

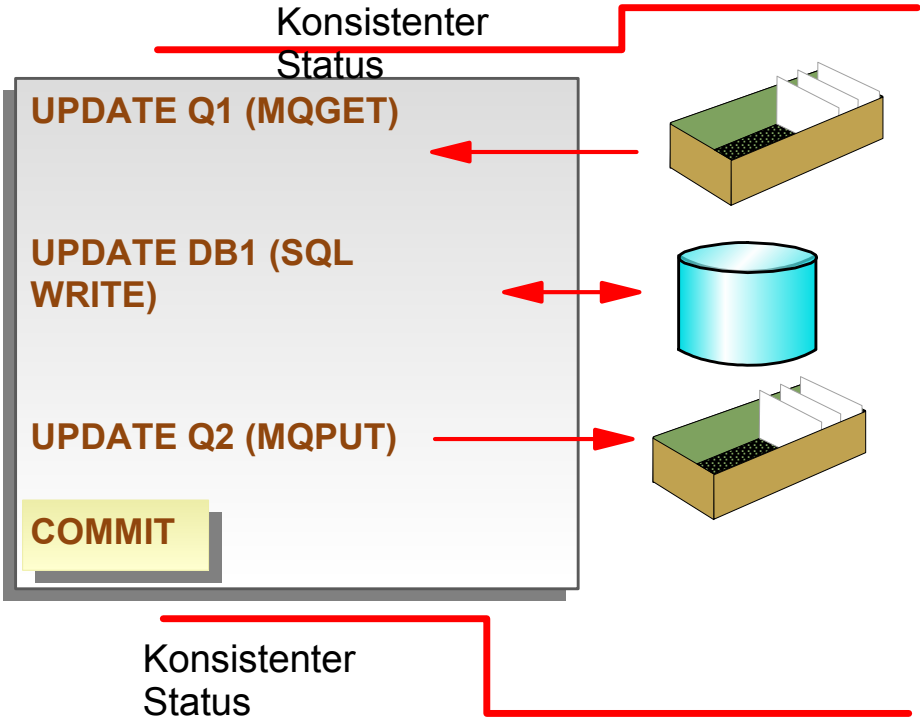
Hanseatic Mainframe Summit 2008

WebSphere MQ (MQSeries) Recovery and Security

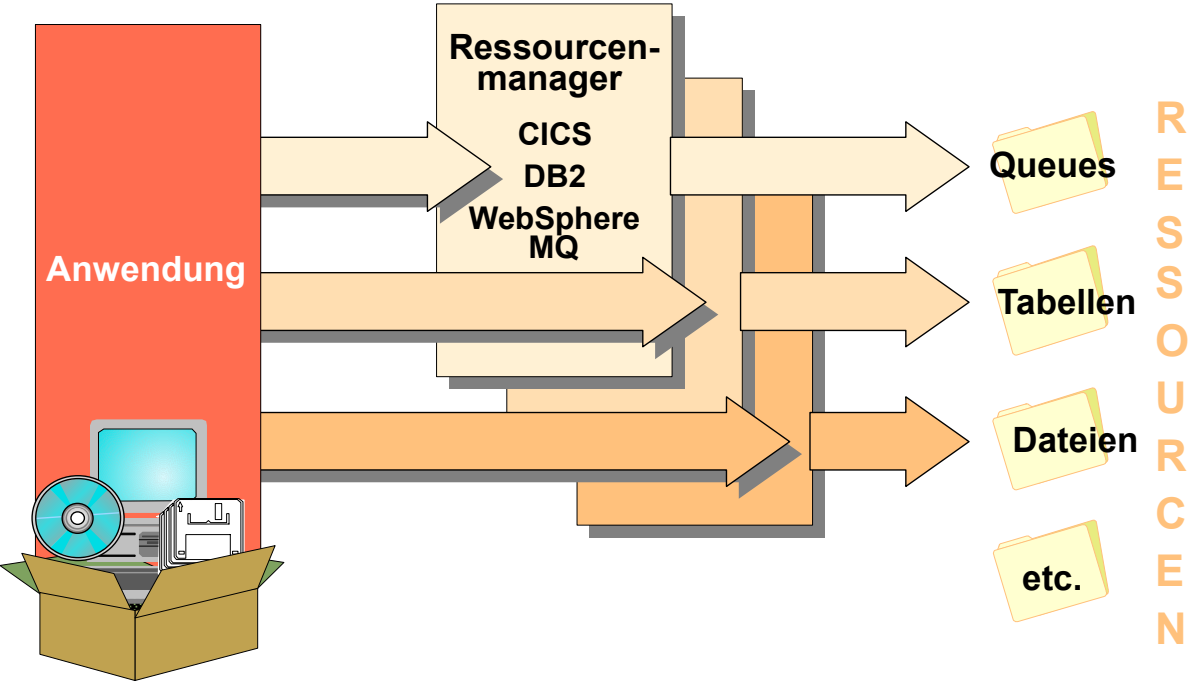
Marcel Amrein, IBM SWG Technical Sales
marcel.amrein@de.ibm.com



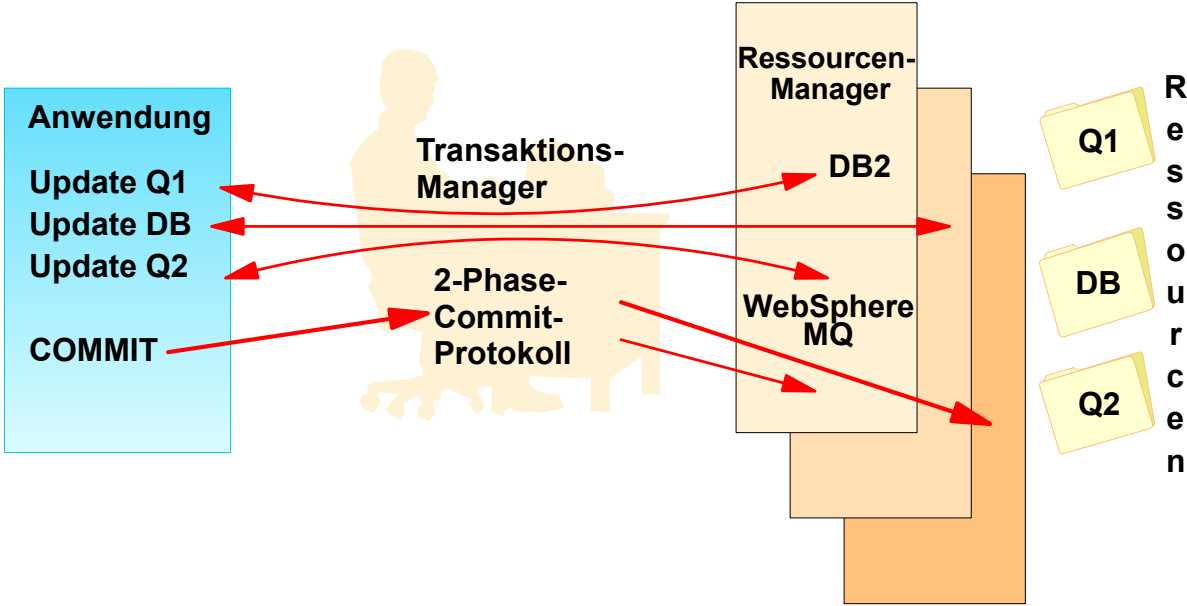
Unit of Work



Ressourcenmanager



Transaktions-Manager



MQGET innerhalb Syncpoint-Steuerung



**MQGET innerhalb
Syncpoint Kontrolle**



Commit



MQPUT innerhalb Syncpoint-Steuerung


MQPUT innerhalb
Syncpoint-Steuerung



1

A diagram showing a single MQPUT operation within a syncpoint control. A light blue box with a dashed border contains the number '1'. This box is enclosed within a larger orange-bordered container.

MQPUT innerhalb
Syncpoint-Steuerung



1 2

A diagram showing two MQPUT operations within a syncpoint control. Two light blue boxes with dashed borders, each containing a number ('1' and '2'), are placed side-by-side. Both boxes are enclosed within a larger orange-bordered container.

MQPUT innerhalb
Syncpoint-Steuerung



1 2 3

A diagram showing three MQPUT operations within a syncpoint control. Three light blue boxes with dashed borders, each containing a number ('1', '2', and '3'), are placed side-by-side. All three boxes are enclosed within a larger orange-bordered container.

Commit



1 2 3

A diagram showing three committed MQPUT operations. Three solid light blue boxes, each containing a number ('1', '2', and '3'), are placed side-by-side. All three boxes are enclosed within a larger orange-bordered container.

Koordinierung von lokalen Units of Work

Eine **lokale** Unit of Work ist ein Einheit, in der nur die Ressourcen des Queue Managers aktualisiert werden

```
MQGET Nachricht aus Server-Queue
MQPUT zusätzliche Anforderungen
MQPUT Antwortnachricht
if error . . .
    MQBACK
if OK . . .
    MQCMIT
```

Koordination globaler UOWs

Eine **globale Unit of Work** ist eine Einheit, in der auch die Ressourcen anderer Ressourcenmanager aktualisiert werden.

```
MQBEGIN
MQGET-Nachricht aus Server-Queue
EXEC SQL INSERT Datenbanksatz
MQPUT Antwortnachricht
...
if error ...
    MQBACK
if OK ...
    MQCMIT
```


Datenbankkoordination

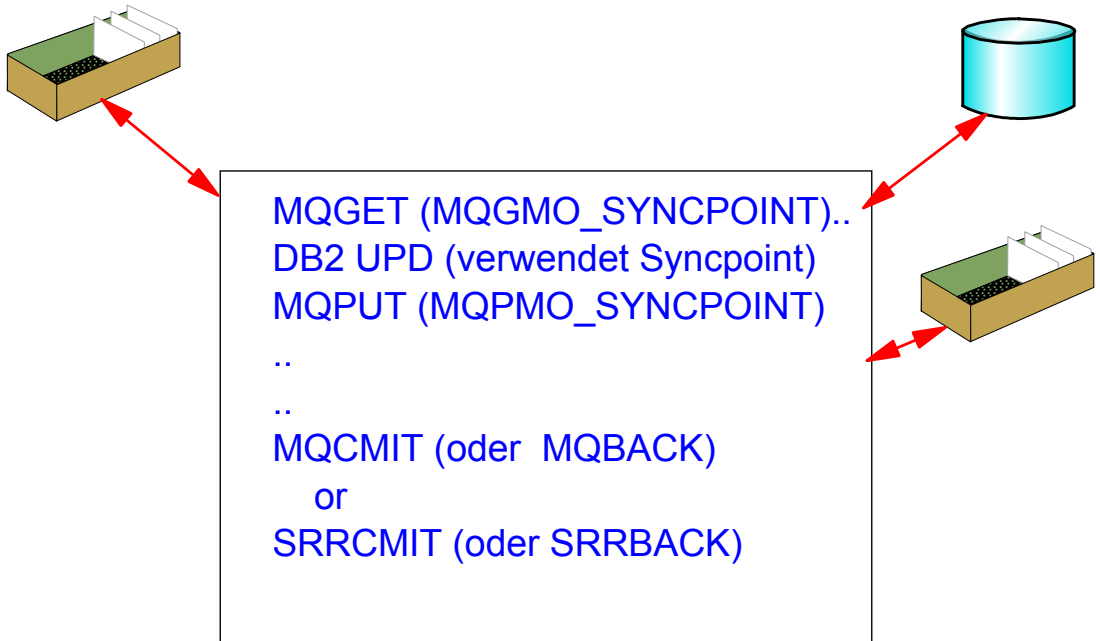
• Unterstützte Datenbankmanager

Plattform	DB2	Oracle	Sybase
AIX	✓	✓	✓
HP-UX	✓	✓	✓
OS/400	✓		
Solaris	✓	✓	✓
Windows	✓	✓	✓

• Einschränkungen

- Ein WebSphere MQ-Client kann an einer globalen Unit of Work nicht teilnehmen
- Nur ein Queue Manager darf an einer globalen Unit of Work teilnehmen
- Normalerweise muss die Aktualisierung der WebSphere MQ- und Datenbankressourcen im gleichen System erfolgen
- Ein Datenbankserver kann sich jedoch auf einem anderen System befinden, sofern er eine XA-konforme Client-Funktion bereitstellen kann

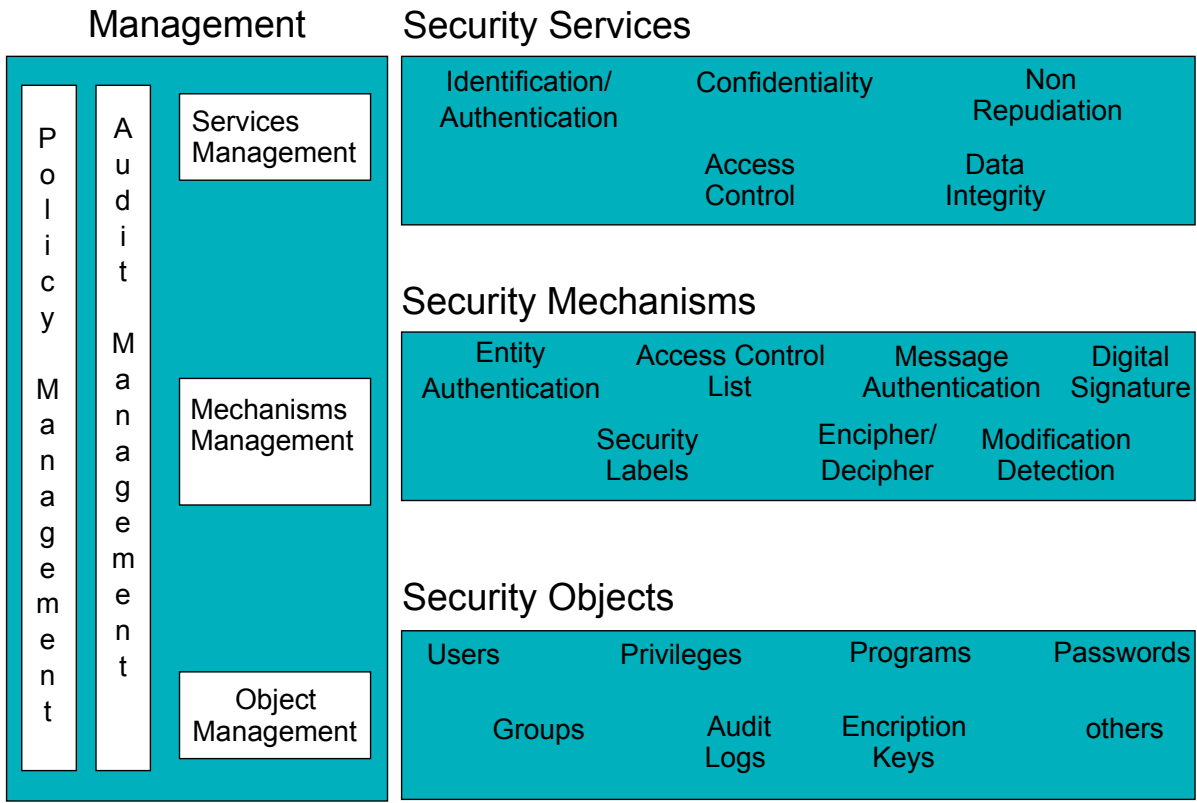
WebSphere MQ for z/OS RRS-Unterstützung



Zusammenfassung

- WebSphere MQ ermöglicht den Nachrichten die Beteiligung an der Verarbeitung von Units of Work
- WebSphere MQ ist ein Ressourcenmanager
- WebSphere MQ kann in einigen Fällen ein Transaktionsmanager sein
- Diskussion der Verarbeitung von Units of Work im Anwendungsdesign

IBM-Sicherheitsarchitektur



Implementierung

Erforderliche Mechanismen auf verschiedenen Stufen:

Anwendungscode und Exits

Produktcode

Umgebungscode

Netzwerkcode

Anwendungscode

Queue Managers
(OAM)
Exits

Umgebung
(CICS, OS/400, RACF . . .)
Exits

Vernetzung (LU6.2, TCP/IP)

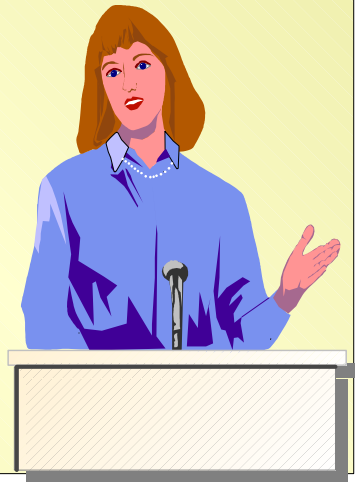
Sicherheit in WebSphere MQ



- **Zugriffskontrolle**
 - Ressourcen
 - Befehle
- **Nachrichtenkontext**
 - Wird mit Nachricht übertragen
- **Exits**
 - MCA
 - Sicherheit
 - Nachricht
 - Senden/Empfangen
 - OAM
 - Intern
 - Extern
 - API

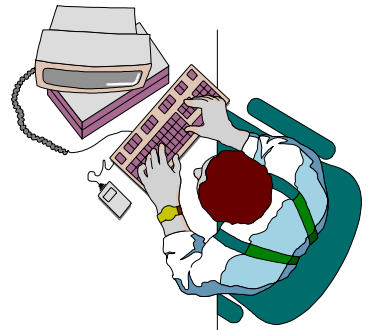
API-Sicherheit

- **Queue Sicherheit**
 - Benutzer-IDs
 - Optionen
- **Prozesssicherheit**
- **Namenslistensicherheit**
- **Kontextsicherheit**
 - MQOPEN/MQPUT1
- **Alternative Benutzersicherheit**



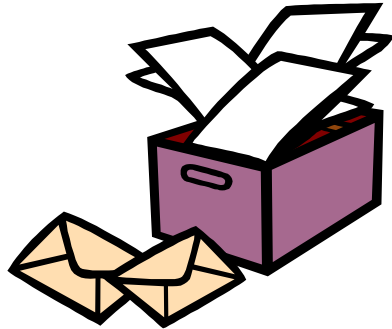
Command Security

- Eingabe des Befehls wird überprüft
- Basierend auf Benutzer-ID
 - Befehlssicherheit
 - Darf dieser Benutzer diesen Befehl ausgeben (z. B. - DISPLAY QUEUE)
 - Befehlsressourcensicherheit
 - Darf dieser Benutzer diese Ressource ändern (z. B. - DELETE QLOCAL ('Lohnabrechnung'))



Nachrichtenkontext

- Wird mit der Nachricht geliefert
 - im Nachrichtendeskriptor
- Besteht aus zwei Teilen
 - Anwendungsnamen
 - Benutzer-ID
 - Abrechnungstoken
 - Anwendungsdaten
 - Ursprungscontext
 - Identity Context
 - Typ
 - Datum und Zeit
 - Anwendungsdaten
- Ermöglicht Systemberechtigung auf ID-Basis
- Unterstützt Accounting-Information
- Ermöglicht Anwendungsberechtigung

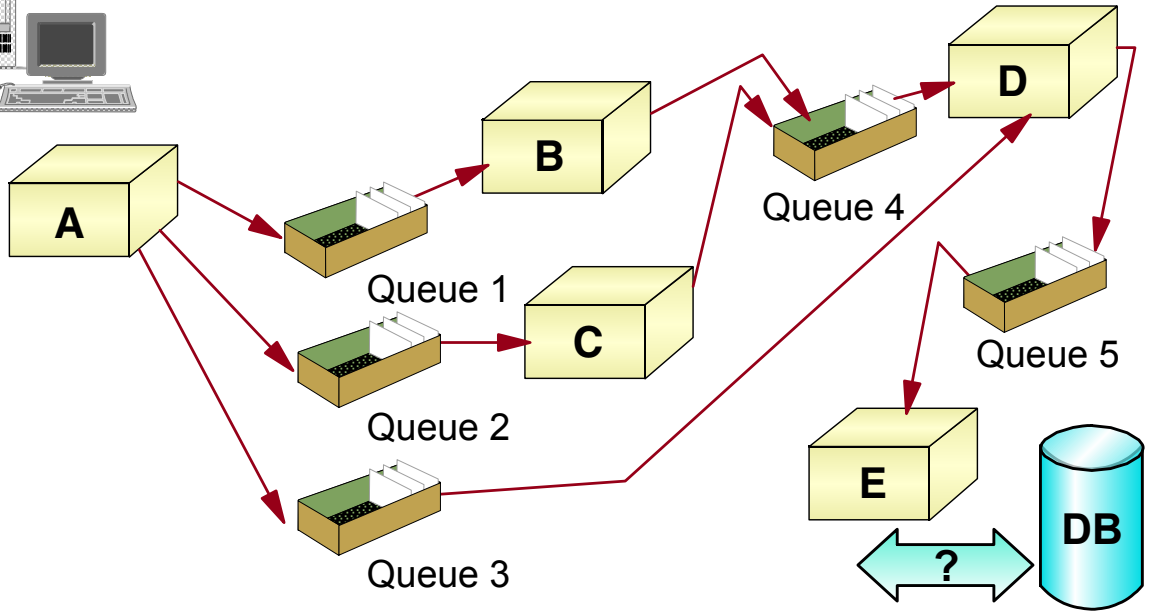
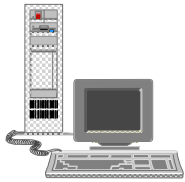


Benutzer-IDs

- TSO Benutzer-ID
- Adressraum-ID
- UNIX-Login
- Konsol-ID
- (keine)
- Verstöße werden protokolliert
 - Im Environment-Log
 - Im QMgr-Log
 - In der QMgr Event Queue



Remote-Zugriff



Befehle

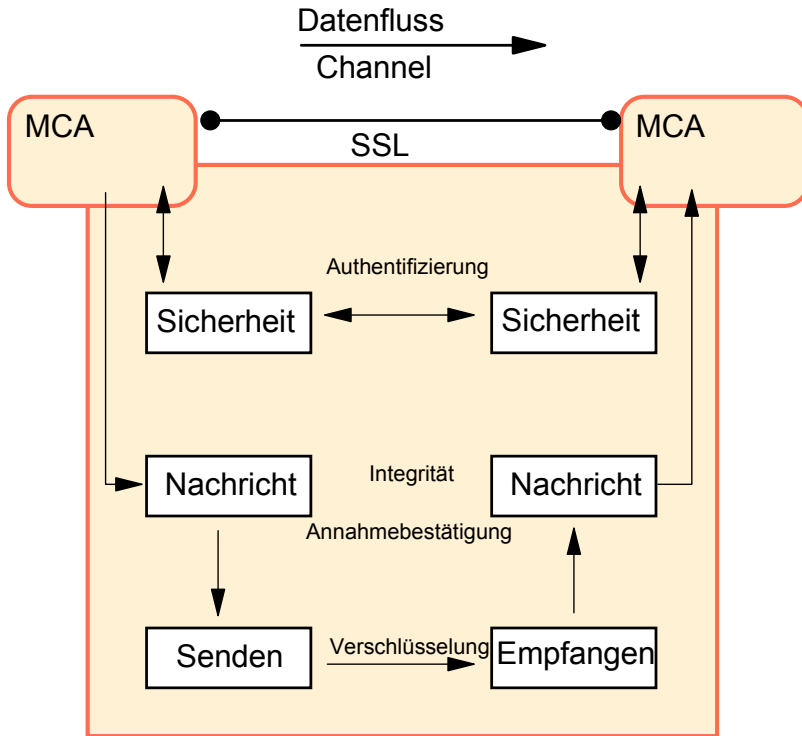
Authentifizierung

Nachrichtenkontext

*Zugriffs-
kontrolle*

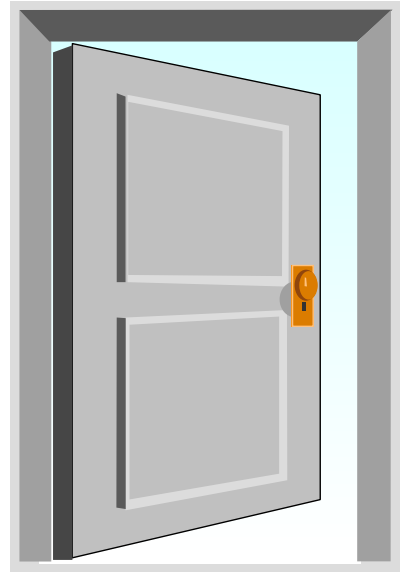
*Verschlüsselung/
Entschlüsselung*

WebSphere MQ Channel-Sicherheit



MCA-Sicherheitsexits

- Nach "Attach" des Empfängers
- Prüft "Vertrauen" in Empfänger
 - Echter MCA
 - Vertrauenswürdiger Manager
 - Gesicherte Codeebene
- Beispiel
 - Generieren von Zufallszahlen
 - Verschlüsseln und senden
 - Entschlüsseln und zurückgeben
 - Werte vergleichen
- Massnahmen
 - OK - weiter
 - Kanal unterdrücken
 - Benachrichtigung an geeignete Queue senden



Secure Sockets Layer (SSL)

- Protokoll zur gesicherten Übertragung von Daten über ein unsicheres Netzwerk
 - Verschlüsselung, Integrität, Autorisierung
 - Schutz der Verbindung
 - Client/Server
 - QM zu QM
- Zur Bekämpfung von Sicherheitsproblemen

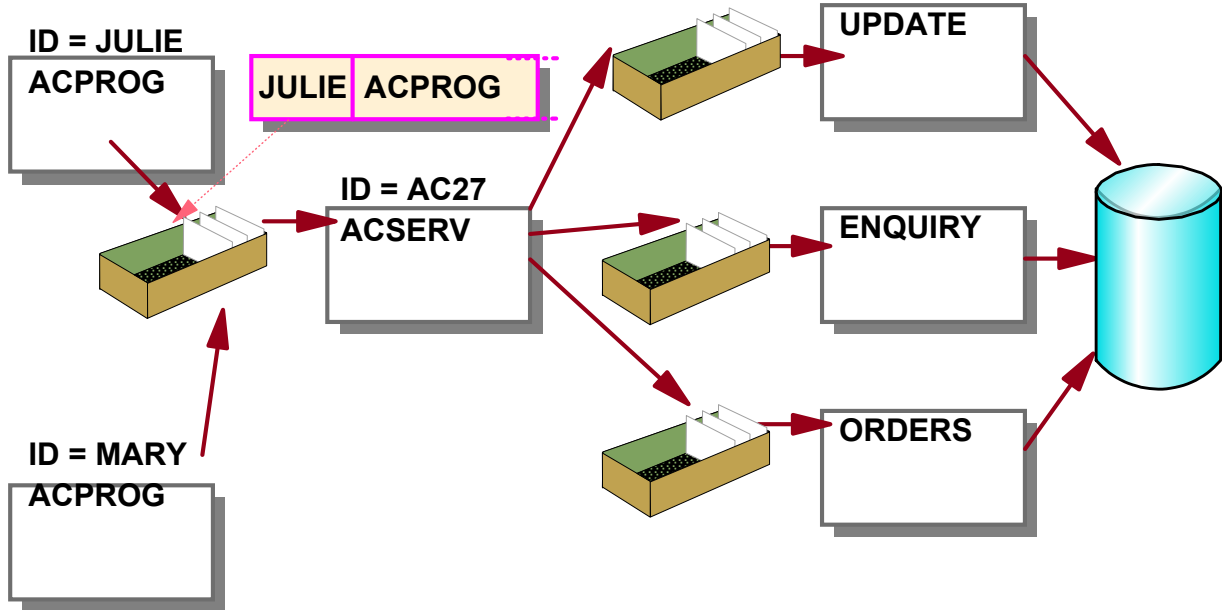
Management und Audit

- Managementmassnahmen
 - Zugriffskontroll-Listen einrichten und ändern
 - Sicherheitsprüfungen an/ausschalten
 - Erstellen / Überwachen von Benutzer-IDs und deren Zeitablauf
 - Passwortüberwachung
- Audit
 - Verstössnachrichten in Jobprotokoll
 - Überwachung der Queue über Security-Verstöße
 - Zugriffsliste

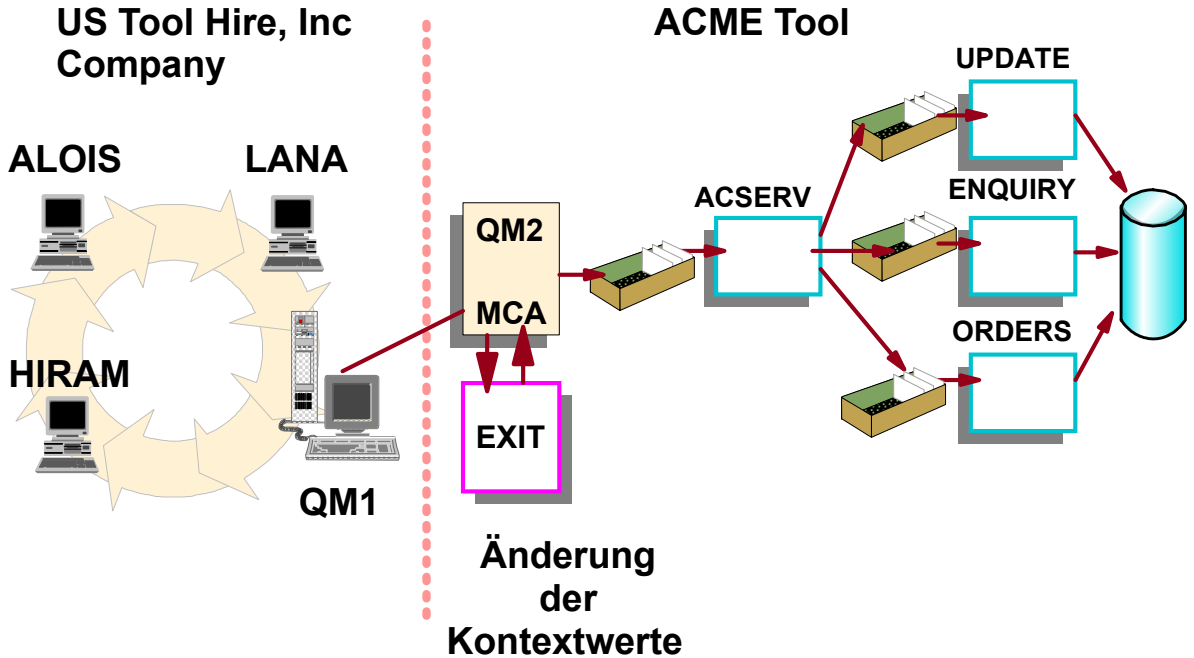


Beispiel - 1

ACME Tool Company



Beispiel - 2



Zusammenfassung

- WebSphere MQ verwendet die Funktionen für das Sicherheitsmanagement, die auf der Plattform verfügbar sind
- Zugriffskontrolle ist das wichtigste Anliegen der WebSphere MQ-Beteiligung
- Der WebSphere MQ-Administrator muss generell mit dem Sicherheitsadministrator zusammenarbeiten, um eine vorschriftsmässige Implementierung sicherzustellen