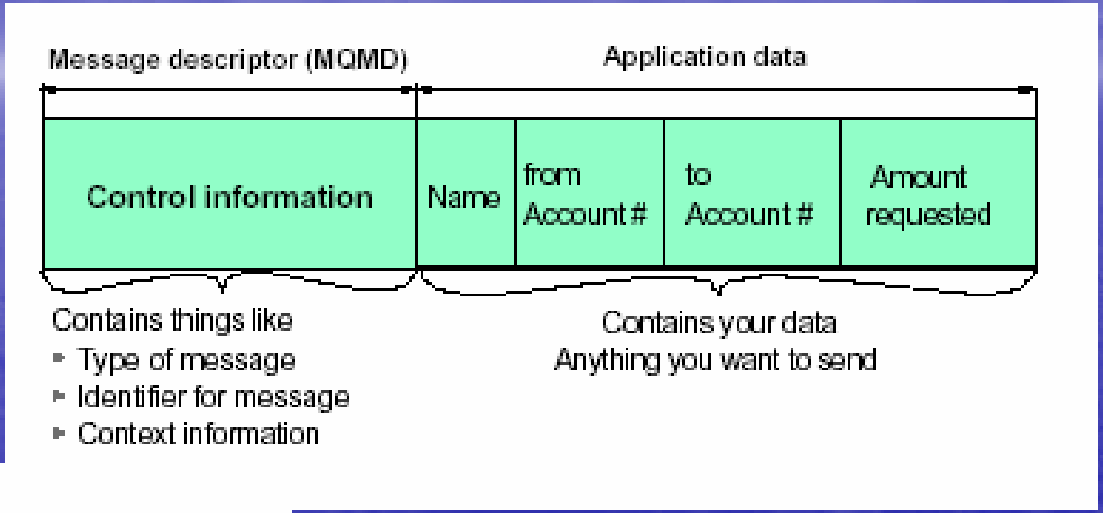
Terminologie

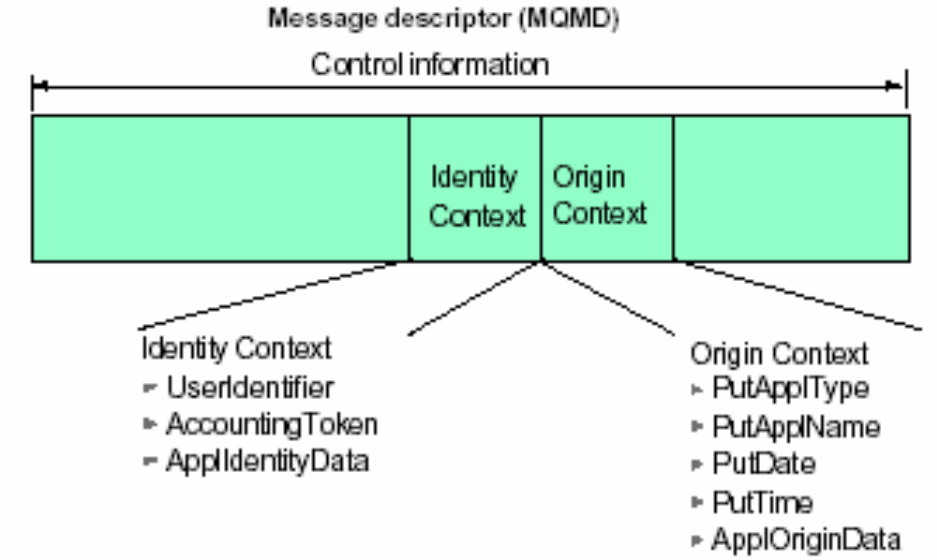
- Identification :
  - Capacité d'identifier de manière certaine un utilisateur ou une application dans un système
- Authentification :
  - Capacité pour un utilisateur ou une application de prouver qui il/elle est

Objectifs

- Limiter l'accès aux utilisateurs autorisés
  - Contrôle d'accès
- Tracer les actions et les anomalies
  - Audit
- Protéger les données sensibles de la divulgation
  - Confidentialité
- Détecter les modifications des données
  - Intégrité
- Prouver la réception d'un message
  - Non répudiation

Anatomie d'un message





Sécurité WebSphere MQ : De quoi dispose-t-on ?

- **Audit**
- Intégrité des données
- Non-répudiation
- Contrôle d'accès
- Identification
- Authentification
- Confidentialité

Audit – z/OS

- Standard External Security Manager (ESM) facilities
- Reslevel audit records

  RACROUTE REQUEST=AUDIT
- Controlled via

  ZPARM: RESAUDIT(YES|NO)
- IMS Bridge audit records

  RACROUTE REQUEST=AUDIT

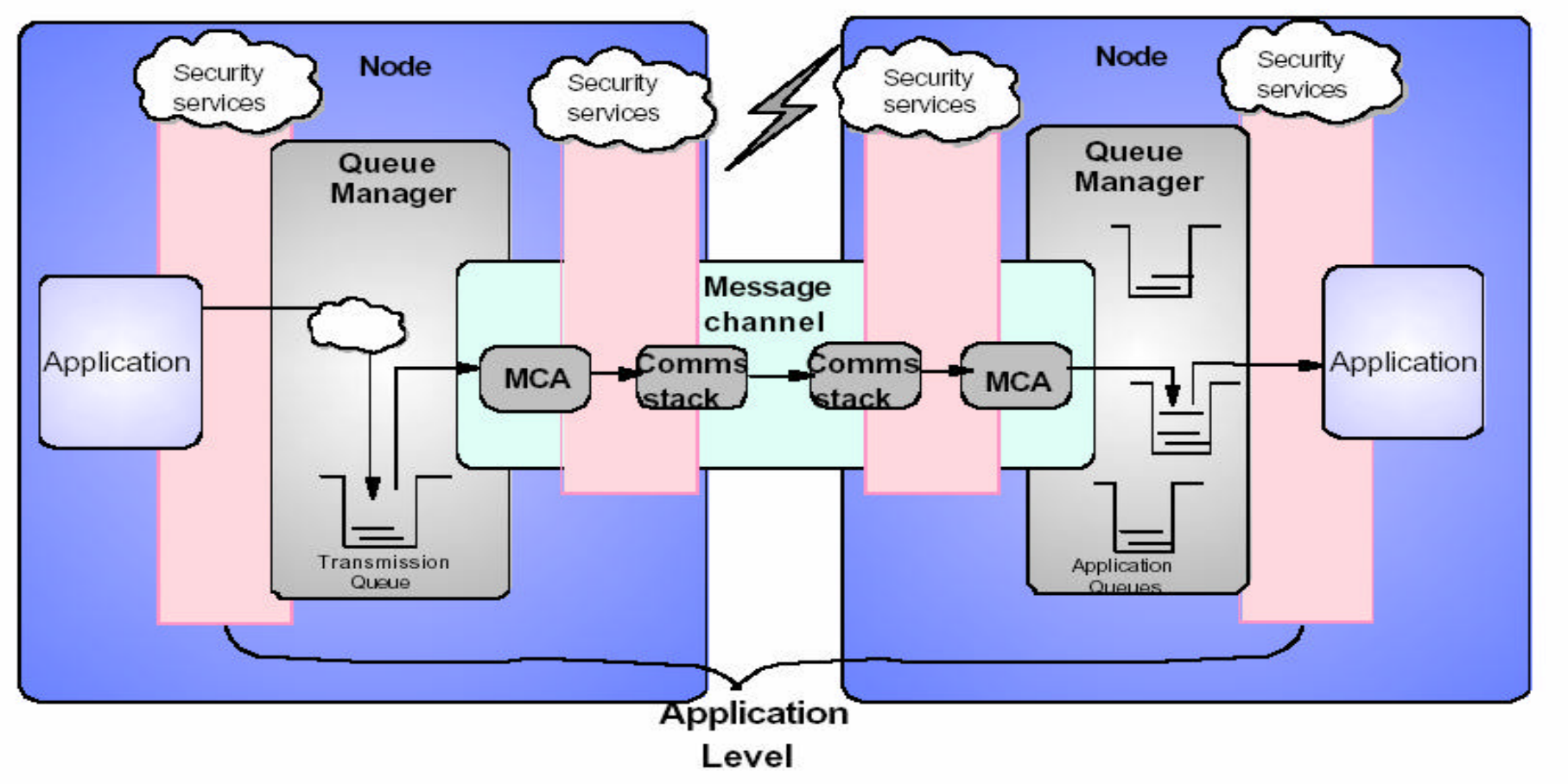
Audit - Distribué

- MQRC_NOT_AUTORIZED events
  - Envoyés dans la file SYSTEM.ADMIN.QMGR.EVENT
  - MQRQ_CONN_NOT_AUTHORIZED
  - MQRQ_OPEN_NOT_AUTHORIZED
  - MQRQ_CLOSE_NOT_AUTHORIZED
  - MQRQ_CMD_NOT_AUTHORIZED

Sécurité WebSphere MQ : De quoi dispose-t-on ?

- Audit
- **Intégrité des données**
- **Non-répudiation**
- Contrôle d'accès
- Identification
- Authentification
- Confidentialité

Sécurité au niveau Applicatif



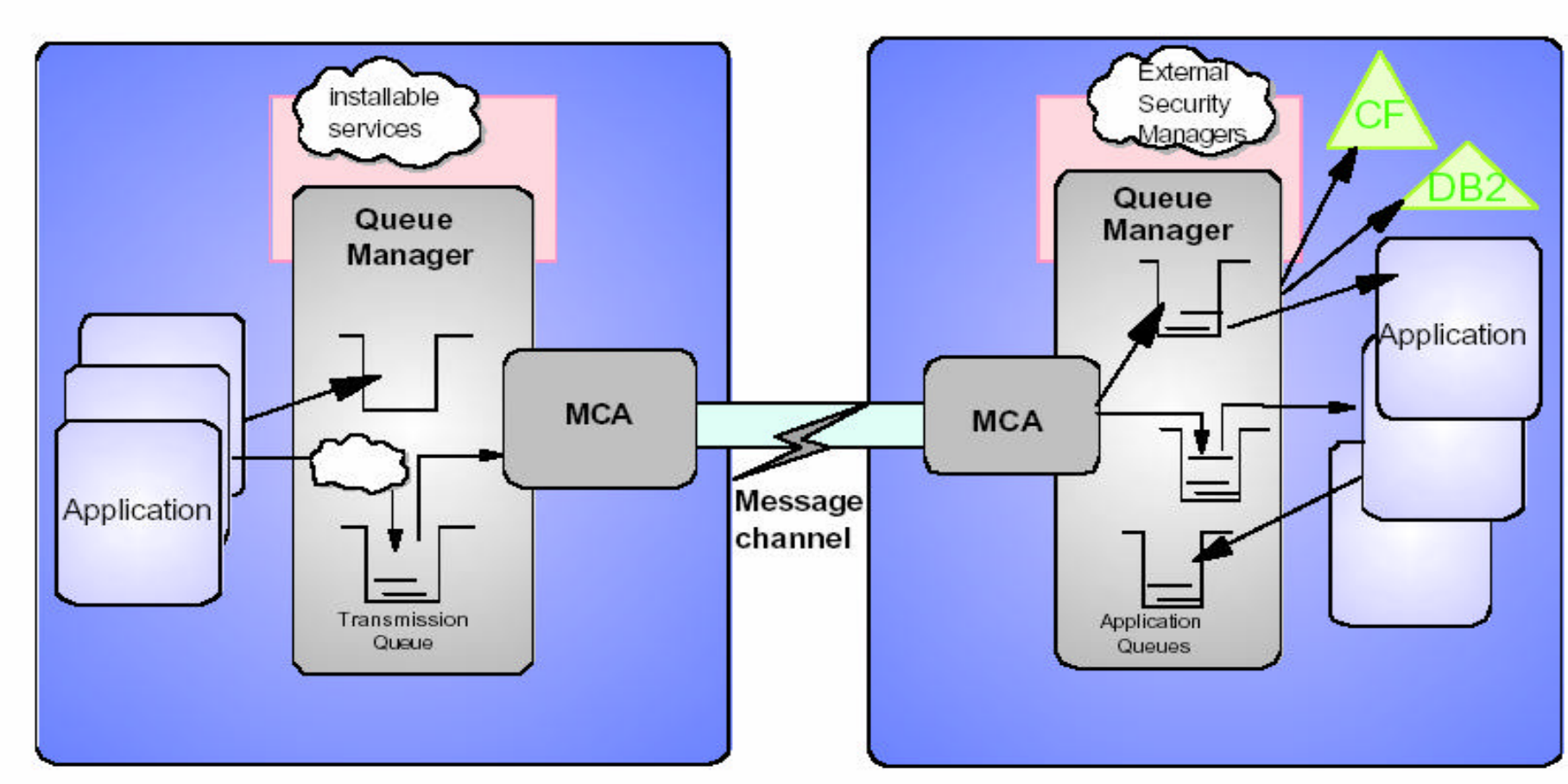
De quoi dispose-t-on ?

- Intégrité des données
  - SSL
  - WebSphere MQ Security Edition (/w TAM4BI)
  - API exits (exemples fournis)
  - Produits commerciaux
- Non répudiation
  - WebSphere MQ Security Edition (/w TAM4BI)
  - API exits (exemples fournis)
  - Produits commerciaux

Sécurité WebSphere MQ : De quoi dispose-t-on ?

- Audit
- Intégrité des données
- Non-répudiation
- **Contrôle d'accès**
- Identification
- Authentification
- Confidentialité

Mécanismes de contrôle d'accès



Mécanismes de contrôle d'accès

- Deux systèmes équivalents :
  - SAF (*System Autorisation Facility*) sur z/OS
  - OAM *Installable Services* en distribué
- Sécurisation des commandes :
  - d'administration MQ
  - d'administration des objets MQ

Sécurisation de l'administration MQ

- Commandes MQ
- Utilisation de l'Explorateur WebSphere MQ
- Panneaux Ops et Control sur z/OS
- Utilitaire CSQUTIL sur z/OS
- Accès aux datasets des Queue Managers sur z/OS

Administration MQ sur Unix & Windows

- Il faut être membre du groupe « mqm » ou être un administrateur windows
- Les administrateurs peuvent utiliser :
  - setmqaut
  - runmqsc
  - crtmqm / strmqm / ...
- Attention aux clients d'administration

Administration MQ sur AS/400 – i5/OS

- Il faut être membre du groupe « QMQMADM » ou avoir les droits *ALLOBJ
- Les administrateurs peuvent utiliser :
  - GRTMQMAUT
  - STRMQMMQSC
  - Les commandes de création d'objets :
    - CRTMQMQ / CHGxxx / DLTxxx
    - CRTMQMCHL / ...
- Attention aux clients d'administration

Administration MQ sur z/OS

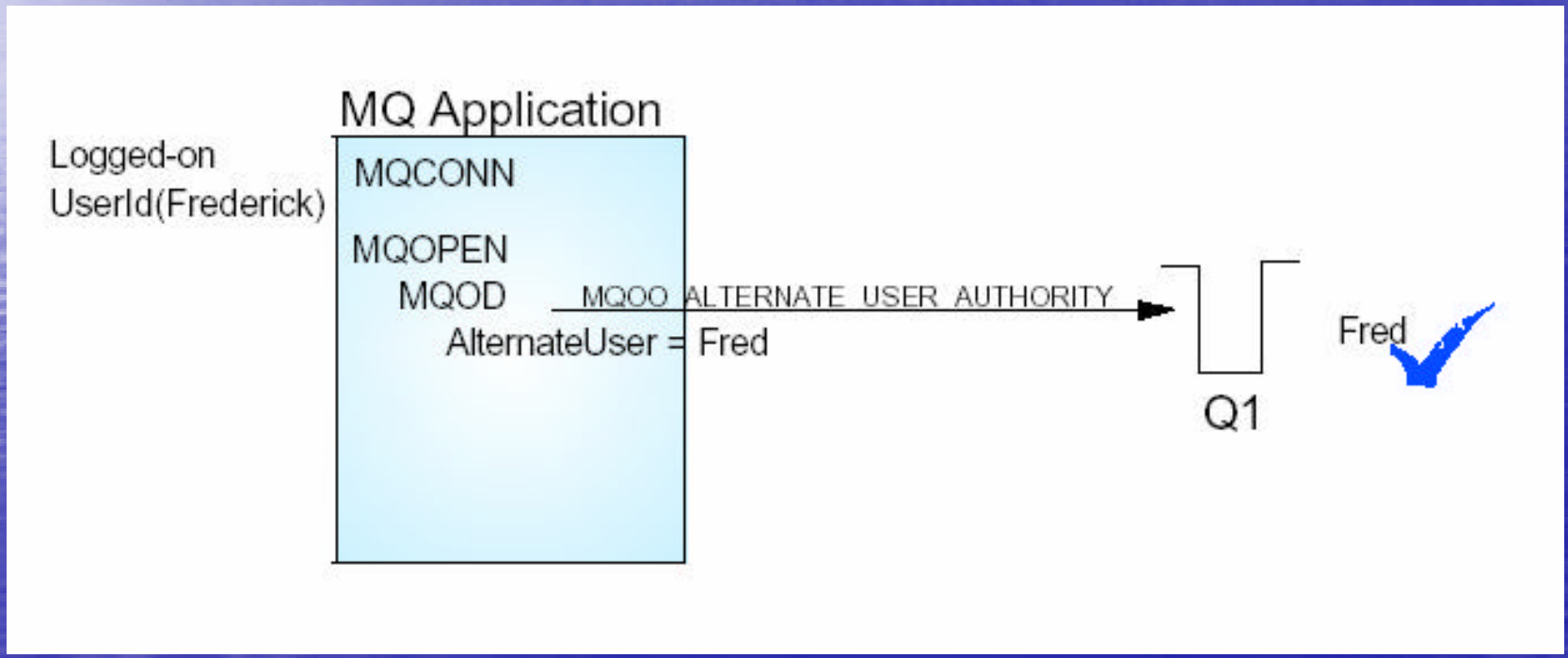
- **Qmgr Security**
  - controlled by RACF profiles that have a special meaning to WebSphere MQ
    - Used to set WebSphere MQ for z/OS internal security switches
- **Command and Command resource security**
  - Command security controls who is allowed to issue an MQSC command
  - Command Resource security - protects WebSphere MQ resources that can have commands issued against them.
- **Data set security:**
  - Qmgr and Chinit started task procedures
  - Access to Qmgr datasets for example:
    - CSQINP1
    - CSQINP2
  - Access to the Ops and Control panels
  - Access to the CSQUTIL Utility program
  - Access for Qmgrs that will use Coupling Facility Structures
  - Access for Qmgrs that will use DB2
  - Access for Qmgrs that will use IMS

Contrôle d'accès via les API

- Queue Managers
  - Lors du MQCONN ou du MQCONNX
- Queues
  - Lors du MQOPEN (ou du MQPUT1)
  - Cas des queues dynamiques (MQOPEN/MQCLOSE)
  - XMITQ si « fully qualified » queue éloignée
  - SYSTEM.CLUSTER.TRANSMIT.QUEUE

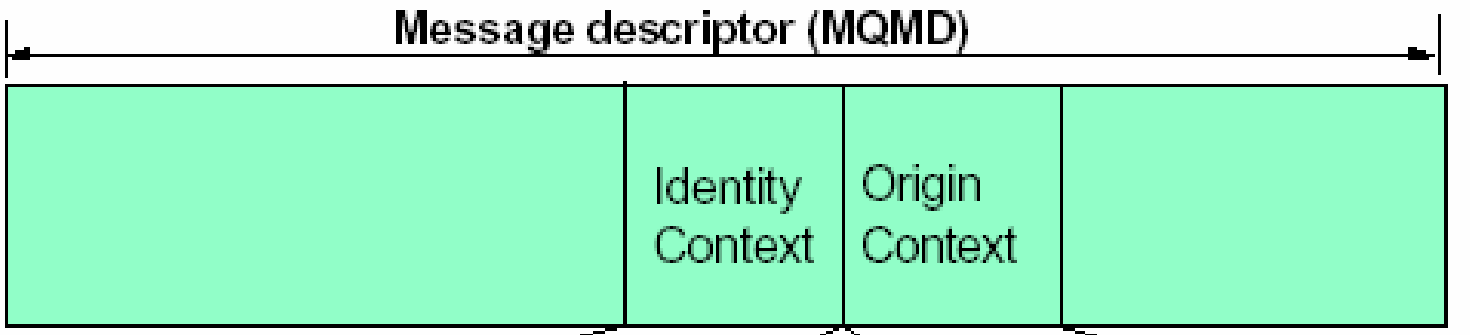
Contrôle d'accès via les API - 2

- Alternate Userid



Contrôle d'accès via les API - 3

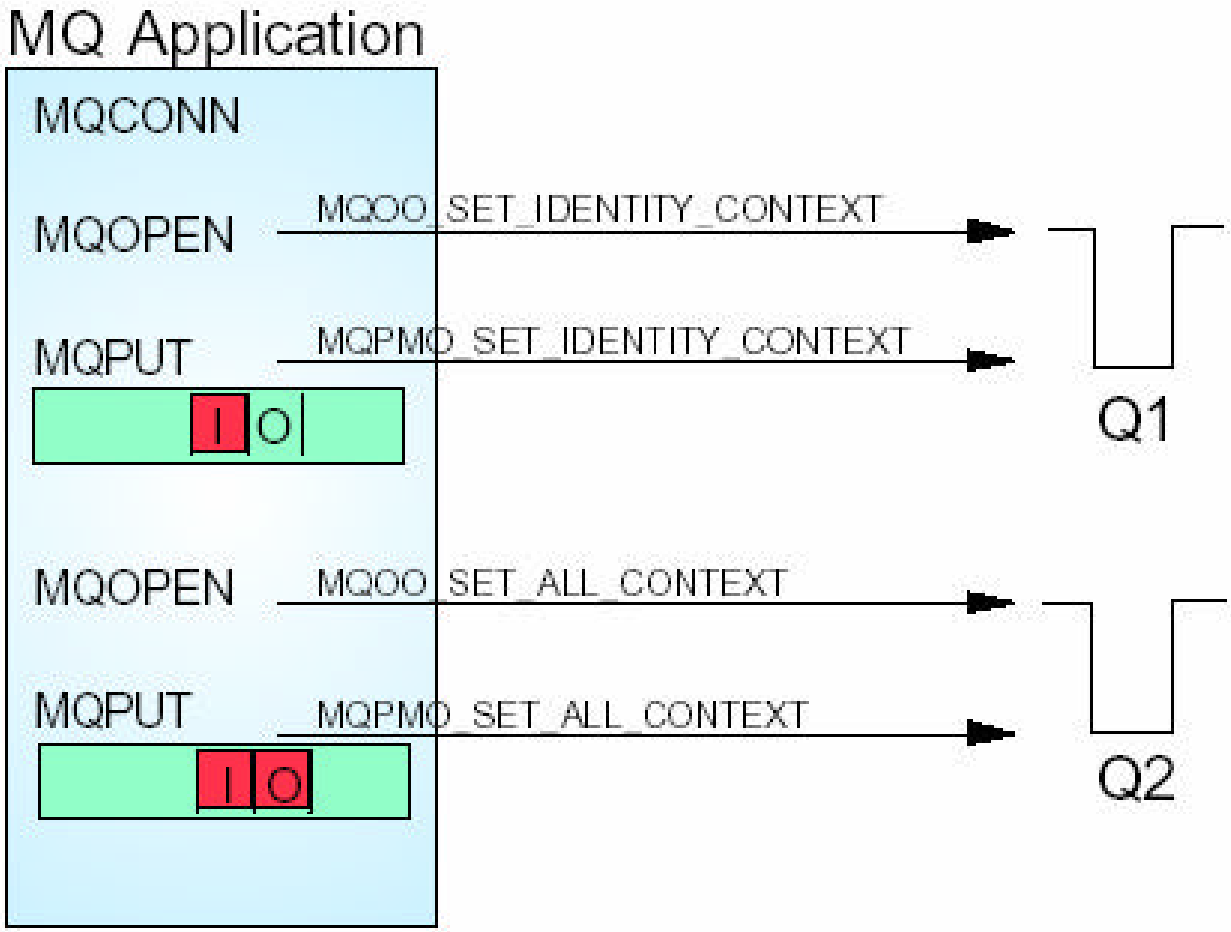
- Message context



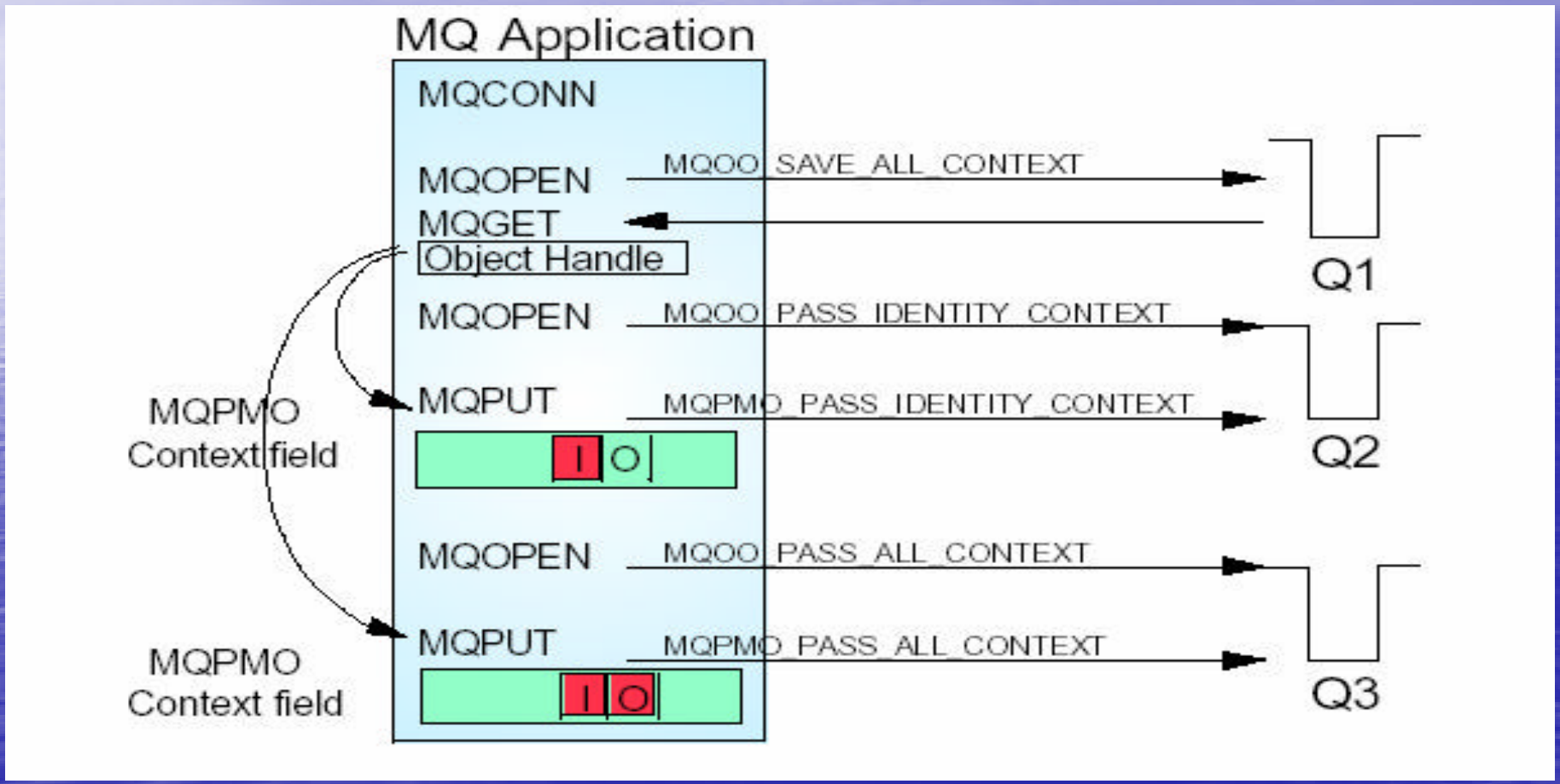
Identity Context
- UserIdentifier
- AccountingToken
- AppIdentityData

Origin Context
- PutApplType
- PutApplName
- PutDate
- PutTime
- AppIOriginData

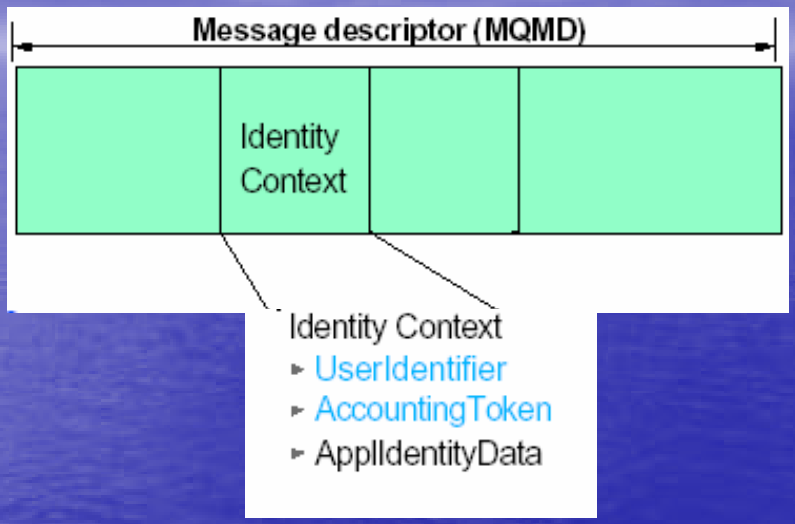
API Security – Setting Context



API Security – Passing Context



Identity Context – Compléments



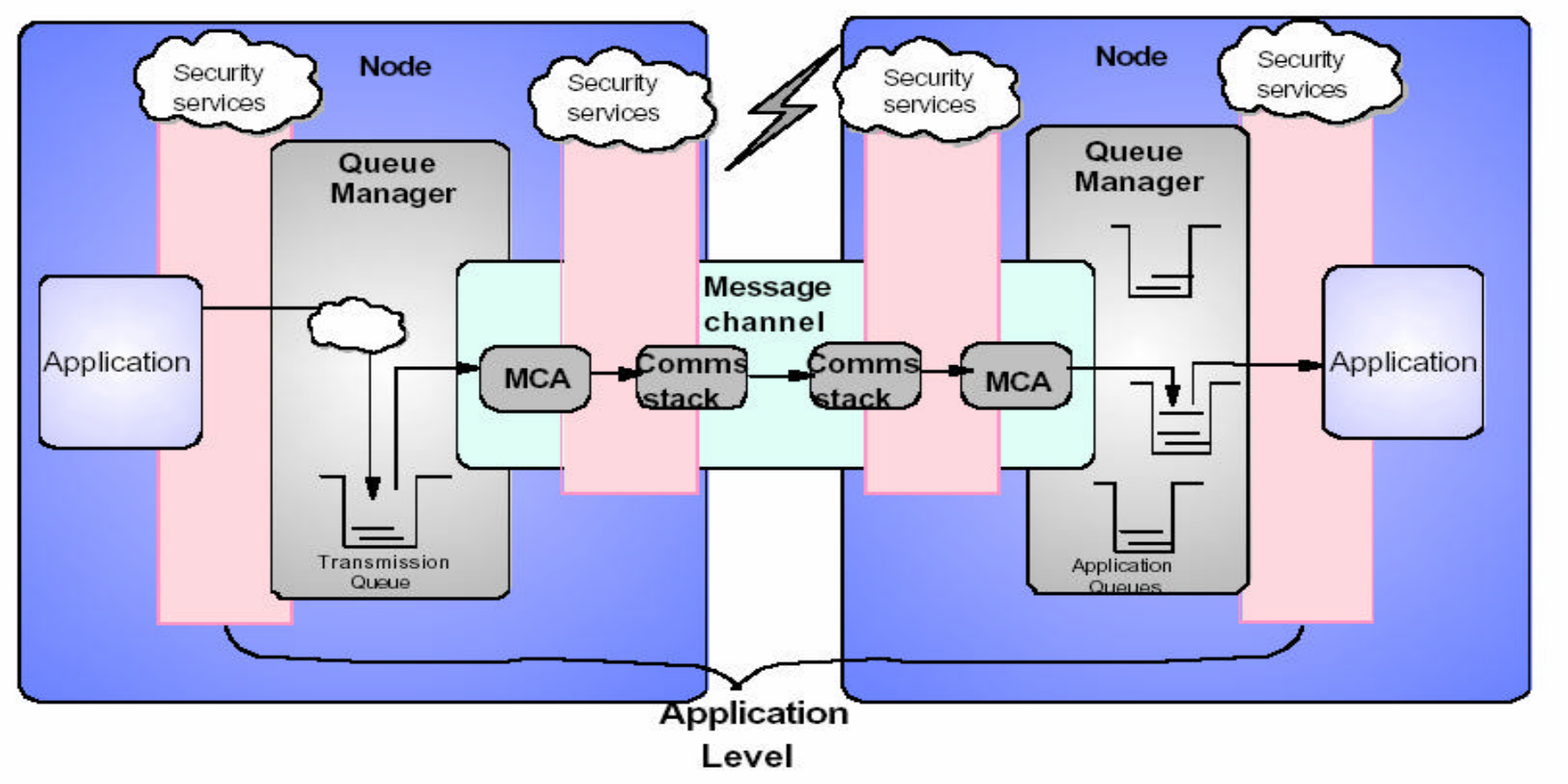
User Identifier :

- UserId d'origine ou Alternate UserId
- Utilisé par les Expiry & COD

Accounting Token :

- Windows SID

Sécurité au niveau lien



Sécurité au niveau lien

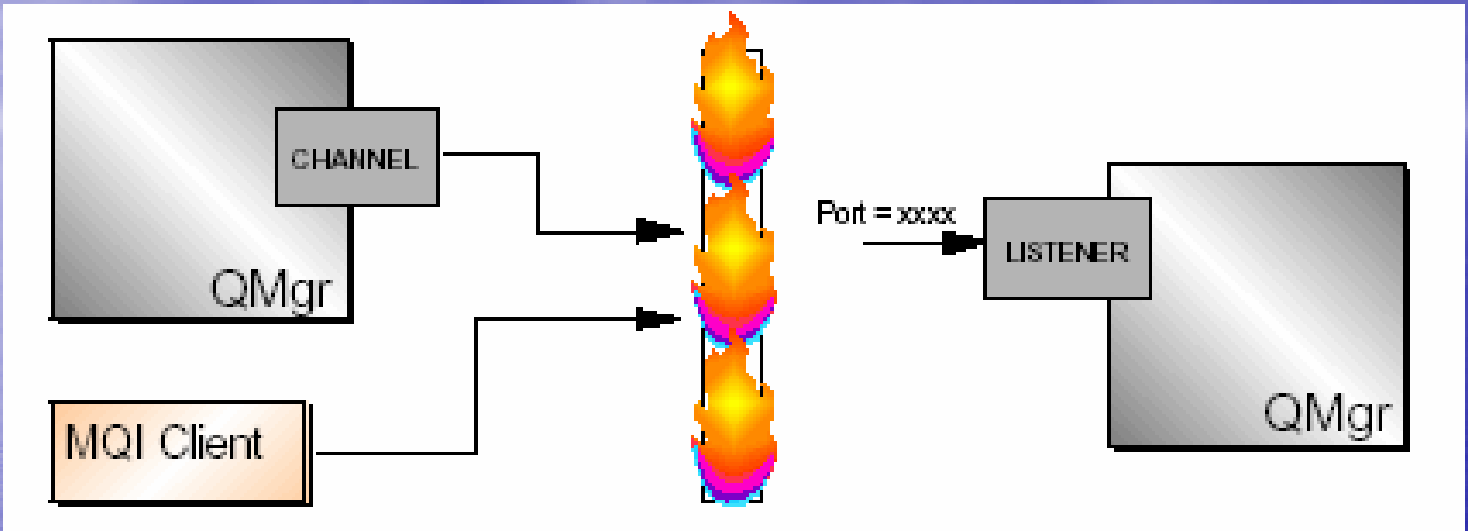
- Confidentialité
  - SSL
  - Exits
- Intégrité (niveau lien)
  - SSL
- Authentification du partenaire
  - SSL
  - Exits de sécurité
- Identification du partenaire
  - Message Context
  - API Exits
  - Exits de sécurité
- Contrôle d'accès
  - MCAUSER
  - Put Authority
  - Message Userid
  - Firewalls
  - ...

Put Autority

- Attribut du Channel Receiver
  - « Default » : les messages sont déposés avec les droits du user exécutant le MCA
  - « Context » : les messages sont déposés avec les droits du « userid » du message

  Sur z/OS, en plus :
  - « OnlyMCA »
  - « ALTMCA »

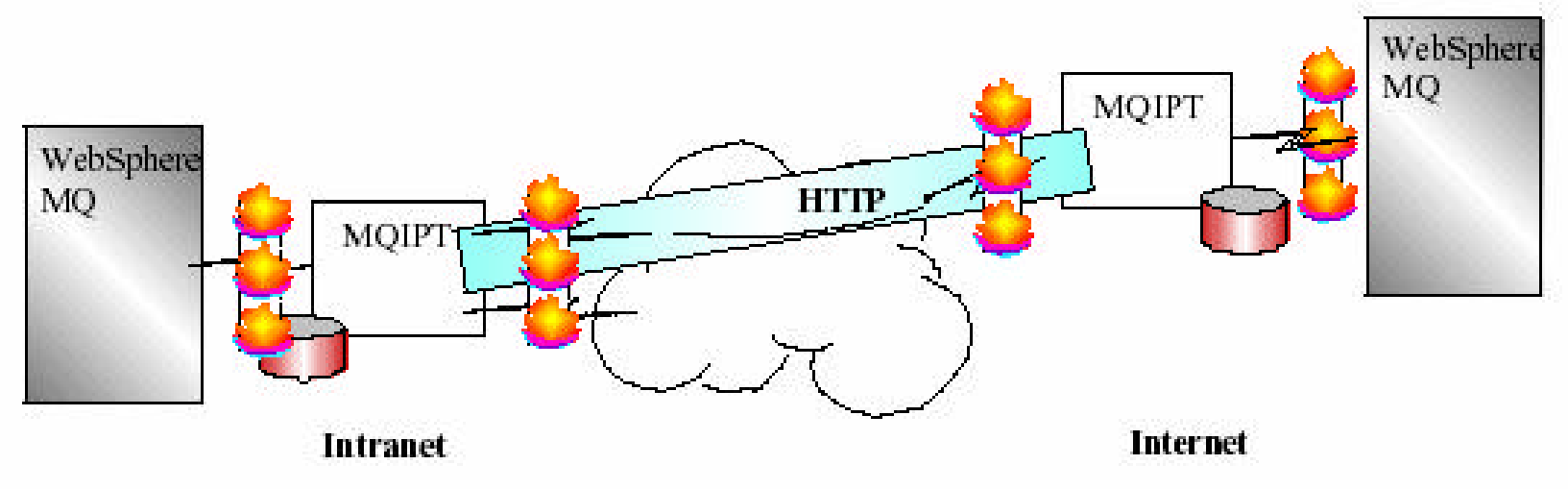
Firewalls



- Configuration du port du listener
- Possibilité de spécifier une plage de ports pour le channel sender / client :

DEFINE CHL(LMD) .... LOCLADDR((3200,3400))

WebSphere MQ Internet Passthru (MQIPT)



- Utilisation comme un « Proxy MQ »
- Installable en DMZ
- Supporte HTTP, HTTPS, SOCKS

Questions ?

Merci !!!