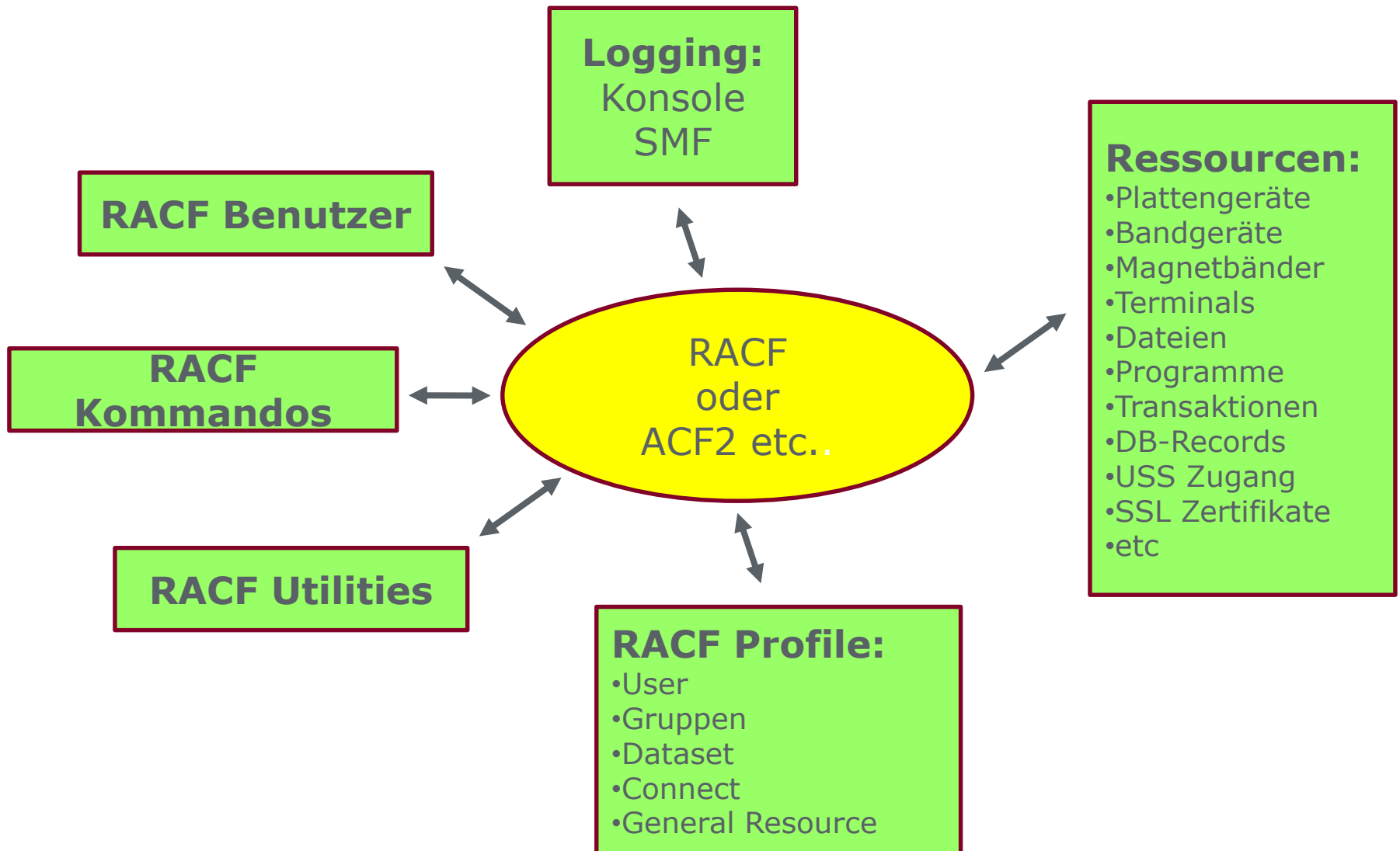




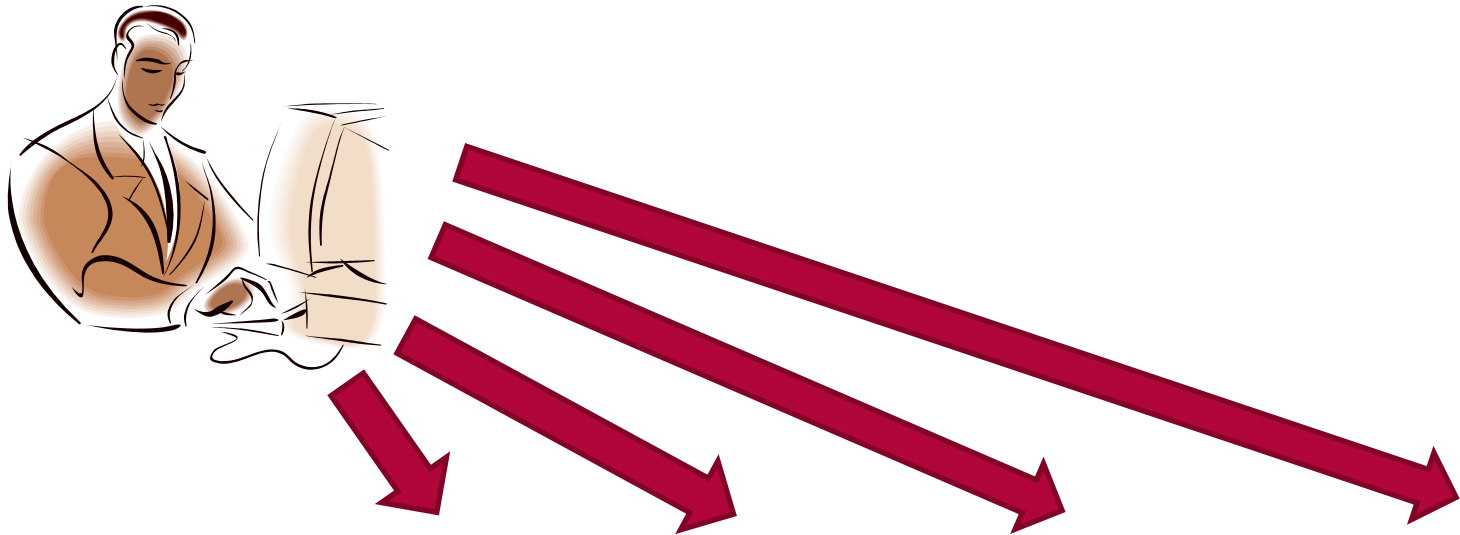
openHPI Resource Access Control Facility (RACF)

Wolfram Greis
European Mainframe Academy
Stein am Rhein (CH)



■ Profilarten:

- Benutzerprofile (User Profiles)
- Gruppenprofile (Group Profiles)
- Dateiprofile (Dataset Profiles)
- Allgemeine Ressourcenprofile (General Resource Profiles)
- Connectprofile (Verbindungen zu RACF Gruppen)



Funktion	User	Group	Dataset	General Resource
DEFINE	ADDUSER	ADDGROUP	ADDSD	RDEFINE
ALTER	ALTUSER	ALTGROUP	ALTDSD	RALTER
LIST	LISTUSER	LISTGROUP	LISTDSD	RLIST
DELETE	DELUSER	DELGROUP	DELDSD	RDELETE

```
----- TSO/E LOGON -----  
  
Enter LOGON parameters below:  
  
Userid      ==> UWGR  
  
Password    ==>  
  
Procedure   ==> BASICD  
  
Acct Nmbr   ==> 3300  
  
Size        ==> 6000  
  
Perform     ==>  
  
Command     ==>  
  
Enter an 'S' before each option desired below:  
          -Nomail          -Nonotice      S -Reconnect          -OIDcard  
  
PF1/PF13 ==> Help    PF3/PF15 ==> Logoff    PA1 ==> Attention    PA2 ==> Reshow  
You may request specific help information by entering a '?' in any entry field
```

- Damit die RACF-Funktionen wirksam werden:
 - ... müssen alle Benutzer und Ressourcen im RACF definiert werden
 - ... muss festgelegt werden, wie die Benutzer die Ressourcen benützen dürfen

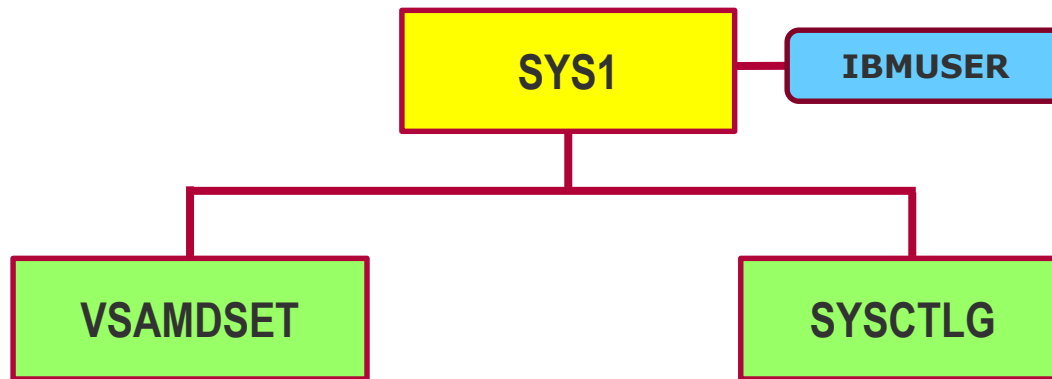
Nur was im Security Server (RACF) definiert ist, ist auch geschützt!!!

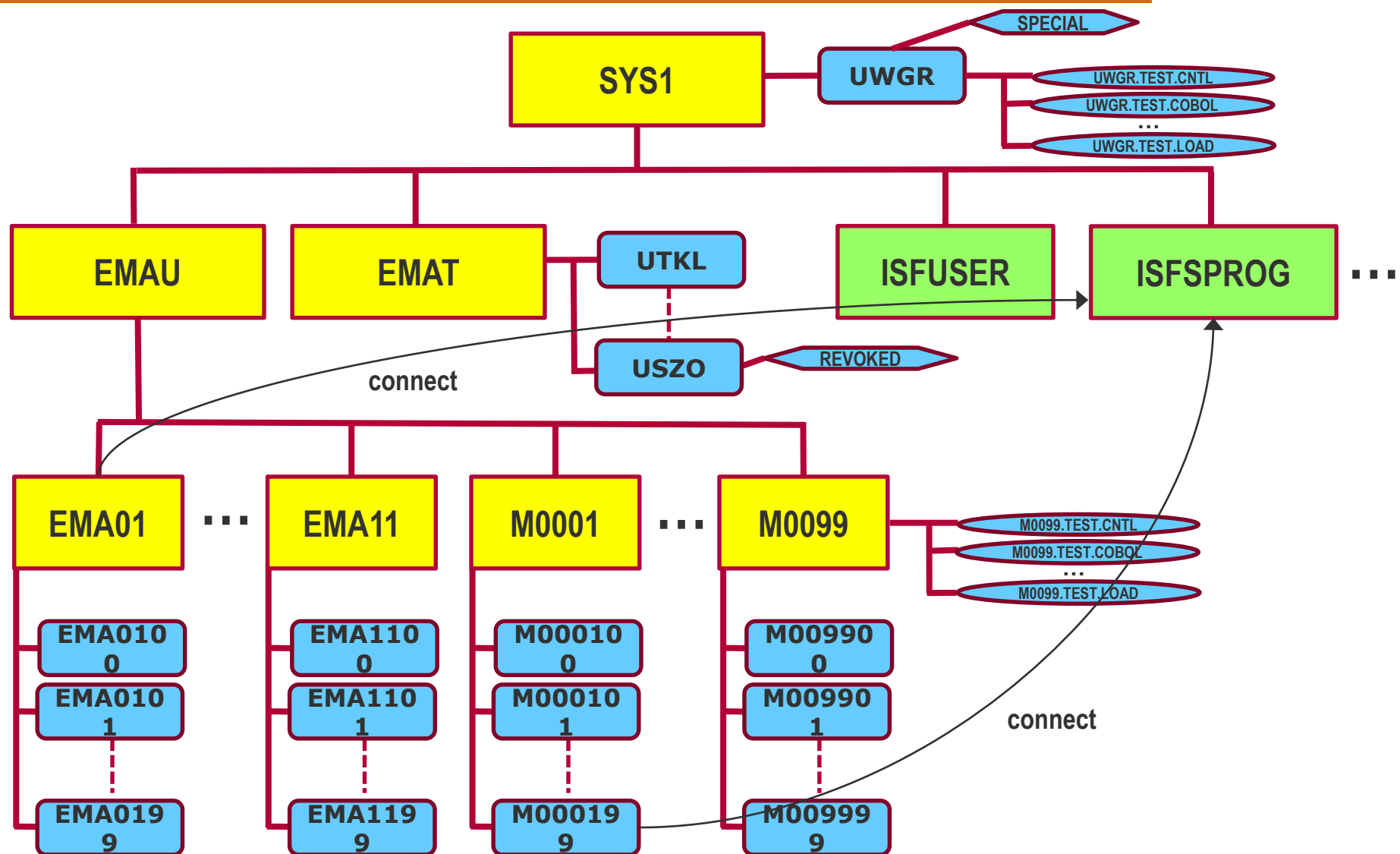
- Die Ressourcen werden im RACF in Klassen zusammengefasst.
- Um Ressourcen schützen zu können, muss die jeweils zugehörige Klasse im RACF aktiv sein

Zwei Arten von Ressourcen werden unterschieden:

- Standardressourcen (USER, GROUP, DATASET)
- Allgemeine Ressourcen (DASDVOL, TAPEVOL, PROGRAM, JESJOBS, TERMINAL ...)

Ausgehend von dieser RACF-Struktur nach der Installation kann die Benutzerstruktur (d.h. Gruppen-, User-, Dateiprofile sowie General Ressource Profile) in Abhängigkeit von der Organisationsstruktur und den eigenen Konventionen mittels RACF-Befehlen definiert werden.





■ Diskrete Profile

- jede Ressource (z.B. jede Datei) wird einzeln im RACF definiert, d.h. es existiert für jede Datei ein Eintrag (Profile) in der RACF-Datenbank.
- Zusätzlich ist als Kennzeichen des RACF-Schutzes für jede Datei im VTOC der Platte ein bestimmtes Bit gesetzt (im DSCB1 auf der Distanz X'5D').

■ Generische Profile

- mehrere Ressourcen werden in einem Profil-Eintrag zusammengefaßt.
- Voraussetzung dafür ist, dass diese Ressourcen die gleichen Zugriffsberechtigungen aufweisen.

Empfehlung: Ausschliesslich generischen Profilen nutzen!

- EMA.**
- EMA.SOURCE.*
- EMA.RACF%.*
- EMA.RACF.CNTL
- EMA.RACF*.**
- EMA.*.ASM

Wird eine Datei angelegt, deren erster Qualifier im Dateinamen EMA ist, bekommt die Datei die Zugriffsberechtigungen des Generic Profiles zugewiesen, dessen Namen dem Dateinamen am weitestgehenden entspricht (*Most specific Profile*).

- **NONE** Kein Zugriff erlaubt
 - **EXECUTE** Erlaubnis zur Ausführung (nicht lesen!)
 - **READ** Leseerlaubnis
 - **UPDATE** Schreiben/Verändern erlaubt
 - **CONTROL** Speziell für VSAM
 - **ALTER** Komplette Kontrolle incl. Schutzänderung
-
- **Anmerkung:** Ausser mit EXECUTE kann mit allen anderen Berechtigungen eine Datei gelesen und damit kopiert werden.
Nach dem Kopieren besteht volle Kontrolle über die Datei!

Mit UACC (Universal Access) wird die Default-Berechtigung vergeben!

- RACF Homepage im Internet
<http://www.ibm.com/servers/eserver/zseries/zos/racf/>
- Enterprise Security und RACF
<http://www.ibm.com/systems/z/advantages/security/>
- RACF Manuals im Internet
<http://www.ibm.com/systems/z/os/zos/bkserv/>
- RACF Redbooks
<http://www.redbooks.ibm.com>

Security

Overview Integrity Solutions Resources

Highly distributed computing, extensive online collaboration, explosive data growth and regulatory requirements have combined to make information security more critical and more complex than ever for organizations today. Security threats have intensified and become increasingly complex to manage.

Many organizations are discovering the advantages of making System z the enterprise security hub. Resilience and security have long been hallmarks of mainframe computing. Making System z the enterprise security hub also enables organizations to take advantage of mainframe extensibility and scalability to consolidate disparate systems to improve efficiencies, standardize operations (especially after mergers or acquisitions) and streamline security management across all computing resources.

With greater than 45 years of integration between hardware and software, IBM System z servers and security software are designed to provide a secure infrastructure. This includes protecting sensitive business critical data, sharing information internally as well as externally, providing enhanced encryption and key infrastructure capabilities, protecting user privacy, providing an extensive audit trail with compliance reporting, reducing fraudulent activities, allowing centralized administration, securing virtualization, and protecting information traveling across the network while maintaining high levels of infrastructure, application and data availability.

With the Common Criteria Evaluation Assurance Level 5 (EAL5) awarded by International Standards Organization, System z has the highest security rating or classification for any commercially available server. The EAL5 rating can provide customers the assurance and confidence that they can run many different applications containing confidential data on one System z which is divided into partitions that keep each application's data secure and distinct from the others. This isolation allows images supporting different operating systems to run in different partitions on a single mainframe.

Many of world's top banks and retailers rely on the mainframe to help secure sensitive business transactions. The best way to secure information is to encrypt it. System z provides exceptional performance and function via cryptographic coprocessors and accelerators that are individually specialized to address various encryption needs.

Resource Access Control Facility

Overview What's New z/VM Resources

Securing Valuable Corporate Data

In 1976, IBM® set the standard for security products when RACF® was introduced!

From the beginning, the RACF Development Team has proudly brought you RACF, the premier product for securing your most valuable corporate data. Working closely with your operating system's existing features, IBM's award-winning Resource Access Control Facility (RACF) licensed program provides improved security for an installation's data. RACF protects your vital system resources and controls what users can do on the operating system.

You decide which resources you want to protect and which users need access to them. RACF provides the functions that let you:

- identify and verify system users
- identify, classify, and protect system resources
- authorize the users who need access to the resources you've protected
- control the means of access to these resources
- log and report unauthorized attempts at gaining access to the system and to the protected resources
- administer security to meet your installation's security goals.

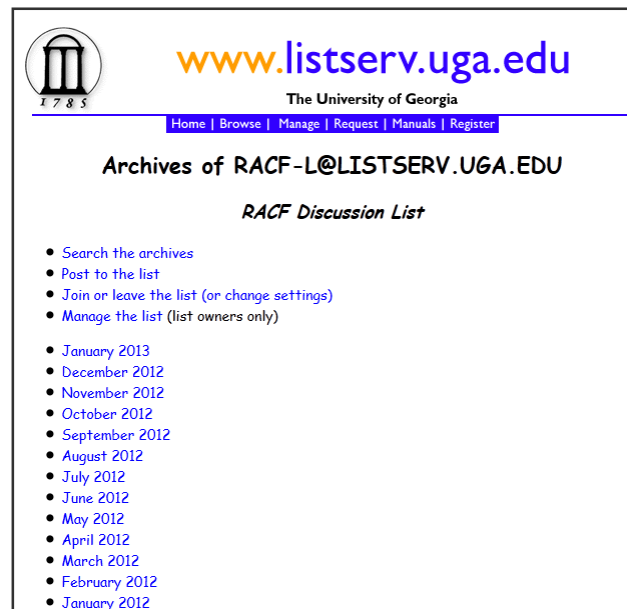
An introduction to RACF can be found in the z/OS Security Server Introduction, which is available in PDF format. Click [here](#) for information about downloading and browsing PDF files.

AT-TLS and CS IPsec can lighten the load for security administrators (357KB)
[Get Adobe® Reader®](#)

IBM Internet Library Terms and Conditions

Please [read and accept](#) IBM's terms and conditions before using the z/OS IBM Internet Library.

- Listserver bzgl. RACF
an der University of Georgia:
<http://listserv.uga.edu/archives/racf-l.html>



Fragen / Diskussionen
gerne im Forum zu diesem MOOC