RACFBroker/z

Entfernter Zugriff auf das
RACF Sicherheitssystem
auf IBM Mainframes
über TCP/IP

RACFBroker/z ist ein Produkt der

XPS Software GmbH
Eching

RACFBroker/z

XPS Software GmbH
Untere Hauptstr. 2
85386 Eching

Tel.: +49 (0)89-456989-0
Fax: +49 (0)89-456989-29
Web: http://www.xps-software.de
E-Mail: info@xps-software.de

Copyright

Warenzeichen

Einleitung

Dieses Dokument beschreibt die notwendigen Schritte zur Installation und Nutzung der Software RACFBroker/z, einem Produkt der XPS Software GmbH, Eching.

RACFBroker/z stellt Anwendungsprogrammen in heterogenen Netzwerken eine Schnittstelle zur Nutzung ausgewählter Funktionen der IBM Mainframe Sicherheitssysteme RACF (Resource Access Control Facility), ACF/2 und TopSecret zur Verfügung. RACFBroker/z basiert auf dem Produkt XPSDaemon von XPS.

Zur Nutzung der Schnittstelle wird neben RACFBroker/z noch die Java Bibliothek RACFBroker/J benötigt. RACFBroker/J basiert auf dem Produkt TRex von XPS und ist in Gegenstand einer eigenen Beschreibung.

Das nachfolgende Schaubild zeigt das konzeptuelle Zusammenspiel der beteiligten Komponenten:

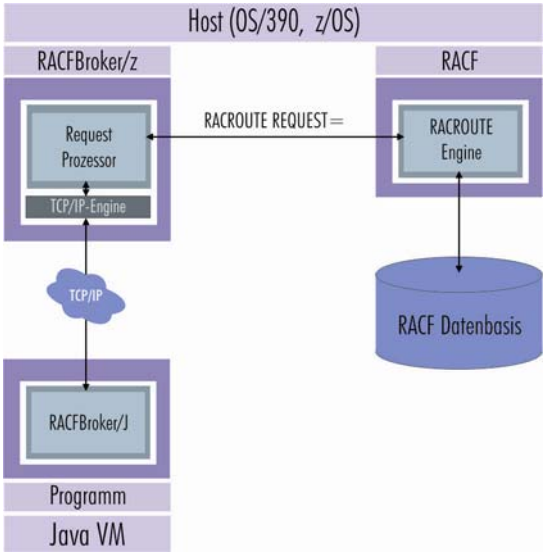

Abb. 1: RACFBroker-Konzept

Ein Java bzw. ein Win32 Programm stellt unter Verwendung des RACFBroker/J APIs eine RACF Anfrage an RACFBroker/z.

Dazu wird zwischen beiden Rechnern eine geschützte TCP/IP Verbindung aufgebaut. Pro Session wird ein symmetrischer Schlüssel erzeugt, der unter Verwendung eines RSA public/private Schlüsselpaares zwischen RACFBroker/z und RACFBroker/J ausgetauscht wird.

Der gesamte Datenaustausch wird dann unter Verwendung des symmetrischen Schlüssels wahlweise mit AES (Advanced Encryption Standard – Rijndael), Triple DES oder Blowfish verschlüsselt abgewickelt, um die Integrität der übertragenen Daten sicherzustellen.

RACFBroker/z leitet die Anfrage unter Verwendung der RACF Programmierschnittstelle RACROUTE an die entsprechende Engine weiter, die diese unter Zugriff auf die RACF Datenbasis ausführt.

Das Ergebnis der Ausführung der Anfrage wird dann von RACFBroker/z an RACFBroker/J zurückgemeldet und dem Anwendungsprogramm zur Auswertung zur Verfügung gestellt.

Inhalt des Installationspaketes

Das Installationspaket wird als komprimiertes Archiv 'RACFBrokerz.zip' ausgeliefert. Im dekomprimierten Archiv befinden sich dieses Dokument sowie das Unterverzeichnis 'MVS', das die benötigten Host-Programmdateien enthält.

Im Unterverzeichnis 'MVS' befinden sich die Dateien 'XPSD450L.BIN' und 'XPSD450M.BIN', die die RACFBroker/z Loadlib und die RACFBroker/z Maclib als XMIT-Dateien enthalten.

RACFBroker/z Installation unter OS/390 und z/OS

Die Installationsbibliotheken befinden sich im Unterverzeichnis 'MVS' des Installationspakets und sind mit Hilfe eines FTP-Clientprogramms zu dem Hostrechner zu übertragen, auf dem RACFBroker/z ausgeführt werden soll.

Die Bibliotheken werden im TSO-XMIT-Format ausgeliefert und sind binär zum Host zu übertragen. Vor der Übertragung sind die Dateien auf dem empfangenden Host anzulegen. Folgende Werte sollten dabei angegeben werden:

Name	Space	Lrecl	Blksz	Recfm
XMIT.XPSDAEM.V450.LOADLIB	400,(100)	80	3200	FB
XMIT.XPSDAEM.V450.MACLIB	100,(10)	80	3200	FB

Danach sind die TSO-XMIT-Dateien vom Client zum Host zu senden und folgendermaßen umzubenennen:

Clientname	Hostname
XPSD450L.BIN	XMIT.XPSDAEM.V450.LOADLIB
XPSD450M.BIN	XMIT.XPSDAEM.V450.MACLIB

Anschließend sind die Dateien durch folgende TSO-Befehle zu übertragen:

Für die Loadlib:

```
RECEIVE INDSN(XMIT.XPSDAEM.V450.LOADLIB)
```

Nach Eingabe des 'RECEIVE'-Befehls erscheint folgender Prompt:

```
INMR901I Dataset XPSDAEM.V450.LOADLIB from ??????? on NODENAME
INMR906A Enter restore parameters or 'DELETE' or 'END' +
```

Hier ist der gewünschte Dateiname folgendermaßen anzugeben:

```
DSN(xpsdaem.V450.loadlib)
```

Da das RACROUTE Makro nur von privilegierten Anwendungen ausgeführt werden darf, ist die RACFBroker/z Loadlib mit APF-Autorisierung auszustatten.

Für die Maclib:

```
RECEIVE INDSN(XMIT.XPSDAEM.V450.MACLIB)
```

Nach Eingabe des 'RECEIVE'-Befehls erscheint folgender Prompt:

```
INMR901I Dataset XPSDAEM.V450.MACLIB from ??????? on NODENAME
INMR906A Enter restore parameters or 'DELETE' or 'END' +
```

Hier ist der gewünschte Dateiname folgendermaßen anzugeben:

```
DSN(xpsdaem.V450.maclib)
```

Starten von RACFBroker/z

Mit dem nachfolgenden Jobstream wird RACFBroker/z gestartet. Ein Muster für den Startjob ist unter dem Namen 'XPSSTART' in der RACFBroker/z Maclib vorhanden.

Beispieljob:

```
//XPSRACFB JOB ,'RACFBROKER START',CLASS=A,MSGCLASS=X
//XPSRACFB EXEC PGM=XPSDAEM,REGION=20M,TIME=1440,                    X
//PARM='MODE=RACF,TCPN=TCPIP1A,PORT=8880,SFEX=XPSSAFEX,ENCR=3DES,RSET=CX
               HECK'
//STEPLIB  DD DISP=SHR,DSN=XPSDAEM.V450R.LOADLIB
//XPSDATA  DD DISP=SHR,DSN=XPSDAEM.V450R.MACLIB
//SYSPRINT DD SYSOUT=*
//SYSUDUMP DD SYSOUT=*
//SNAPDMP  DD SYSOUT=*
//LOG      DD SYSOUT=*
```

Abb. 2: Startup-Job MVS

Nachdem RACFBroker/z erfolgreich gestartet wurde, steht die Funktionalität sofort zur Verfügung. Die Nutzung bedarf keiner weiteren zusätzlichen Konfiguration.

Beschreibung der Parameter des RACFBroker/z Startjobs:

MODE= Unter Verwendung dieses Parameters wird das RACFBroker/z Trägersystem XPSDaemon über den gewünschten Verarbeitungsmodus informiert. Zulässige Verarbeitungsmodi werden anhand der installierten Lizenzdatei geprüft. Zum Betrieb von RACFBroker/z ist die Angabe 'MODE=RACF' zwingend erforderlich.

TCPN= Mit diesem Parameter ist RACFBroker/z über den Namen der TCP/IP Started Task in Kenntnis zu setzen.

PORT= Damit RACFBroker/z Anfragen bearbeiten kann, müssen diese von RACFBroker/J über TCP/IP an RACFBroker/z übermittelt werden. Mit Hilfe dieses Parameters ist festzulegen, welchen TCP/IP Port RACFBroker/z zu diesem Zweck überwachen soll. Bei der Wahl der Portnummer ist darauf zu achten, dass keine Konflikte mit Portnummern entstehen, die bereits von anderen Applikation auf eingehende Anfragen überwacht werden.

SFEX= Hier ist der Name eines Exit-Programmes anzugeben, dem RACFBroker/z bei Erreichen bestimmter Punkte im Rahmen der Verarbeitung einer Anfrage die

Kontrolle übergeben soll. Das Exit-Programm wird durch Übergabe einer Parameterliste über den aktuellen Stand der Verarbeitung informiert und kann bei Bedarf Einfluss auf die weitere Verarbeitung der Anfrage nehmen.

ENCR= Der Datenaustausch zwischen RACFBroker/z und RACFBroker/J erfolgt verschlüsselt. Dazu tauschen die beiden Kommunikationspartner im Rahmen des Verbindungsaufbaus einen eigens für jede Session generierten symmetrischen Key unter Verwendung des RSA public/private Key Verfahrens aus. Unter Verwendung dieses Parameters kann festgelegt werden, welches symmetrische Verschlüsselungsverfahren zum Einsatz kommen soll. Die nachfolgende Tabelle enthält die zulässigen Werte:

ENCR=	Schlüssellänge	Bedeutung
AES	256 Bit	Zur Verschlüsselung wird der Advanced Encrpytion Algorithm Rijndael verwendet.
3DES	168 Bit	Die Verschlüsselung erfolgt unter Einsatz von TripleDES.
BLOWFISH	128 Bit	Die übertragenen Daten werden mit Hilfe des Blowfish Algorithmus verschlüsselt.

RSET= Dem Ausführen der RACFBroker Funktion "Passwort zurücksetzen" sollte besondere Aufmerksamkeit gewidmet werden.
Das Zurücksetzen eines Benutzerpassworts erfolgt ohne Kenntnis des aktuell gültigen Passwortes. Aus diesem Grund wird der Aufruf dieser Funktion standardmäßig nur solchen Anwendern erlaubt, die über das RACF Attribut 'Special' verfügen. Name und Passwort eines autorisierten Benutzers sind bei Aufruf dieser Funktion unter Verwendung der RACFBroker/j Programmierschnittstelle zu übergeben.
Die Standardeinstellung, die auch aktiv wird, wenn dieser Parameter nicht angegeben wird, lautet 'RSET=CHECK'.
Falls auf diese Einschränkung verzichtet werden soll, was zum Beispiel beim Einsatz im Rahmen einer Serverapplikation der Fall sein kann, bei der der ausführende Benutzer durch andere Kriterien eindeutig identifiziert wird, ist dies durch die Angabe von 'RSET=NOCHECK' bekannt zu geben.