KONFIGURACJA KOMUNIKACJI MQ DLA INTERFEJSU KOMUNIKACYJNEGO A2A

SPIS TREŚCI

I Informacje podstawowe

Komunikacja elektroniczna z KDPW w ramach interfejsu komunikacyjnego A2A odbywa się w oparciu o połączenia MQ zestawiane z menadżerem kolejek MQ o nazwie A2A*env*, gdzie skrót *env* oznacza środowisko pracy: PRD – produkcyjne, TST – testowe. W ramach środowiska testowego warstwy komunikacyjnej MQ funkcjonować może kilka środowisk testowych dla poszczególnych usług.

II Konfiguracja menadżerów kolejek MQ

II.1. Atrybuty konfiguracyjne menadżerów kolejek A2A*env*

Niektóre atrybuty konfiguracyjne menadżerów kolejek A2A*env* odbiegają od domyślnych wartości przewidzianych przez IBM. Istotne z punktu widzenia komunikacji z podmiotami zewnętrznymi (zwanych dalej Uczestnikami) są następujące:

Atrybut QM	**Wartość domyślna**	**Wartość dla A2A*env***
CCSID	*zależna od platformy*	819
MAXMSGL	4 194 304	104 857 600
VERSION	*brak*	09020004

II.2. Parametry sieciowe menadżerów kolejek A2A*env*

Komunikacja z menadżerami kolejek MQ A2Aenv odbywa się w oparciu o protokoły TCP/IP. Parametry sieciowe tych menadżerów są następujące:

Środowisko usługi	Nazwa menadżera kolejek	Adres IP	Port TCP
PRD	A2APRD	195.136.21.56	1434
TSTA	A2ATST	195.136.21.57	1434
TSTB	A2ATST	195.136.21.57	1434

III Możliwe warianty połączeń MQ

Menadżer MQ A2A*env* pozwala na jednoczesną obsługę ruchu MQ dla różnych usług świadczonych przez KDPW. Jako standard wewnętrzny przyjęte zostało ustalenie, że z każdą dostępną dla Uczestnika usługą w każdym ze środowisk wiąże się oddzielny zestaw kanałów MQ. Umożliwia to większą elastyczność w dostosowaniu się KDPW do złożonej infrastruktury informatycznej Uczestnika.

Standard wewnętrzny KDPW przewiduje dwa typy dwukierunkowych połączeń MQ z podmiotami zewnętrznymi:

1) klient-serwer z użyciem jednego kanału typu server connection (SVRCN)

W takiej konfiguracji po stronie menadżera kolejek A2A*env* w KDPW zostaje zdefiniowany kanał MQ oraz dwie lokalne kolejki MQ: wejściowa (INP) przechowująca komunikaty od Uczestnika do KDPW oraz wyjściowa (OUT) przechowująca komunikaty od KDPW do Uczestnika. Po stronie Uczestnika zainstalowany jest klient MQ, który łączy się menażerem kolejek przy użyciu w/w kanału.

2) serwer-serwer z użyciem dwóch kanałów (SDR-RCVR)

W takiej konfiguracji zarówno po stronie KDPW jak i Uczestnika działa menadżer kolejek. Po stronie KDPW zostają zdefiniowane dwa kanały MQ: nadawczy (sender) oraz odbiorczy (receiver). Uczestnik zobowiązany jest do utworzenia analogicznych kanałów w ramach swojego menadżera kolejek. Po stronie KDPW utworzone zostają dwie kolejki MQ: lokalna wejściowa (INP) przechowująca komunikaty od Uczestnika do KDPW oraz zdalna wyjściowa (OUT) dla komunikatów od KDPW do Uczestnika. Uczestnik tworzy analogiczne kolejki MQ w ramach swojego menadżera, tj.: zdalną wyjściową (INP) dla komunikatów do KDPW oraz lokalną wejściową (OUT) przechowującą komunikaty z KDPW.

IV Uwierzytelnianie podłączającego się systemu

Jako podstawowy mechanizm uwierzytelniania drugiej strony w połączeniach MQ przyjęto protokół TLS z wykorzystaniem certyfikatów PKI wystawianych przez Urząd Certyfikacji KDPW. W obu środowiskach warstwy komunikacyjnej, tj. PRD i TST wystawiany jest jeden certyfikat na Uczestnika. Może on być wykorzystany do uwierzytelnienia systemu Uczestnika, tj. klienta MQ bądź menedżera kolejek MQ w momencie zestawiania połączenia z menadżerem kolejek A2A*env* dla dowolnej usługi, która została dla Uczestnika skonfigurowana.

V Konfiguracja kanałów MQ

V.1. Atrybuty konfiguracyjne kanałów MQ

Niektóre atrybuty konfiguracyjne kanałów MQ w menadżerze kolejek A2A*env* odbiegają od domyślnych wartości przewidzianych przez IBM. Istotne z punktu widzenia komunikacji z Uczestnikami są następujące:

Atrybut kanału MQ	**Wartość domyślna**	**Wartość dla kanału w A2A*env***
COMPMSG	NONE	ZLIBFAST
DISCINT	999999	6000
MAXMSGL	4 194 304	104 857 600
SSLCIPH		TLS_AES_256_GCM_SHA384
SSLPEER		*Powszechnie znana nazwa (common name) z pola podmiot certyfikatu drugiej strony połączenia*

W przypadku połączeń serwer-serwer wymaga się ustawienia analogicznych wartości w menedżerze kolejek Uczestnika. Przy takiej konfiguracji w celu włączenia weryfikacji nazwy menadżera kolejek KDPW należy określić poniższe atrybuty kanałów po stronie Uczestnika:

Środowisko	**Atrybut kanału MQ**	**Wartość dla kanału MQ Uczestnika**
PRD	SSLPEER	CN=A2APRD
TSTA	SSLPEER	CN=A2ATST
TSTB	SSLPEER	CN=A2ATST

V.2. Schemat nazw kanałów MQ

Wszystkie kanały w zakresie komunikacji MQ obsługiwanej przez menadżery kolejek A2A*env* muszą mieć nazwy zgodne z poniższym schematem.

srv.senv.code.con

gdzie:

srv - oznaczenie usługi

senv - nazwa środowiska usługi (możliwe wartości: PRD, TSTA, TSTB)

code - kod Uczestnika w ramach usługi

con - typ połączenia:

C – server-connection (*SVRCN) dla klient-serwer,

KU – KDPW-Uczestnik dla serwer-serwer, receiver (*RCVR) po stronie Uczestnika,

UK – Uczestnik-KDPW dla serwer-serwer, sender (*SDR) po stronie Uczestnika

VI Obsługa COA dla połączeń typu serwer-serwer

Niektóre usługi KDPW wykorzystują mechanizm raportów MQ typu Confirmation of Arrival (COA) do logowania informacji o dostarczeniu komunikatów MQ. W celu umożliwienia przesyłania tych potwierdzeń do menedżera kolejek A2A*env* należy skonfigurować menadżer kolejek po stronie Uczestnika w następujący sposób:

1) Jeśli kolejka transmisyjna do menadżera kolejek A2A*env* w KDPW ma nazwę inną niż nazwa tego menadżera (zależną od środowiska PRD/TSTA/TSTB) należy utworzyć alias dla tego menadżera w menadżerze kolejek Uczestnika.

Przykład dla menadżera kolejek A2ATST w KDPW:

DEFINE QREMOTE (A2ATST) RNAME(' ') RQMNAME(A2ATST)

XMITQ(nazwa_kolejki_transmisyjnej_do_A2ATST)

2) Należy przydzielić uprawnienia +put oraz +passid do tej kolejki transmisyjnej dla użytkownika o nazwie zdefiniowanej w polu MCAUSER w kanale typu *RCVR odpowiedzialnym za komunikację z KDPW w menadżerze kolejek Uczestnika.

VII Konfiguracja kolejek MQ

VII.1. Atrybuty konfiguracyjne kolejek MQ

Niektóre atrybuty konfiguracyjne kolejek MQ w menadżerze kolejek A2A*env* odbiegają od domyślnych wartości przewidzianych przez IBM. Istotne z punktu widzenia komunikacji z Uczestnikami są następujące:

Atrybut kolejki MQ	**Wartość domyślna**	**Wartość dla kanału w A2A*env***
DEFPSIST	NO	YES
MAXMSGL	4 194 304	104 857 600

W przypadku połączeń serwer-serwer wymaga się ustawienia analogicznych wartości w menedżerze kolejek Uczestnika.

VII.2. Schemat nazw kolejek MQ

Wszystkie kolejki komunikatów w zakresie komunikacji MQ obsługiwanej przez menadżery kolejek A2A*env* muszą mieć nazwy zgodne z poniższym schematem.

srv.env.code.direction

gdzie:
srv - oznaczenie usługi
senv - nazwa środowiska (możliwe wartości: PRD, TSTA, TSTB)
code - kod uczestnika RT (Sender ID)
direction - kierunek kolejki MQ (możliwe wartości: INP – komunikaty od Uczestnika do KDPW, OUT – komunikaty od KDPW do Uczestnika)

VIII Obowiązujące ustalone wartości pól nagłówka MQMD komunikatów MQ

W procesie tworzenia aplikacji obsługujących komunikację MQ z KDPW po stronie Uczestnika należy przyjąć następujące ustawienia:

CodedCharSetId = 1208

IX Informacje wymagane od Uczestnika przez KDPW

W celu skonfigurowania połączenia obsługującego komunikację MQ dla Uczestnika dla wybranej usługi w wybranym środowisku KDPW oczekuje od Uczestnika następujących informacji:

- wybrany wariant połączenia (klient-serwer lub serwer-serwer)
- dane kontaktowe do osoby odpowiedzialnej za konfigurację MQ po stronie Uczestnika
- sieć przez którą będzie realizowane połączenie (Intermet/Frame-Relay/MPLS)
- adresację IP Uczestnika do połączeń z A2Aenv
- dane kontaktowe do osoby odpowiedzialnej za konfigurację sieci po stronie Uczestnika
- w przypadku wybrania konfiguracji serwer-serwer dodatkowo:
  - nazwa menadżera kolejek po stronie Uczestnika
  - adres IP i port TCP procesu nasłuchującego tego menadżera. Jeżeli Uczestnik posiada zapasowy/e menadżer/y kolejek MQ należy również przesłać ich parametry.

Powyższe dane należy przesłać pocztą elektroniczną na adres di_serwis@kdpw.pl.

X Konfiguracja łącza telekomunikacyjnego

Uczestnicy mogą połączyć się do menadżera kolejek A2Aenv poprzez następujące sieci:

1) Internet
Transmisja musi być zabezpieczona technologią VPN (Lan to Lan) zgodnie z parametrami:
Protokół: IKE/IPSec (ESP)
Uwierzytelnienie: klucz pre-share
Algorytm szyfrowania: AES-256
Funkcja skrótu: SHA256 (SHA-1)

2) Frame-Relay

Obsługiwani operatorzy: Exatel, Orange
Transmisja musi być zabezpieczona technologią VPN zgodnie z parametrami:

- Protokół: IKE/IPSec (ESP)
- Uwierzytelnienie: klucz pre-share
- Algorytm szyfrowania: AES-256
- Funkcja skrótu: SHA256 (SHA-1)

3) MPLS
Obsługiwani operatorzy: Exatel, Orange
Kluczowe parametry MPLS:

- Sieć typu L3
- Routing BGPv4

Uwierzytelnienie: Protokół TLS z wykorzystaniem certyfikatów PKI, uruchomiony w obrębie menadżerów MQ.