

z/OS LDAP – ein zentraler Security Service



**Mit
IBM System z
in die
Zukunft**



Empalis z/OS-Tag 2008
IBM Forum Stuttgart, 2008-07-09
Oliver Paukstadt, Millenux GmbH
Christian Tatz, Empalis GmbH

Agenda

- LDAP Theorie & Grundlagen
- Anbindung eines Linux/Unix Systems
- Anbindung einer Applikation (am Beispiel squid)
- RACF native Authentication

- ICTX Backend
- z/OS Identity Cache
- Remote Authorization und Auditing

Firmenübersicht

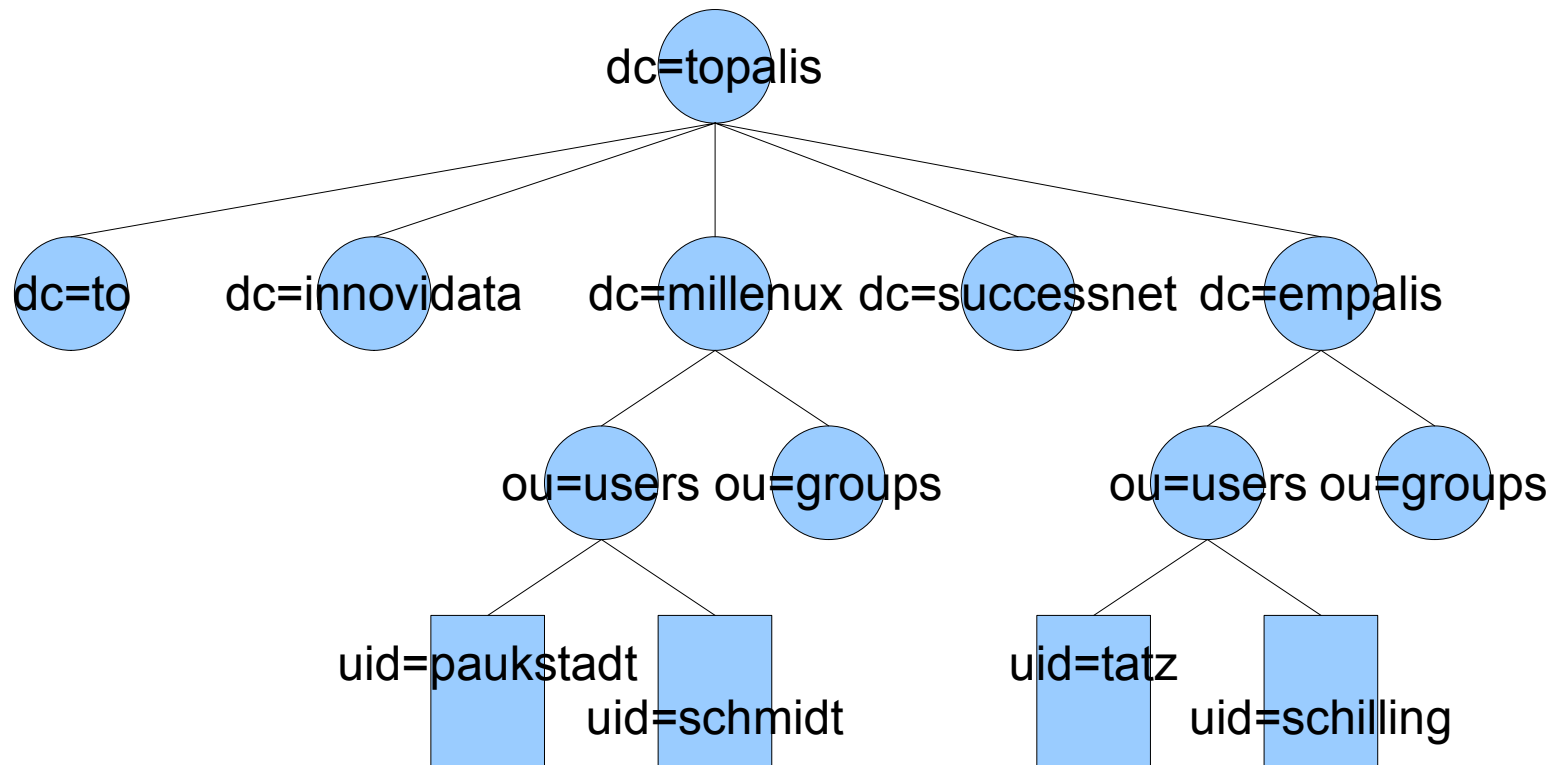


 <p>THINKING OBJECTS SOFTWARE COACH</p>	 <p>InnoviData</p>	 <p>MI ENUX</p>	 <p>successnet.ag interactive business solutions</p>	 <p>Empalis</p>
Rechenzentrumsbetrieb Systemintegration Systems Management IT-Security Hosting Virtualisierung Datenbank-administration Datensicherung	Software-entwicklung Applikations-integration SAP-Anbindung Reportingsysteme Open-Source-Frameworks System-programmierung OpenOffice-Integration Datenmodelle	Open-Source-Consulting Linux-Migration Linux auf Mainframes Workgroup-Lösungen Linux Terminalserver Thin Client Computing	Web-Lösungen mit Content-Management-Systemen Web-Lösungen auf Open-Source-Basis Interface- und Flash-Design Online-Redaktion Prüfung auf Usability und Corporate Design	Storage Management mit TSM System-programmierung Mainframe Lotus Domino Notes und Web-sphere Infra-strukturen Systemsmanagement und Security mit Tivoli

LDAP – Was ist das?

- **Lightweight Directory Access Protocol**
 - Verzeichnisdienst
 - DAP (X.500)
- **Hierarchische Struktur**
 - Baumartige Struktur
- **Spezialisierte Datenbank**
 - Sehr viele lesende Zugriffe
 - Relativ wenig schreibende Zugriffe

Beispiel LDAP Struktur



Beispiel für ein LDAP-Objekt

```
dn: cn=Oliver Paukstadt,ou=users,dc=millenux,dc=topalis
objectclass: inetorgperson
objectclass: posixaccount
objectclass: shadowAccount
objectclass: ibm-nativeauthentication
objectclass: ibm-auxaccount
cn: Oliver Paukstadt
surname: Paukstadt
gecos: Oliver Paukstadt
givenName: Oliver
uid: paukstadt
uidnumber: 8888
gidnumber: 8888
homedirectory: /home/paukstadt
loginshell: /bin/bash
ibm-nativeid: UI13467
host: server-001.topalis
host: virtual-087.topalis
....
```

Definition der Objekte

- Jedes Objekt gehört zu mindestens einer Objektklasse (Objectclass)
 - PosixAccount
 - uidNumber, gidNumber, loginShell, ...
 - InetOrgPerson
 - Mail, mobile, ...
- Definierte Objektklassen für die Abbildung einer Unix-Umgebung
 - RFC 2307
- Objektklassen enthalten verpflichtende und freiwillige Attribute
- Es besteht die Möglichkeit, eigene Objektklassen zu definieren

Eindeutiger Objektname

- Durch den Pfad in der Baumstruktur ergibt sich ein eindeutiger Name des Objektes
 - Distinguished Name (DN)
 - dn: cn=Oliver Paukstadt, ou=users, dc=millenux, dc=topalis
 - dn: cn=Christian Tatz, ou=users, dc=empalis, dc=topalis

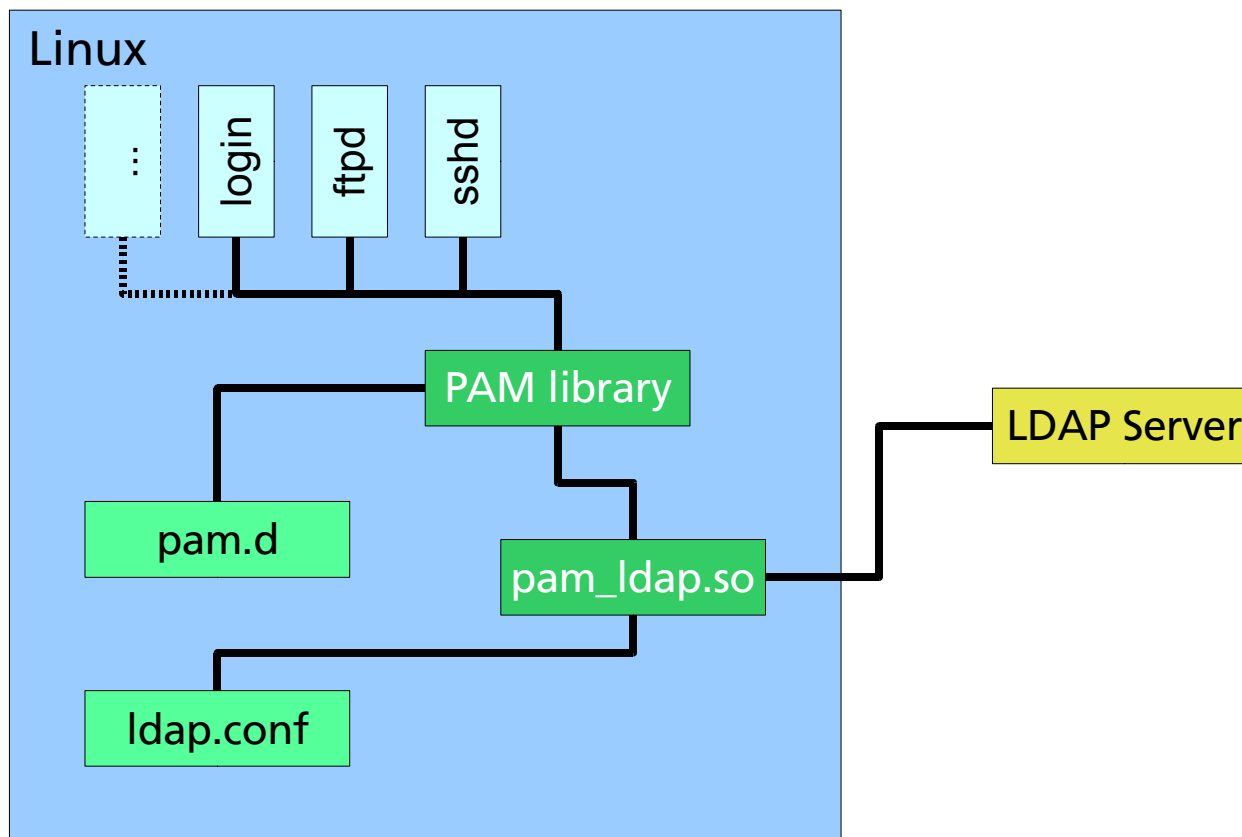
Zugriffsberechtigungen

- Die Zugriffsberechtigungen auf die Attribute der Objekte können pro Attribut granular vergeben werden
 - Password darf (auch für den Benutzer selbst) nicht lesbar sein
 - Mail-Attribut muss beispielsweise vom Mail-Server lesbar sein
 - UidNumber muss vom Betriebssystem lesbar sein
- **Anonymer Zugriff ist möglich**
- **Zugriff mit Authentifizierung (bind)**
 - Systeme dürfen nicht das Passwort-Attribut auslesen oder vergleichen sondern müssen sich anmelden

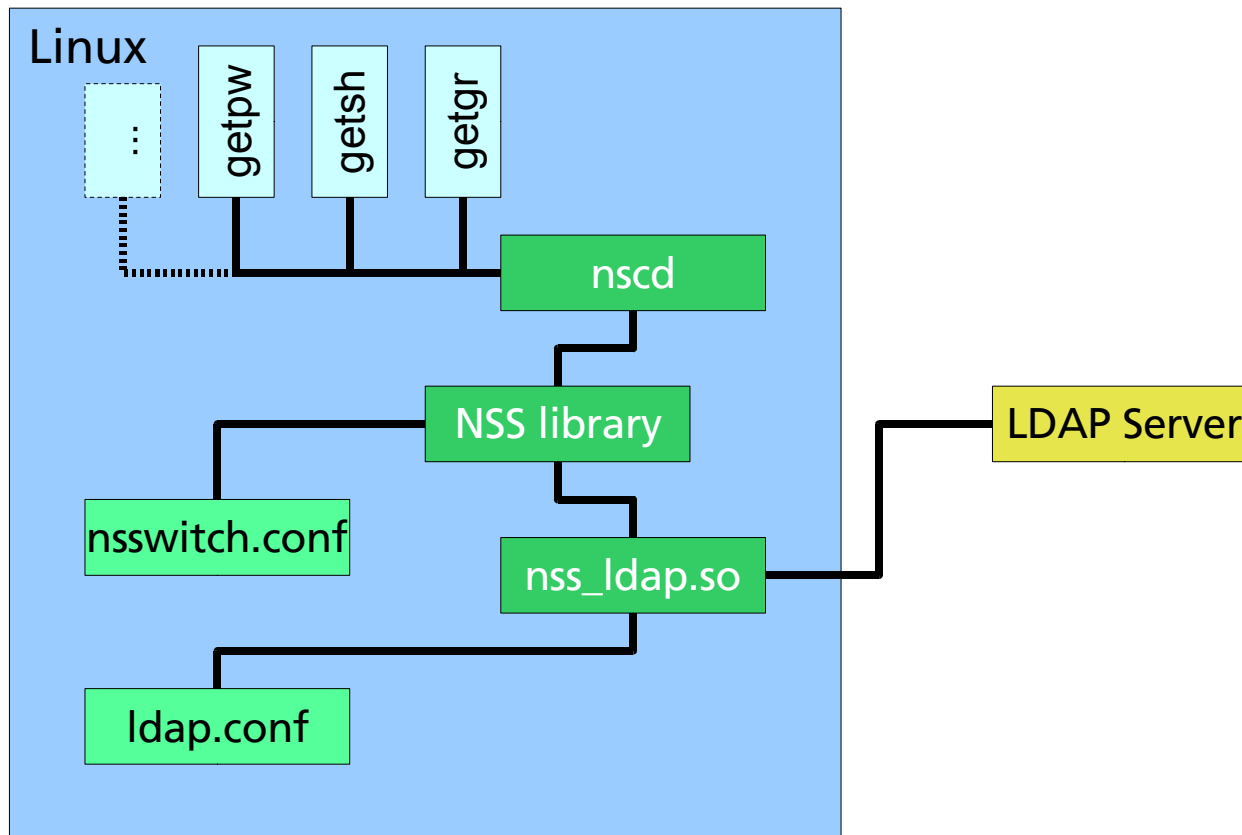
Anbindung eines Linux-Systems

- **Authentifizierung am System**
 - Benutzer gibt Login und Passwort ein
 - Anonyme Suche im LDAP zu welchem DN der Login gehört
 - Eventuell in Kombination mit weiteren Attributen oder Einschränkungen auf Teilbäume
 - Anmeldung am LDAP mit diesem DN und dem Passwort
- **Anzeigen von Benutzer-IDs**
 - Mapping der numerischen Benutzer-IDs in Klartext bei den üblichen System-Kommandos: ls, ps,
- **Gilt für die meisten aktuellen Unix-Systeme ebenso**

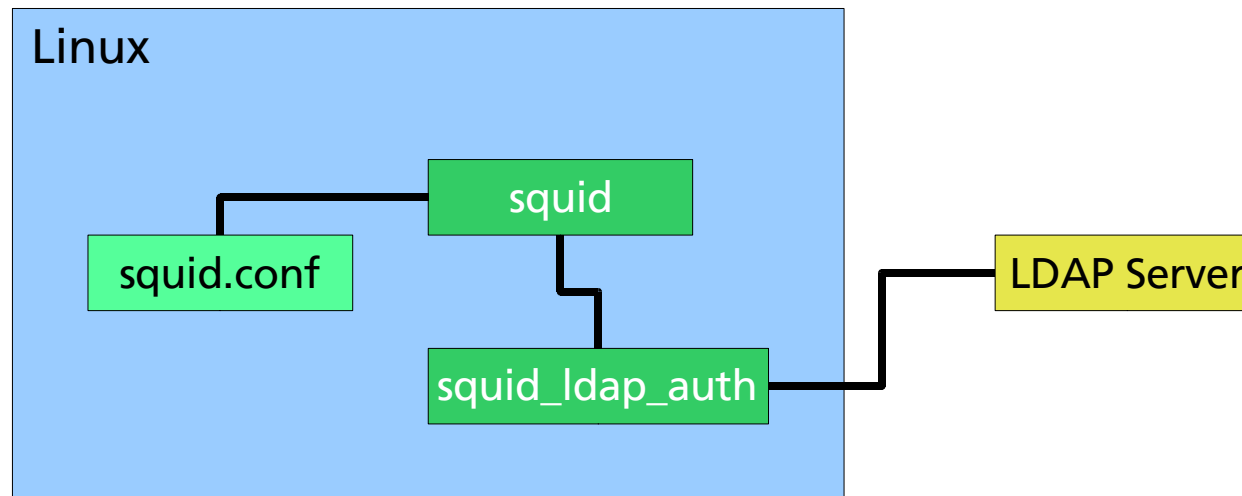
Pluggable Authentication Modules mit LDAP



Name Switch Service mit LDAP



Anbindung einer Applikation (squid Webproxy)

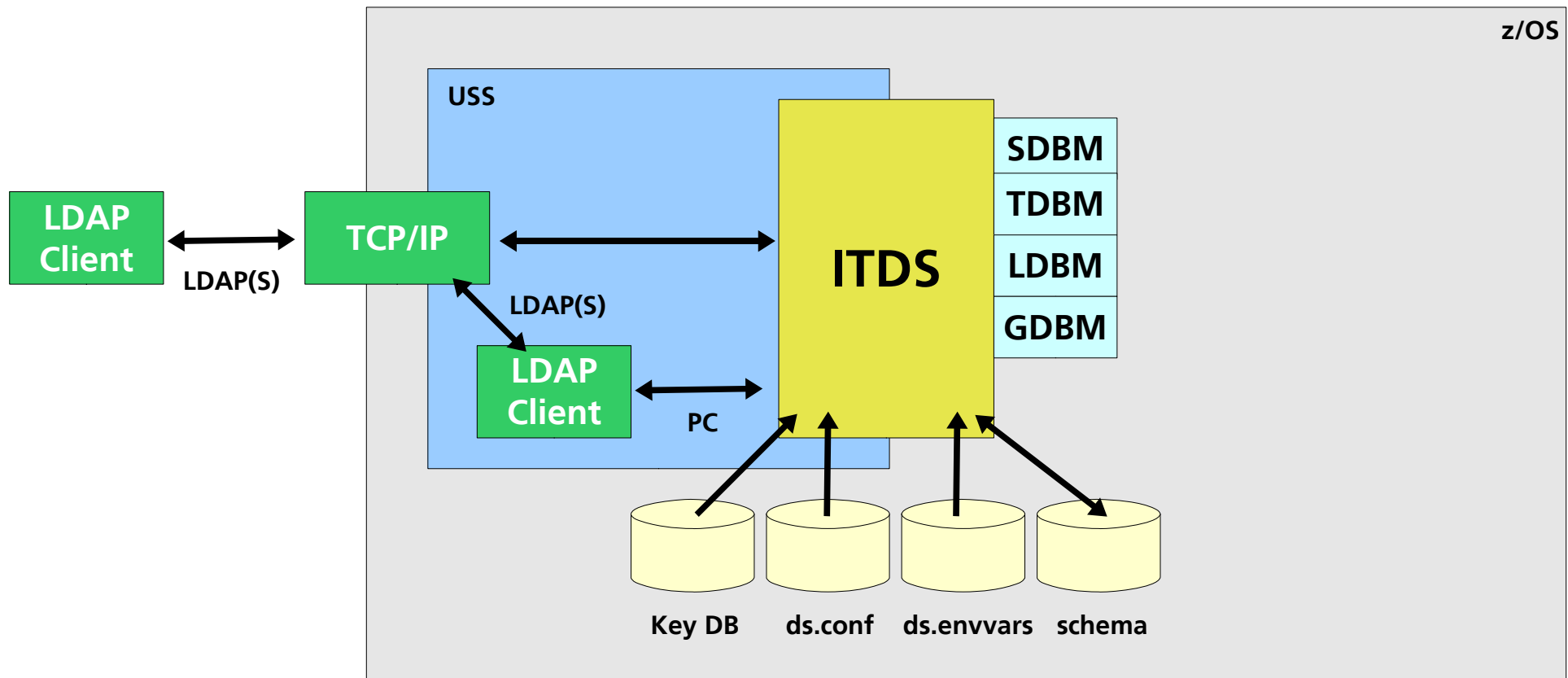


```
auth_param basic program /usr/lib/squid_ldap_auth -b"dc=topalis" -f"uid=%s" -h ldap.topalis
acl ldapauth proxy_auth REQUIRED
http_access allow ldapauth
http_access deny all
```

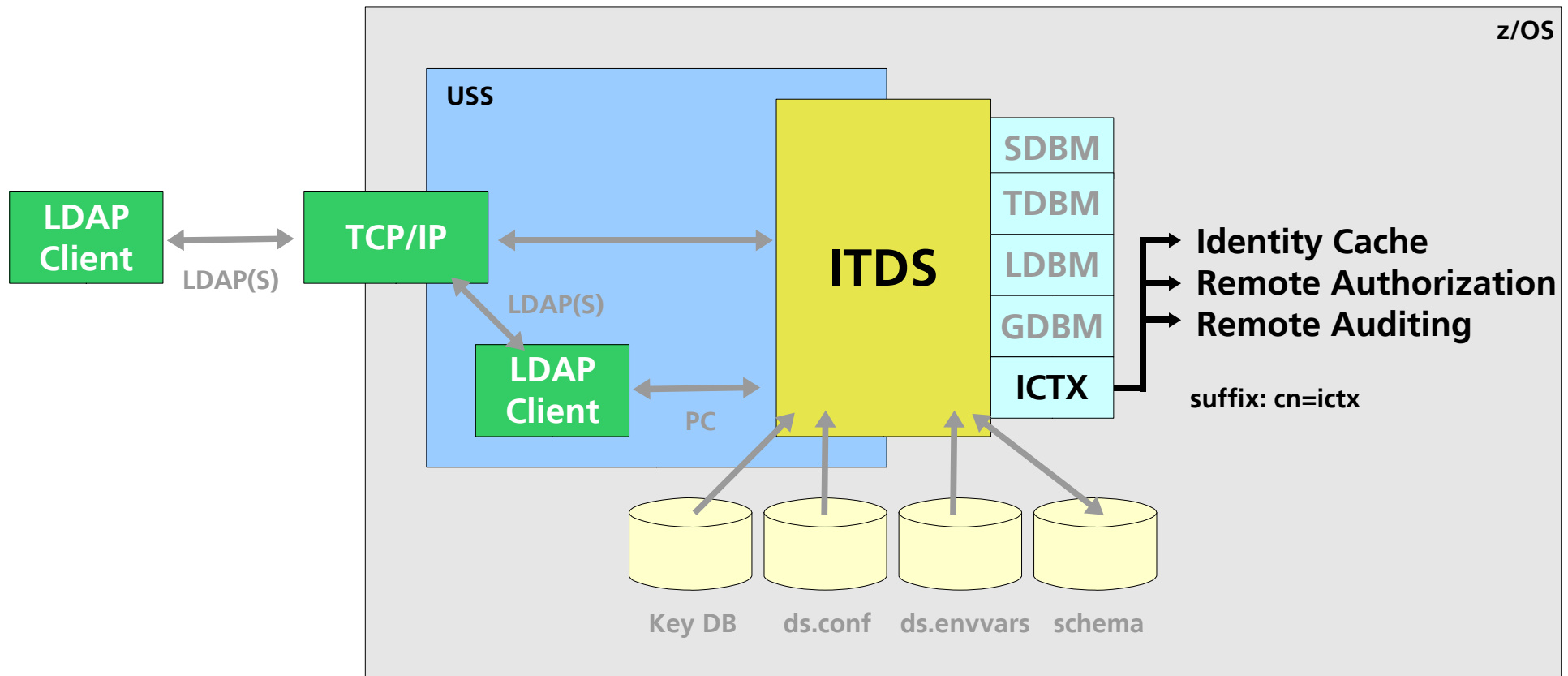
RACF Native Authentication

- Einschalten im LDAP Server
 - `nativeUpdateAllowed`
 - `useNativeAuth`
 - `nativeAuthSubtree`
- Definieren des Mappings der UserID
 - `ObjectClass: ibm-nativeAuthentication`
 - `ibm-nativeID: <racf-id>`

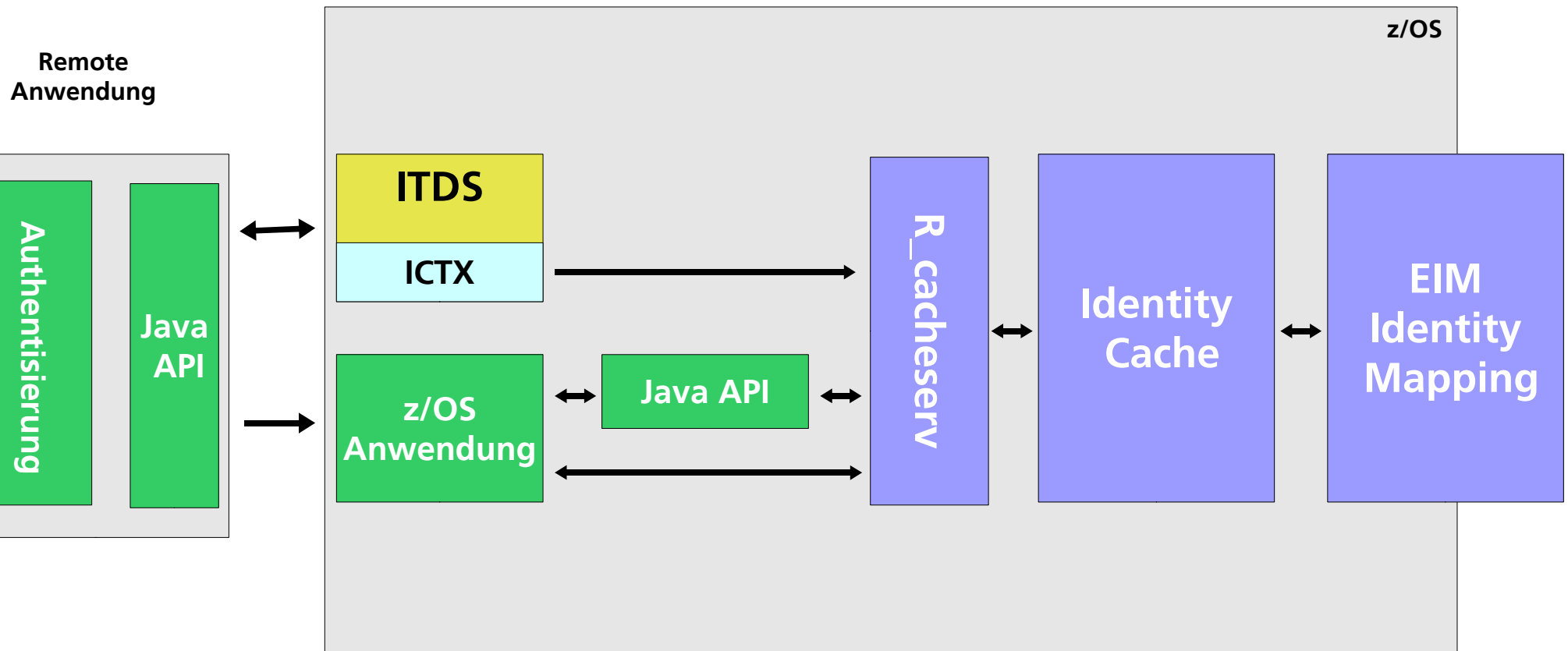
IBM Tivoli Directory Server for z/OS - ITDS



ITDS – z/OS EIM ICTX Backend

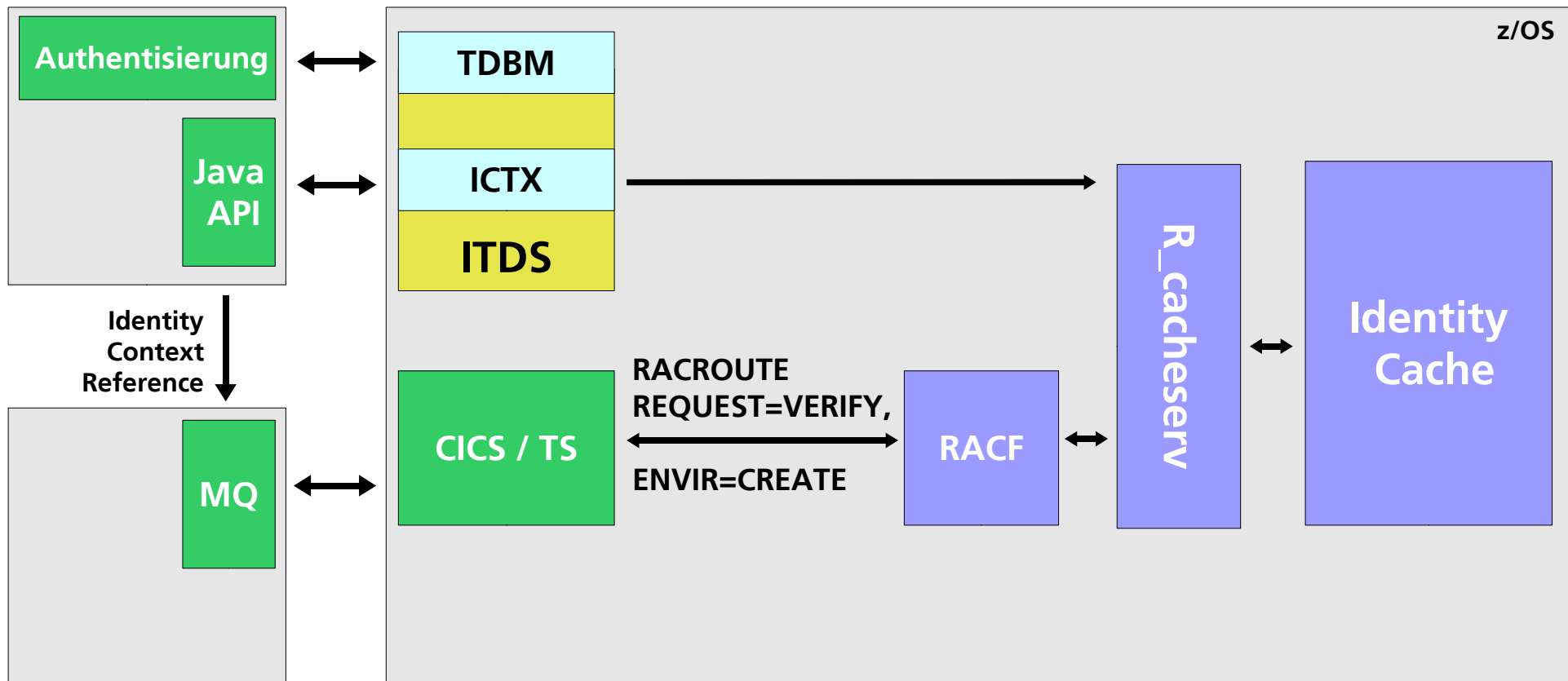


z/OS Identity Cache



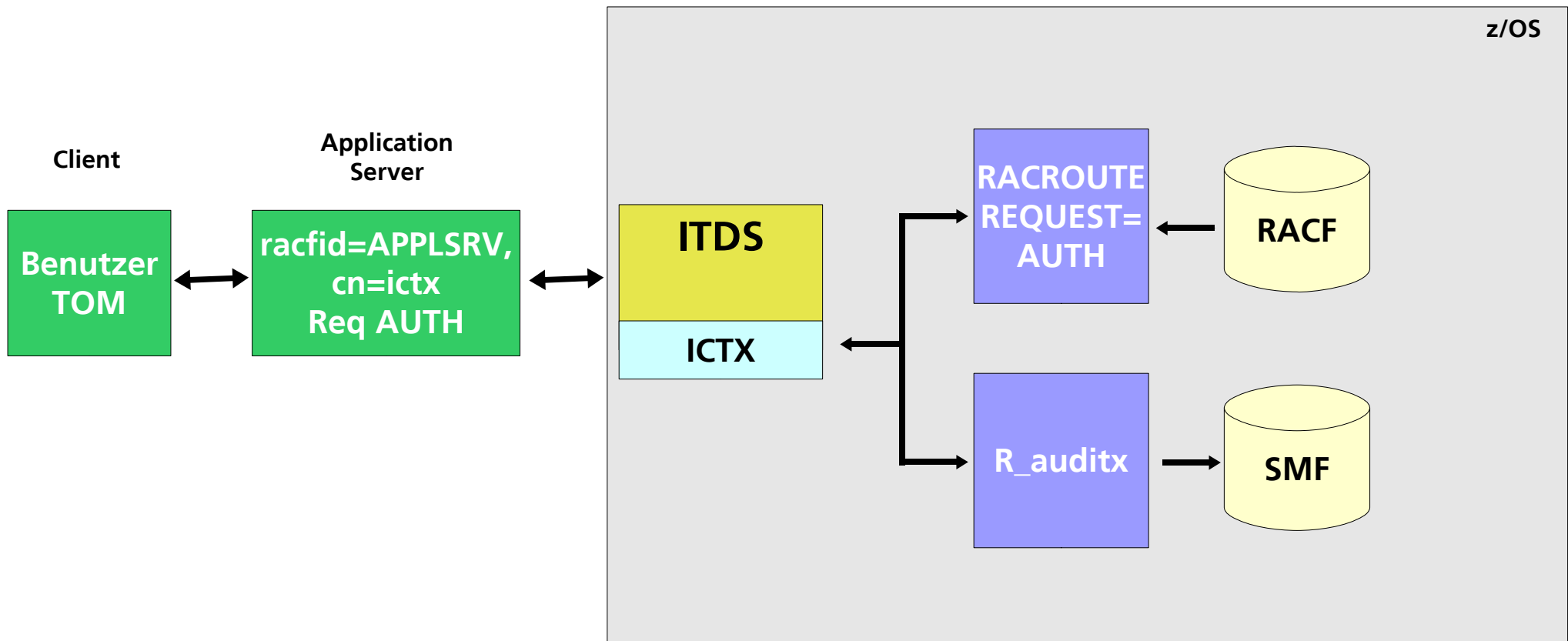
z/OS Identity Cache - Anwendungsbeispiel

WAS-1 AIX

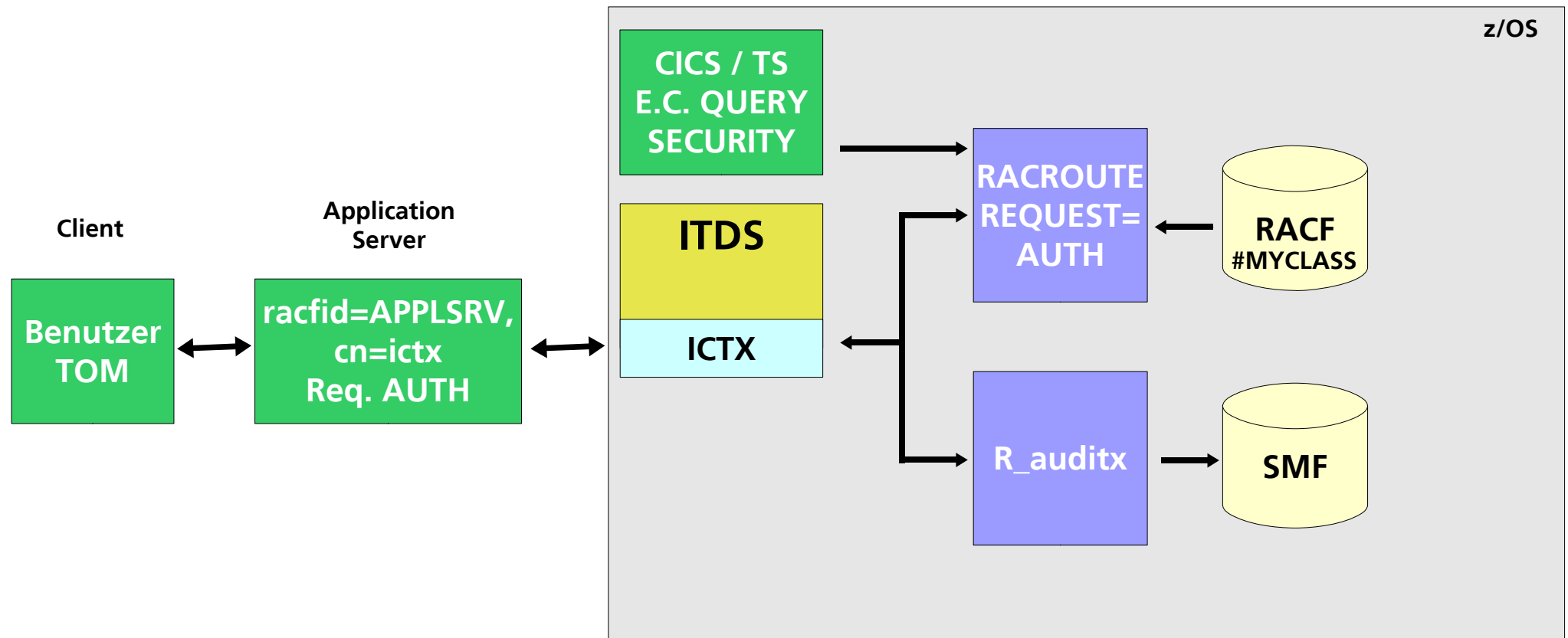


WAS-2 AIX

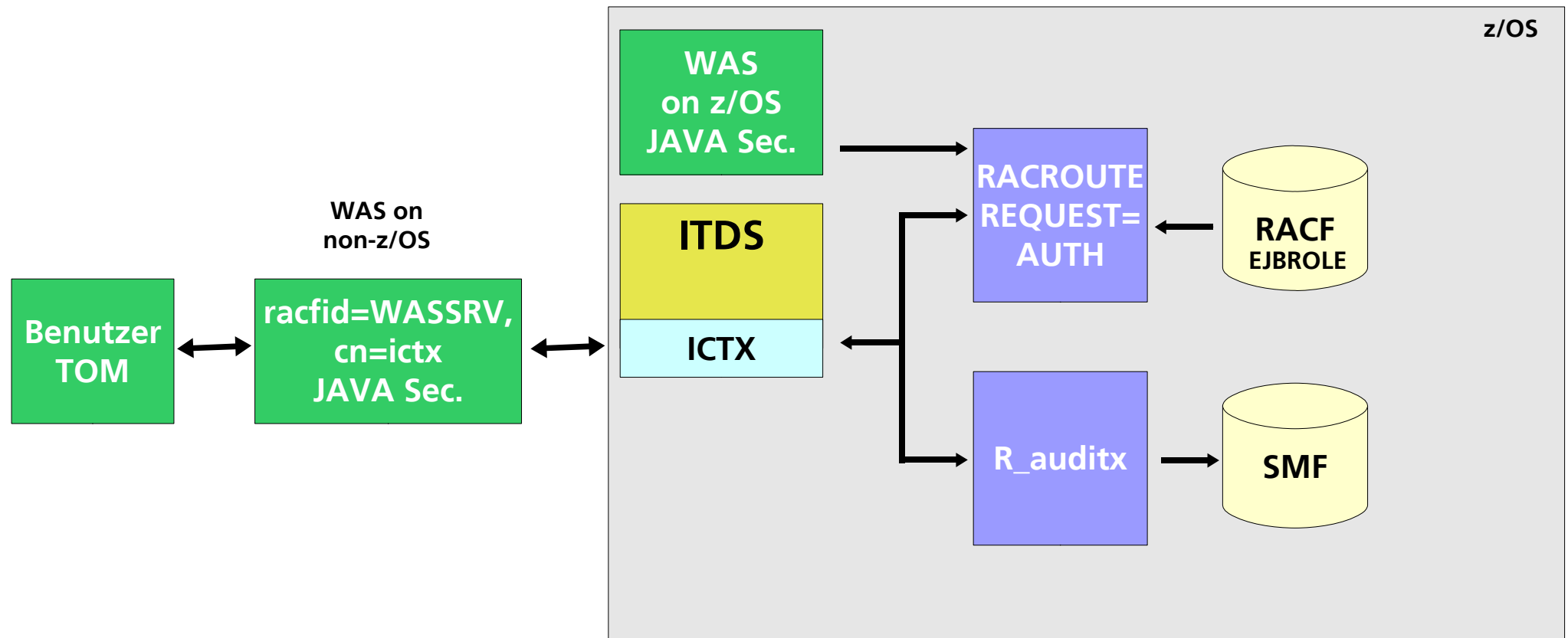
Remote Authorization und Auditing



Remote Authorization und Auditing - Anwendungsbeispiel 1



Remote Authorization und Auditing - Anwendungsbeispiel 2



Referenzen I

- LDAP
 - IBM Tivoli Directory Server Administration and Use, SC23-5191
 - Advanced LDAP User Authentication: Limiting Access to Linux Systems Using the Host Attribute, REDP3863.PDF
<http://www.redbooks.ibm.com>
 - Linux on IBM zSeries and S/390: Securing Linux for zSeries with a Central z/OS LDAP Server (RACF), REDP0221.PDF
<http://www.redbooks.ibm.com>

Referenzen II

- **ICTX**
 - EIM Guide and Reference, SA22-7875
 - ICTX Java API Javadoc
<http://www-03.ibm.com/systems/z/os/zos/downloads>
 - ICTX Java API
`/usr/lpp/eim/lib/ictx.jar`
- **WAS plugin**
 - IBMRRAP code, documentation, and utilities for WebSphere Application Server (WAS) 6.0 and WAS 6.1
<http://www-03.ibm.com/systems/z/os/zos/downloads>



Kontakt

Oliver Paukstadt
IT-Consultant

Millenux GmbH
Lilienthalstraße 2/1
70825 Korntal-Münchingen

Tel. +49 711 88770 300

Fax +49 711 88770 349

Oliver.Paukstadt@millenux.com
www.millenux.com

Christian Tatz
Senior-Consultant

Empalis GmbH
Lilienthalstraße 2/1
70825 Korntal-Münchingen

Tel. +49 711 88770 200

Fax +49 711 88770 249

Christian.Tatz@empalis.com
www.empalis.com