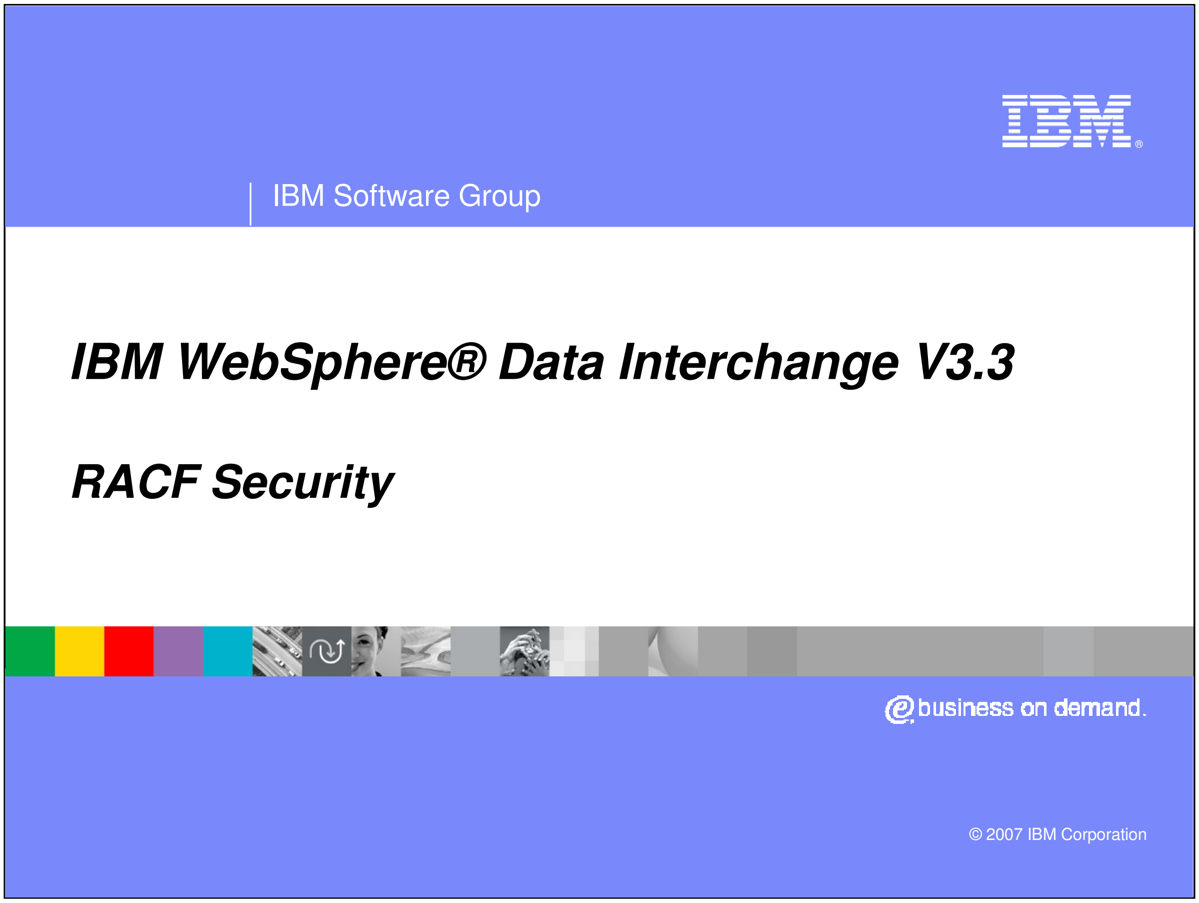


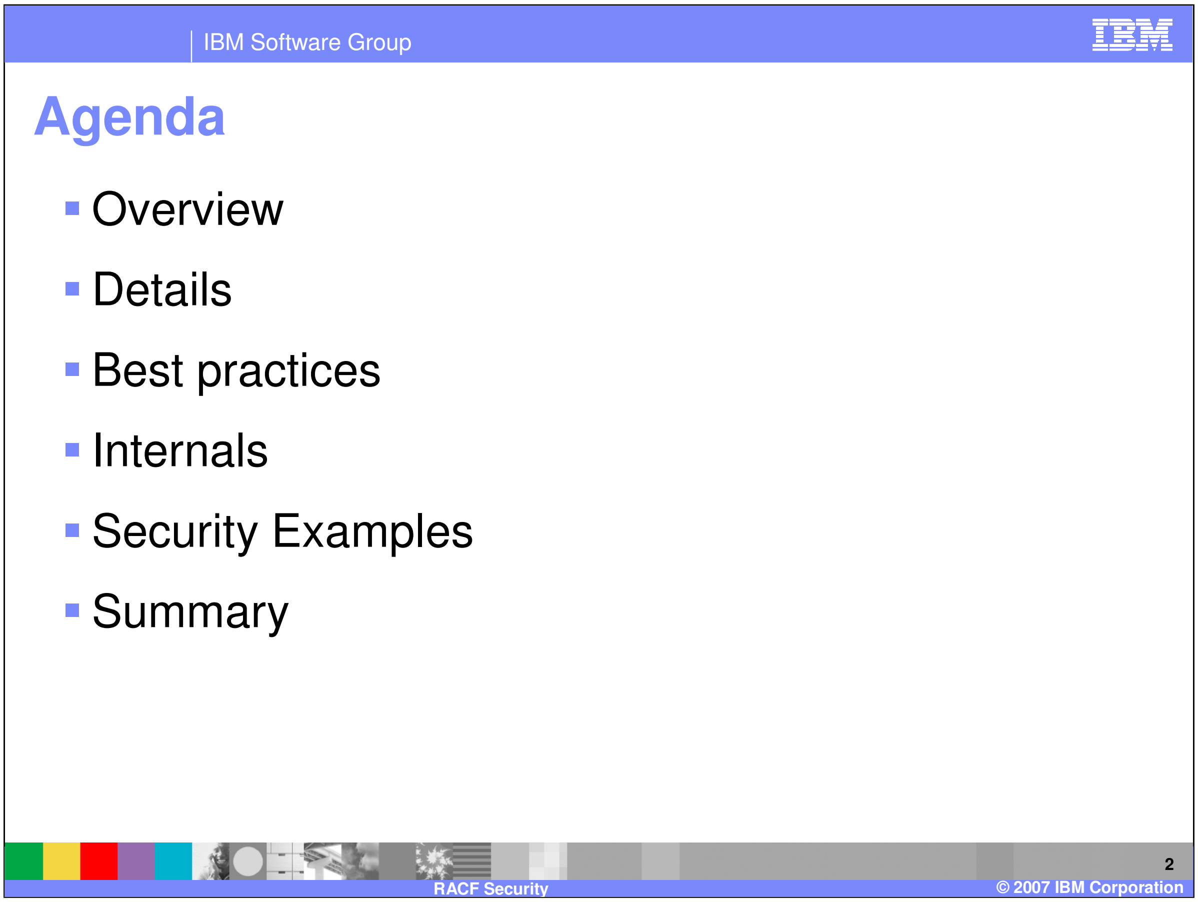
IBM Software Group

IBM WebSphere® Data Interchange V3.3

RACF Security

business on demand.

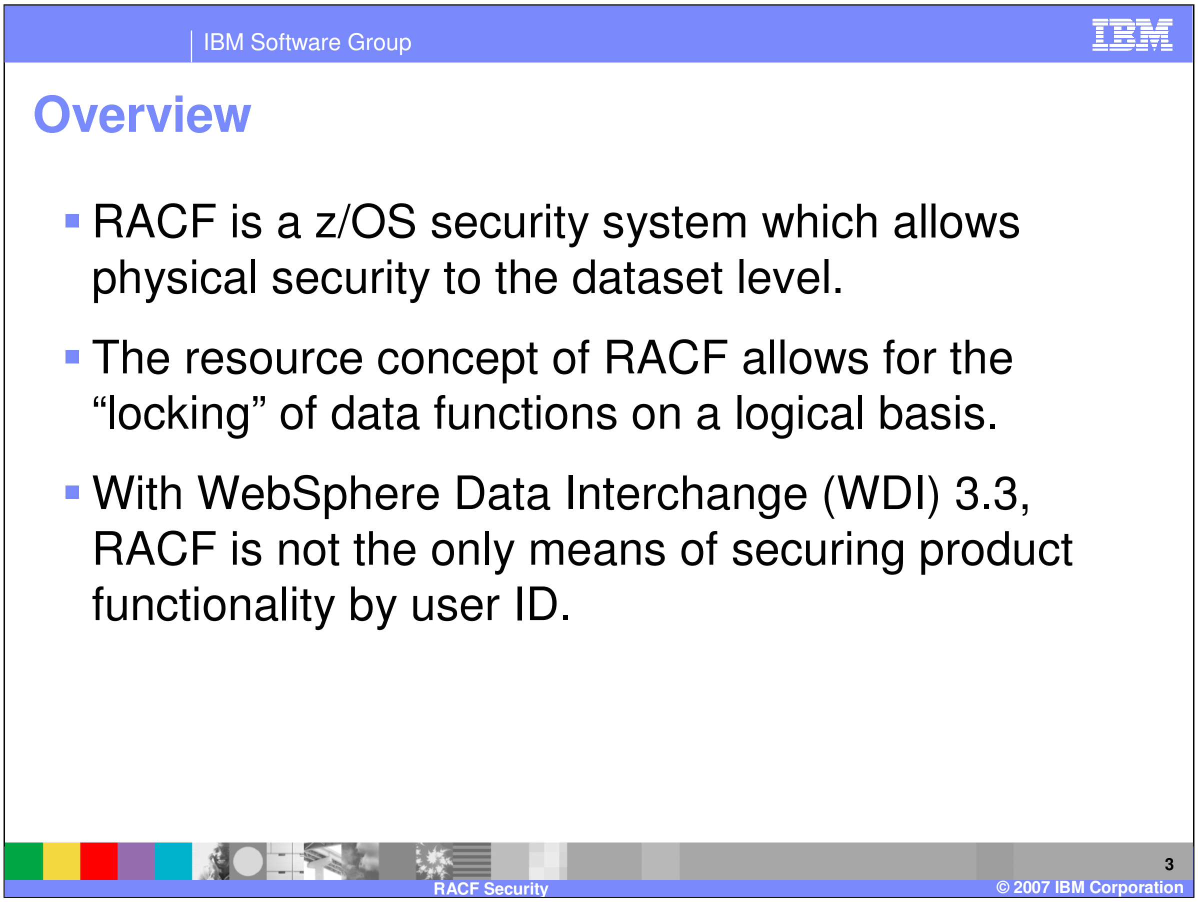
This presentation will review Resource Access Control Facility (RACF) Security.



Agenda

- Overview
- Details
- Best practices
- Internals
- Security Examples
- Summary

The presentation will give an overview with details and examples.



IBM Software Group

Overview

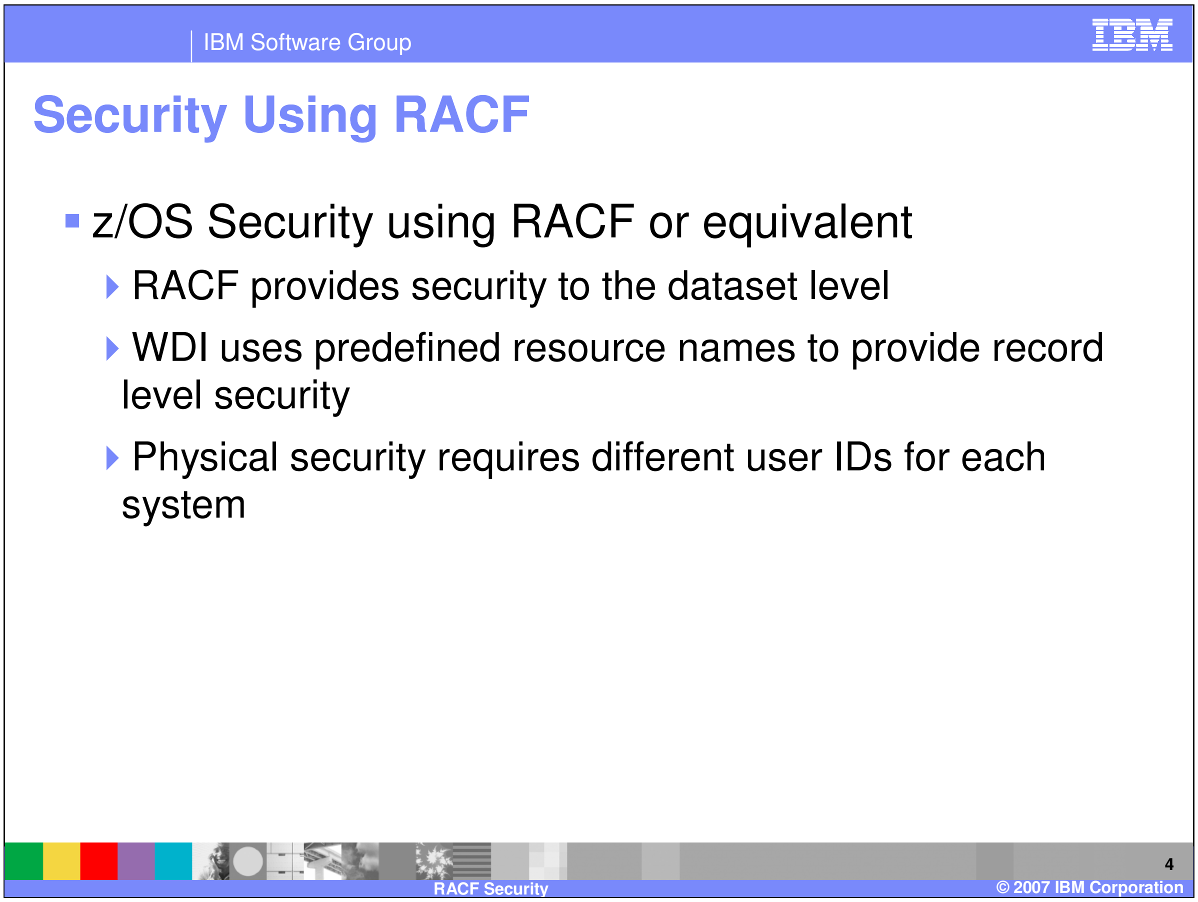
- RACF is a z/OS security system which allows physical security to the dataset level.
- The resource concept of RACF allows for the “locking” of data functions on a logical basis.
- With WebSphere Data Interchange (WDI) 3.3, RACF is not the only means of securing product functionality by user ID.

3

RACF Security

© 2007 IBM Corporation

The Resource Access Control Facility (RACF) is a z/OS security system which allows physical security to the dataset level. WebSphere Data Interchange (WDI) used RACF exclusively in earlier z/OS releases so that VSAM files and DB2 data tables were treated the same. The resource concept of RACF allowed for the “locking” of data functions on a logical basis, much as does ENQ / DEQ does for system functions. With WDI 3.3, RACF calls are still available for backwards compatibility purposes, but are not the only means of securing product functionality by user ID.



IBM Software Group

Security Using RACF

- z/OS Security using RACF or equivalent
  - RACF provides security to the dataset level
  - WDI uses predefined resource names to provide record level security
  - Physical security requires different user IDs for each system

4

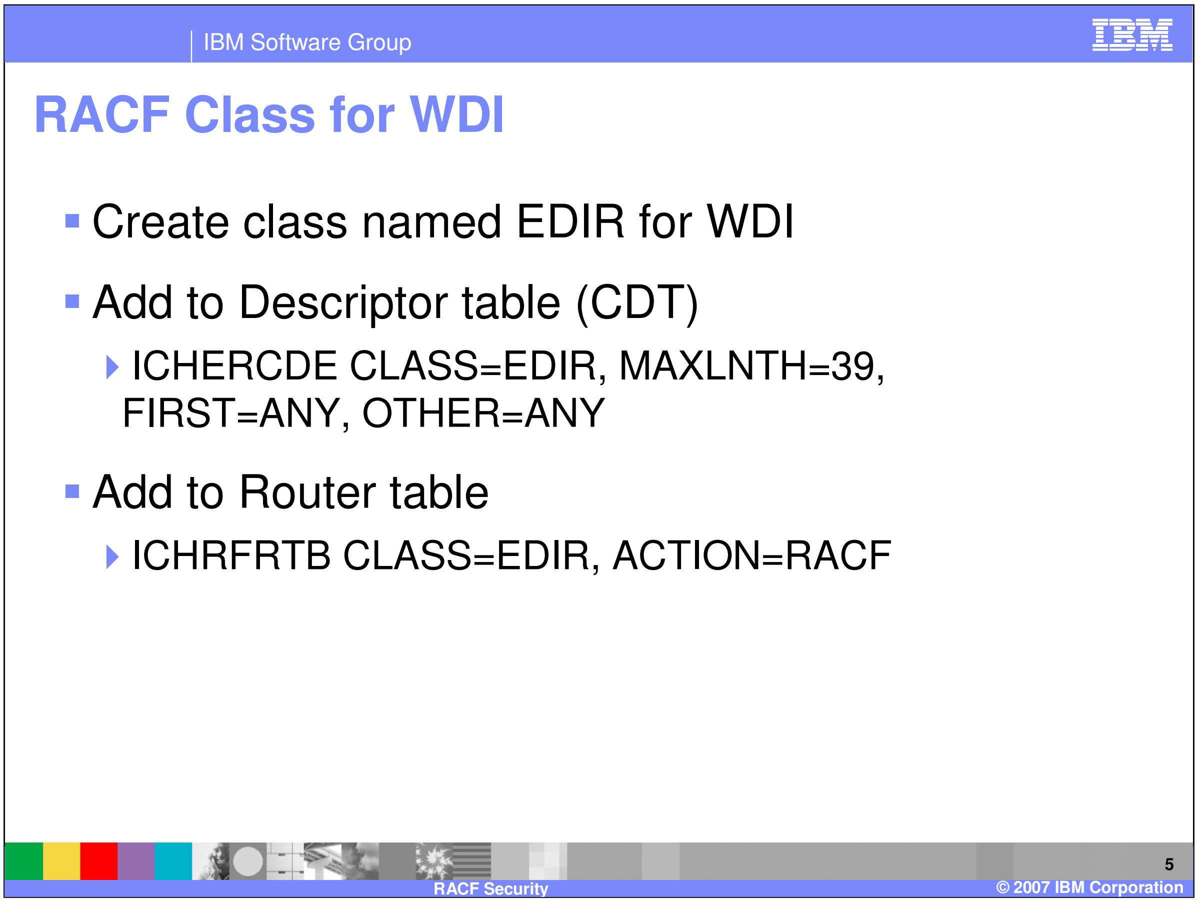
RACF Security

© 2007 IBM Corporation

Security for WebSphere Data Interchange is provided by the Resource Access Control Facility (RACF**) or an equivalent product that is consistent with System Authorization Facility (SAF) interfaces. To protect WebSphere Data Interchange programs and data, use RACF (or an equivalent) and the resource names described later.

WebSphere Data Interchange provides the level of security that RACF or an equivalent can provide in the MVS/TSO environment. This lets you control access to the WDI systems, and files during WebSphere Data Interchange execution. WebSphere Data Interchange provides control over the record-level access through predefined resource names. However, because RACF or an equivalent provides security only to the data set level, users have access to the entire data set.

If you have installed more than one WebSphere Data Interchange system, have multiple system-related resource names, and have a user that needs to have different authority levels based on the system-related resource names, the only way to guarantee the authority levels is to use a different MVS/TSO user ID for each system-related resource name.



IBM Software Group

RACF Class for WDI

- Create class named EDIR for WDI
- Add to Descriptor table (CDT)
  - ICHERCDE CLASS=EDIR, MAXLNTH=39, FIRST=ANY, OTHER=ANY
- Add to Router table
  - ICHRFRTB CLASS=EDIR, ACTION=RACF

5

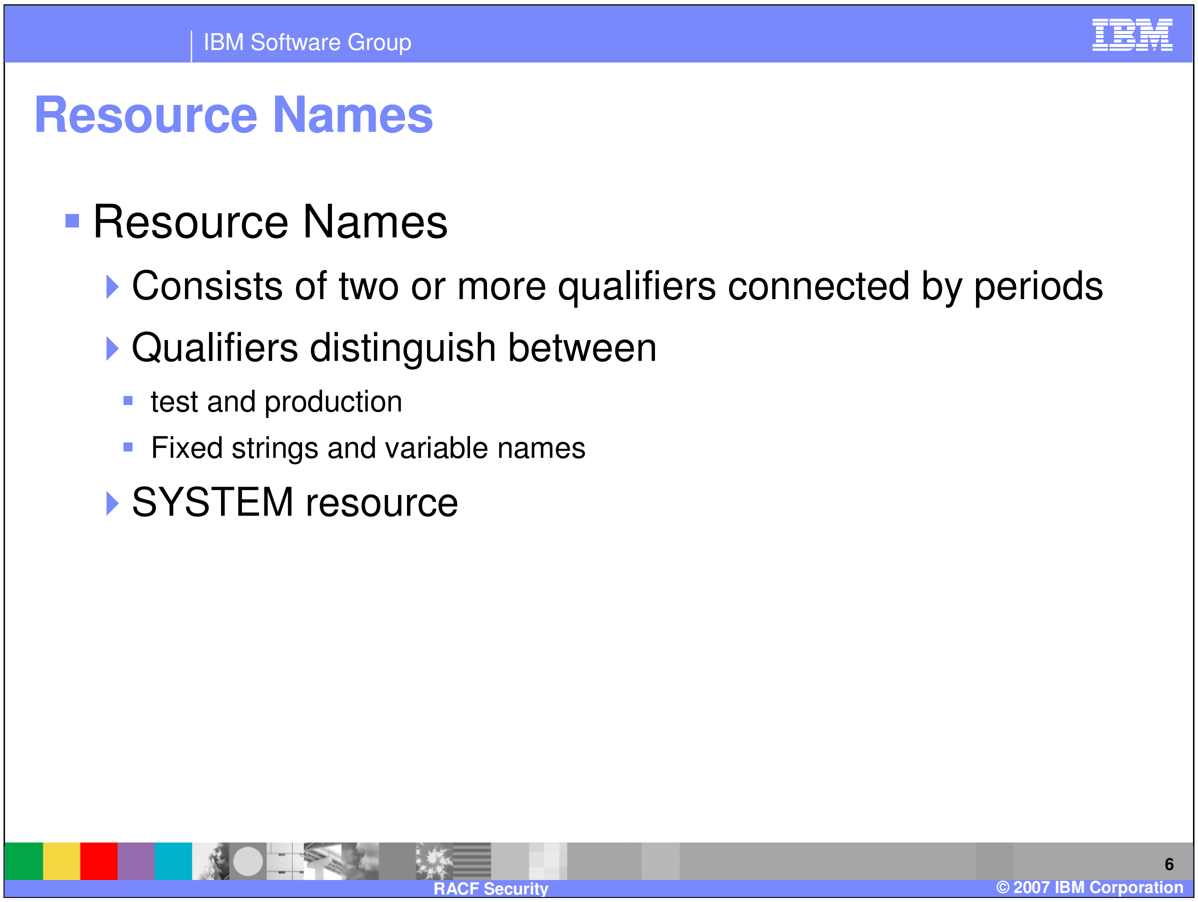
RACF Security

© 2007 IBM Corporation

To protect WDI resources, create a new RACF class called EDIR. Add this class to the class descriptor table (CDT) using the ICHERCDE macro. For details, see your access control facility documentation. For EDIR, specify the macro as follows. Values not shown are chosen locally. You must also add class EDIR to the RACF router table using the ICHRFRTB macro with ACTION = RACF:

ICHRFRTB CLASS=EDIR, ACTION=RACF

Customers using TopSecret instead of RACF should add a RESCLASS, EDIR, to their Resource Descriptor Table (RDT) and manage it as any resource.



Resource Names

- Resource Names
  - Consists of two or more qualifiers connected by periods
  - Qualifiers distinguish between
    - test and production
    - Fixed strings and variable names
  - SYSTEM resource

The resource names are RACF profile names. Each resource name consists of two or more qualifiers connected by periods. Qualifiers that appear in uppercase are to be used as shown. Those in lowercase are variables. The variable sys, for system name, is required only if you have installed more than one copy of WebSphere Data Interchange on the same system. For example, you would use sys to distinguish between a test and a production version. You can use two types of system-related resource names:

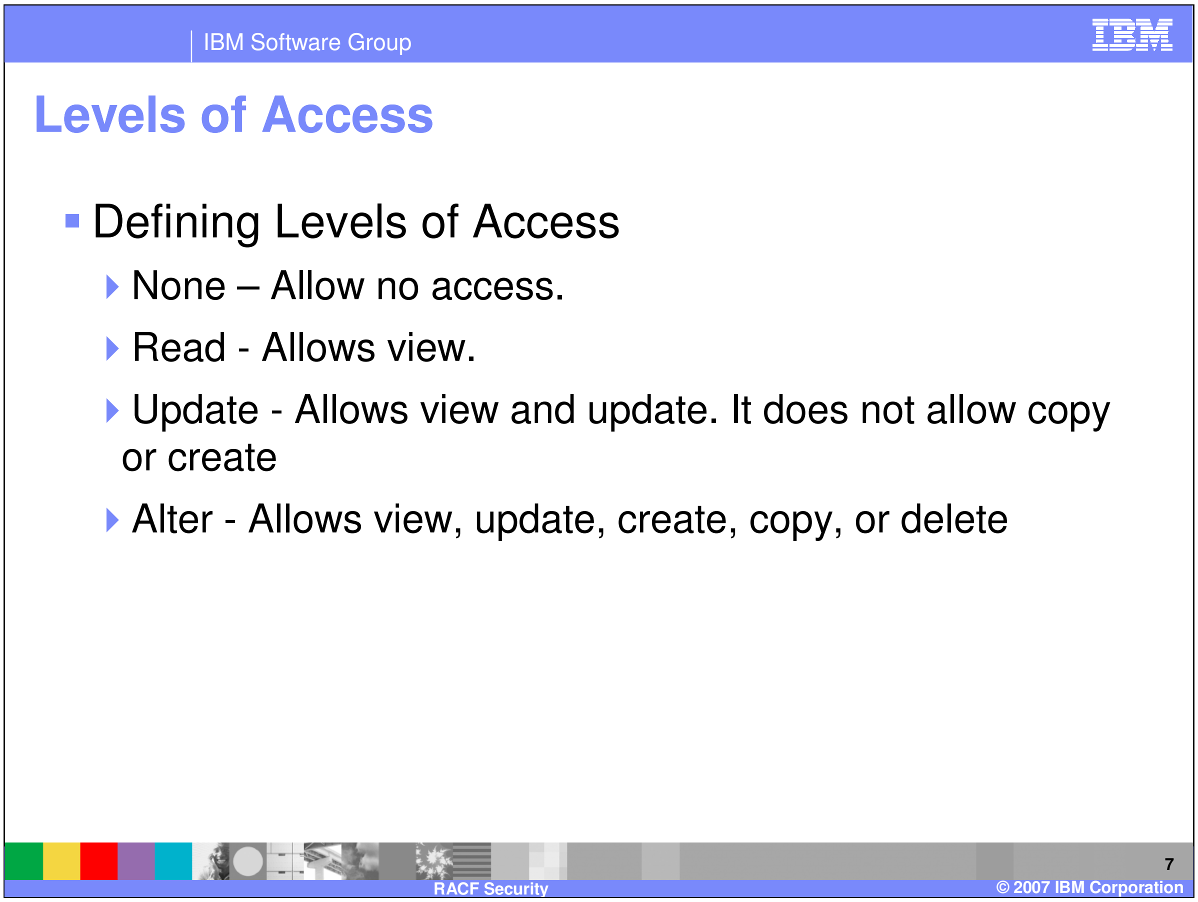
SYSTEM.sys, where sys is the system name for one copy of WDI, such as the copy used for testing or the copy used for production. Using system names, you can provide separate protection for each copy of WDI. The system name can be up to 8 characters. If a system name is not provided when WDI is started, DIENU is used by default.

SYSTEM determines how the system name is used to grant users access to the WebSphere Data Interchange product.

If the SYSTEM resource is defined, users must be specifically granted access under the SYSTEM.sys resource name, or they are denied access to the product.

If the SYSTEM resource is not defined, users are granted access to the product unless they are specifically excluded under the SYSTEM.sys resource name.

For all resource names which have variables at the end of the name, you can customize your access to the resource.



IBM Software Group

Levels of Access

- Defining Levels of Access
  - None – Allow no access.
  - Read - Allows view.
  - Update - Allows view and update. It does not allow copy or create
  - Alter - Allows view, update, create, copy, or delete

7

RACF Security

You can grant the following access levels to resource names:

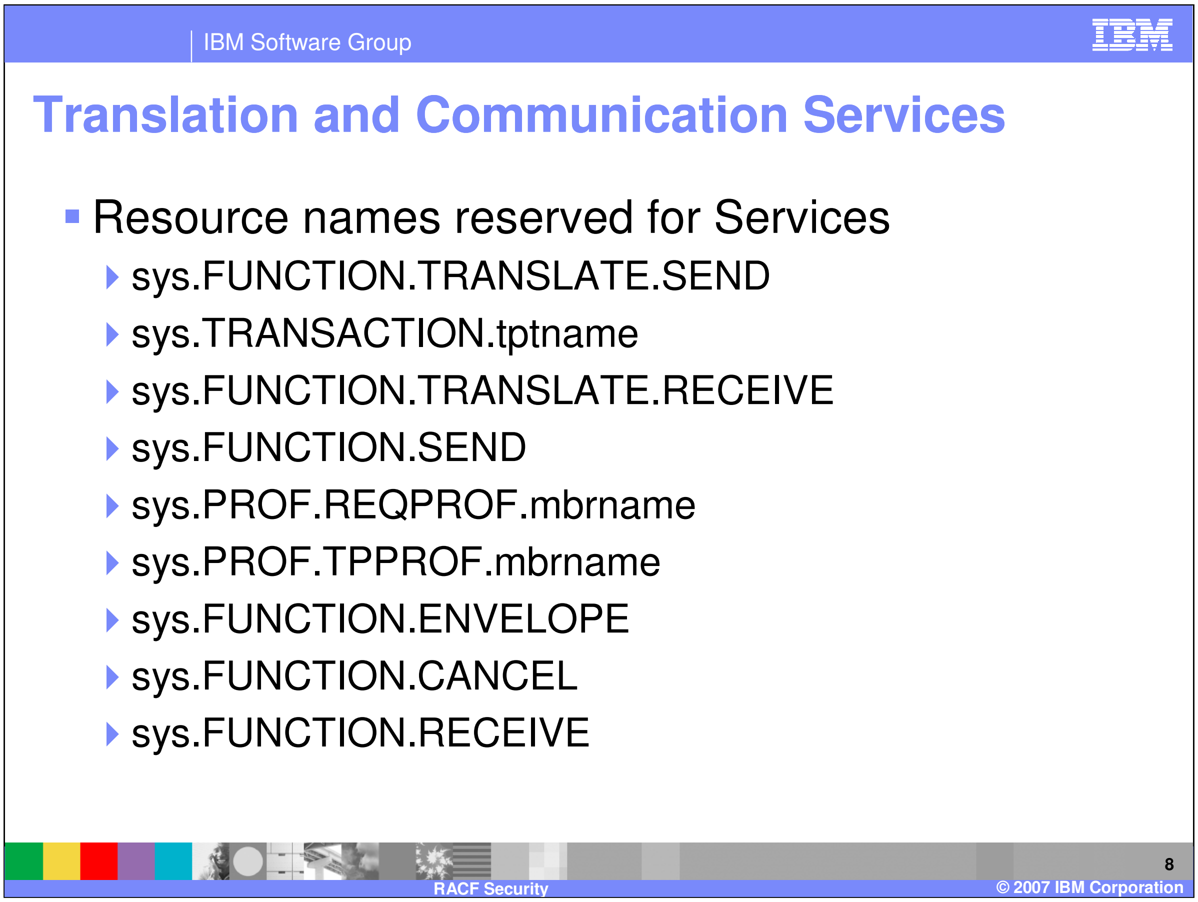
None - Users cannot access the resource.

Read - Allows users to view the resource.

Update - Allows users to view and update the resource. It does not allow the user to copy or create

the resource.

Alter - Allows users to view, update, create, copy, or delete the resource.



IBM Software Group

Translation and Communication Services

- Resource names reserved for Services
  - sys.FUNCTION.TRANSLATE.SEND
  - sys.TRANSACTION.tptname
  - sys.FUNCTION.TRANSLATE.RECEIVE
  - sys.FUNCTION.SEND
  - sys.PROF.REQPROF.mbrname
  - sys.PROF.TPPROF.mbrname
  - sys.FUNCTION.ENVELOPE
  - sys.FUNCTION.CANCEL
  - sys.FUNCTION.RECEIVE

8

RACF Security

© 2007 IBM Corporation

WDI provides services (function calls) that are available through an application program interface (API). and the WDI Utility. The resource names used to protect these functions are the following:

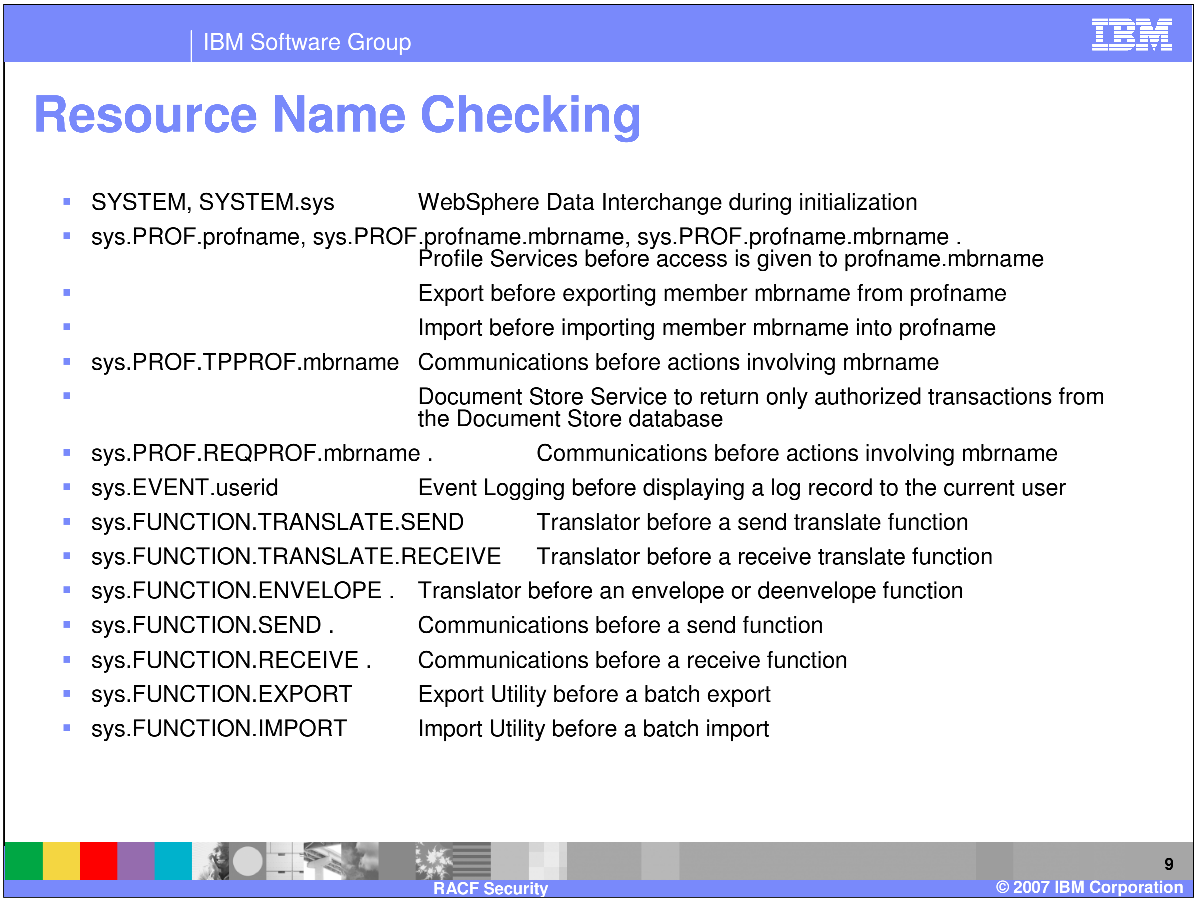
sys.FUNCTION.TRANSLATE.SEND for the Translate for Sending function. Only users who have access under this resource can translate documents for sending. In addition, users must have access under the appropriate sys.TRANSACTION.tptname resource, or the translation is not allowed.

sys.FUNCTION.TRANSLATE.RECEIVE for the Translate Received Transactions function. Only users who have access under this resource can translate documents that have been received. In addition, users must have access under the appropriate sys.TRANSACTION.tptname resource, or the translation is not allowed.

sys.FUNCTION.SEND for the Send Network function. Only users who have access under this resource can send documents to the network. In addition, users must have access under the appropriate sys.PROF.REQPROF.mbrname and sys.PROF.TPPROF.mbrname, or the send is not allowed.

sys.FUNCTION.ENVELOPE for the Envelope and Deenvelope functions. Only users who have access under this resource name can envelope or deenvelope documents.

sys.FUNCTION.CANCEL for the Network Cancel function. Only users who have access under this resource can cancel documents from the network or use the RECALL function from the



IBM Software Group

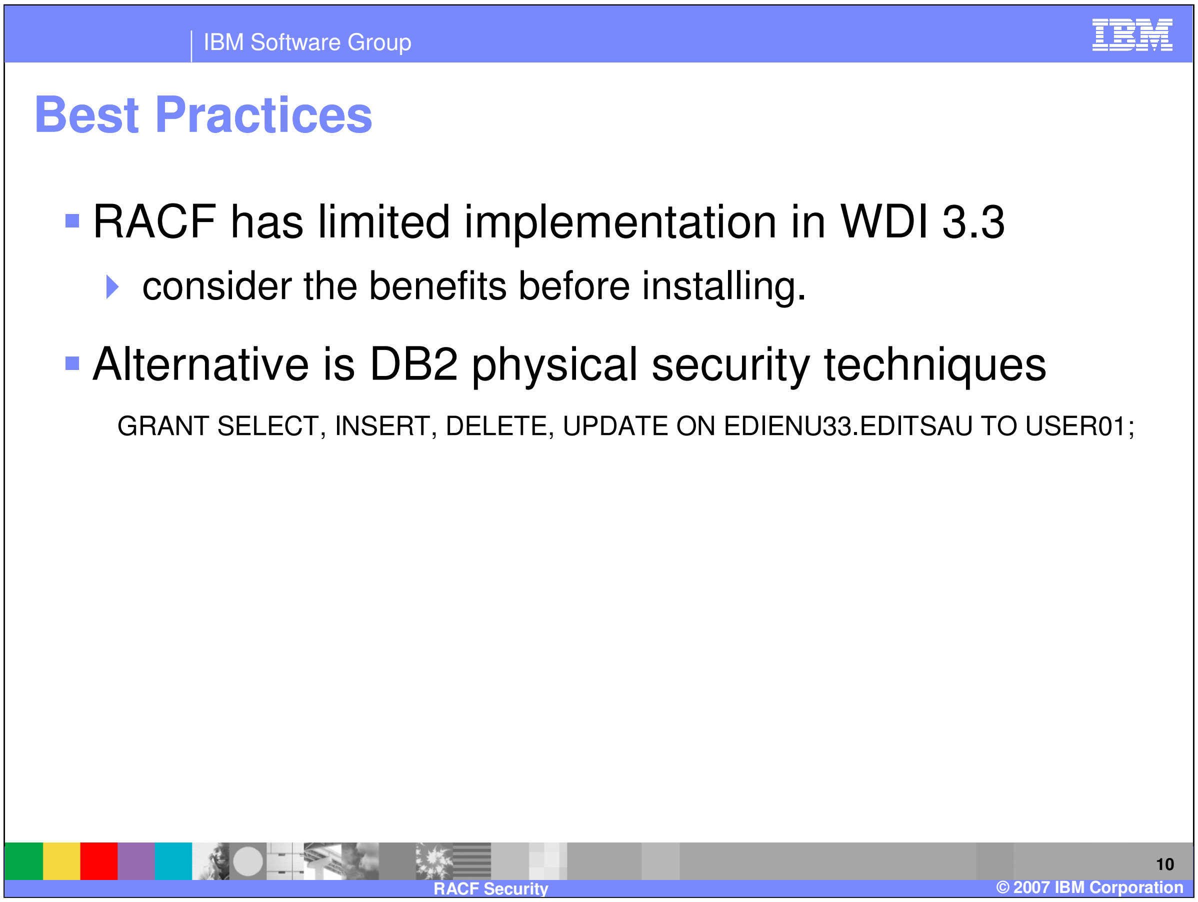
Resource Name Checking

SYSTEM, SYSTEM.sys	WebSphere Data Interchange during initialization
sys.PROF.profname, sys.PROF.profname.mbrname, sys.PROF.profname.mbrname .	Profile Services before access is given to profname.mbrname
	Export before exporting member mbrname from profname
	Import before importing member mbrname into profname
sys.PROF.TPPROF.mbrname	Communications before actions involving mbrname
	Document Store Service to return only authorized transactions from the Document Store database
sys.PROF.REQPROF.mbrname .	Communications before actions involving mbrname
sys.EVENT.userid	Event Logging before displaying a log record to the current user
sys.FUNCTION.TRANSLATE.SEND	Translator before a send translate function
sys.FUNCTION.TRANSLATE.RECEIVE	Translator before a receive translate function
sys.FUNCTION.ENVELOPE .	Translator before an envelope or deenvelope function
sys.FUNCTION.SEND .	Communications before a send function
sys.FUNCTION.RECEIVE .	Communications before a receive function
sys.FUNCTION.EXPORT	Export Utility before a batch export
sys.FUNCTION.IMPORT	Import Utility before a batch import

9

RACF Security

This represents the WDI resource names and the services that check the user authorization.



IBM Software Group

Best Practices

- RACF has limited implementation in WDI 3.3
  - consider the benefits before installing.
- Alternative is DB2 physical security techniques

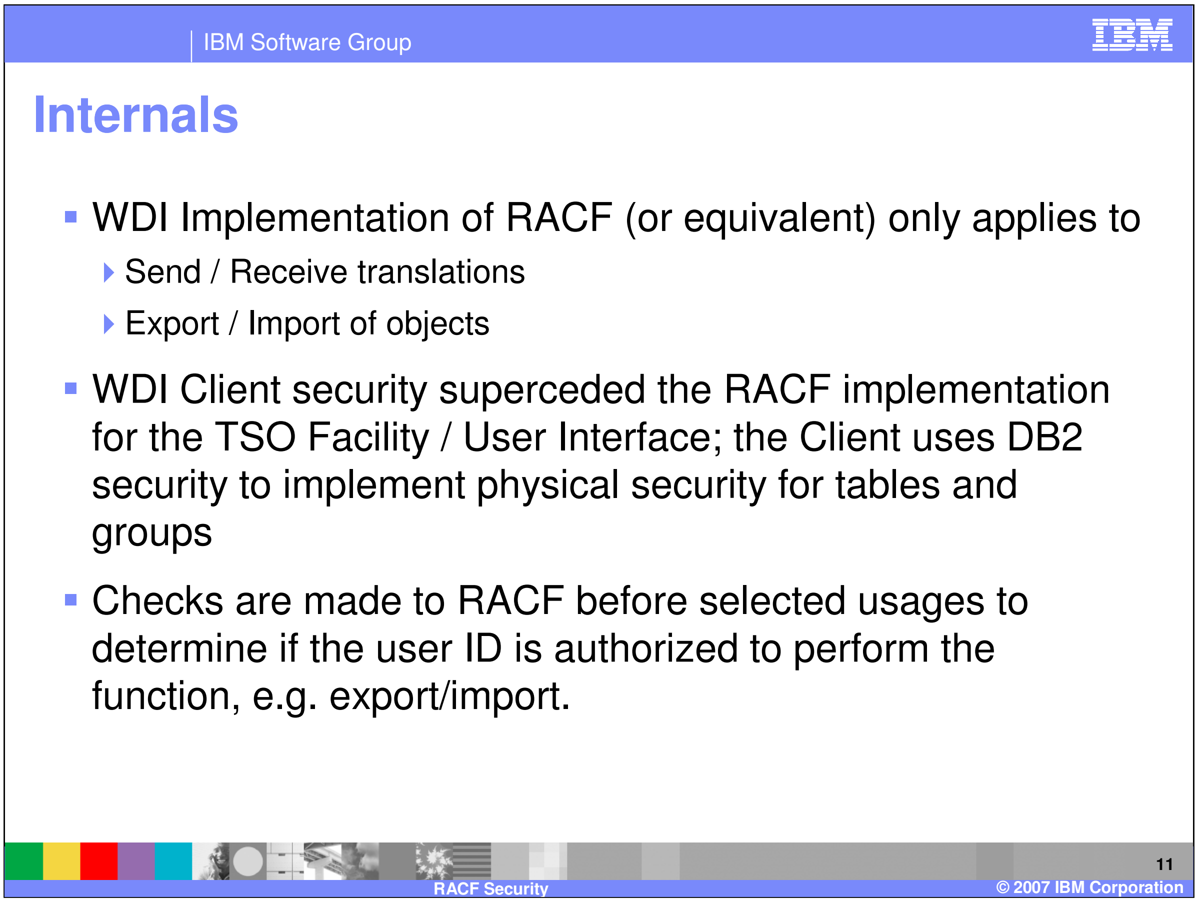
```
GRANT SELECT, INSERT, DELETE, UPDATE ON EDIENU33.EDITSAU TO USER01;
```

10

RACF Security

© 2007 IBM Corporation

Since RACF has limited implementation in WDI 3.3, consider the benefits before installing. Consider using DB2 physical security techniques for example the GRANT function rather than RACF.



IBM Software Group

Internals

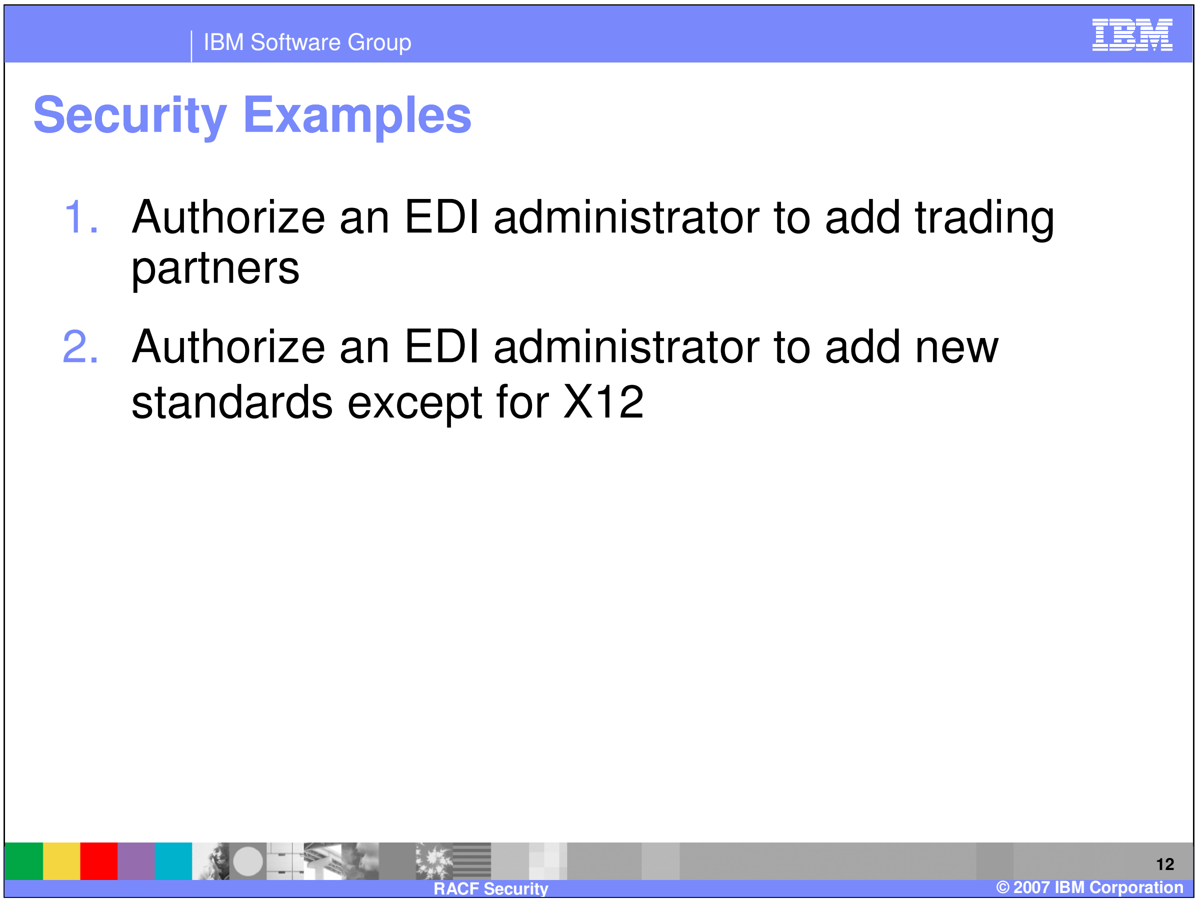
- WDI Implementation of RACF (or equivalent) only applies to
  - Send / Receive translations
  - Export / Import of objects
- WDI Client security superceded the RACF implementation for the TSO Facility / User Interface; the Client uses DB2 security to implement physical security for tables and groups
- Checks are made to RACF before selected usages to determine if the user ID is authorized to perform the function, e.g. export/import.

11

RACF Security

The WDI Implementation of RACF (or equivalent) only applies to the Send and Receive translation processing and Export, Import of objects.

WDI Client security superceded the RACF implementation for the TSO Facility and User Interface. The Client uses DB2 security to implement physical security for tables and groups. Checks are made to RACF before selected usages to determine if the user ID is authorized to perform the function with export and import.



IBM Software Group

Security Examples

1. Authorize an EDI administrator to add trading partners
2. Authorize an EDI administrator to add new standards except for X12

12

RACF Security

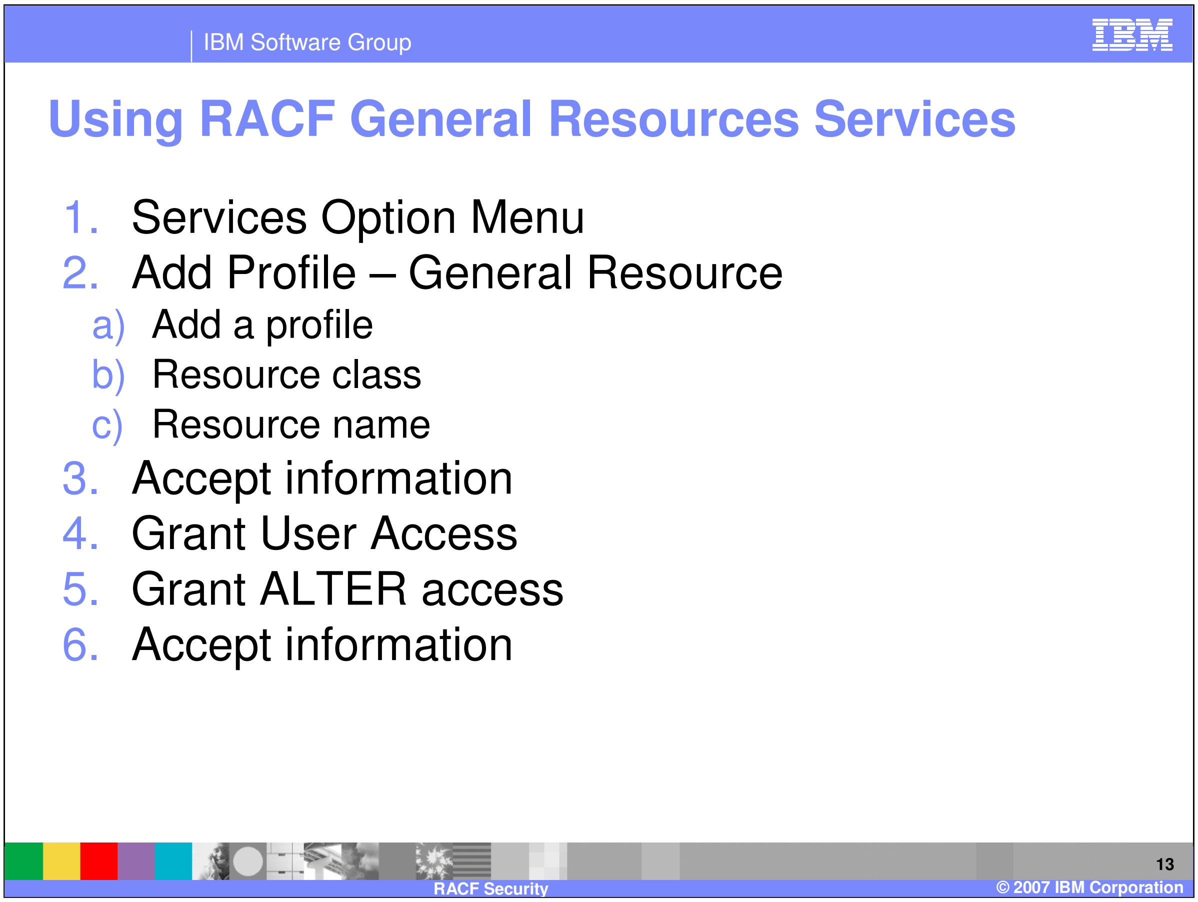
© 2007 IBM Corporation

The following examples show the resource names (RACF profiles) with which you associate a user’ ID to enable the user to perform certain tasks.

Example 1: Authorize an EDI administrator to add trading partners. Only one copy of WDI is installed. This requires resource access to

DIENU.PROF.TPPROF.* for all trading partner profiles.

Example 2: Authorize an EDI administrator to add new standards except for X12. Only one copy of WDI is installed. This requires resource access to DIENU.STANDARD for access to the EDI standards. Use ALTER access for this resource name. Use DIENU.STANDARD.X12* to limit access to all standards beginning with the string “” to READ access only.



Using RACF General Resources Services

1. Services Option Menu
2. Add Profile – General Resource
   a) Add a profile
   b) Resource class
   c) Resource name
3. Accept information
4. Grant User Access
5. Grant ALTER access
6. Accept information

The following steps show an example of defining a RACF profile for the general resource SYSTEM.DIENU and then granting access to the resource.

1. From the RACF - Services Option Menu, select option 2 to add a profile for a general resource.

2. Complete the fields as follows:

a. Type **1** in the Option field to add a profile.

b. Type **EDIR** in the RESOURCE CLASS field.

c. Type **SYSTEM.DIENU** in the RESOURCE NAME field.

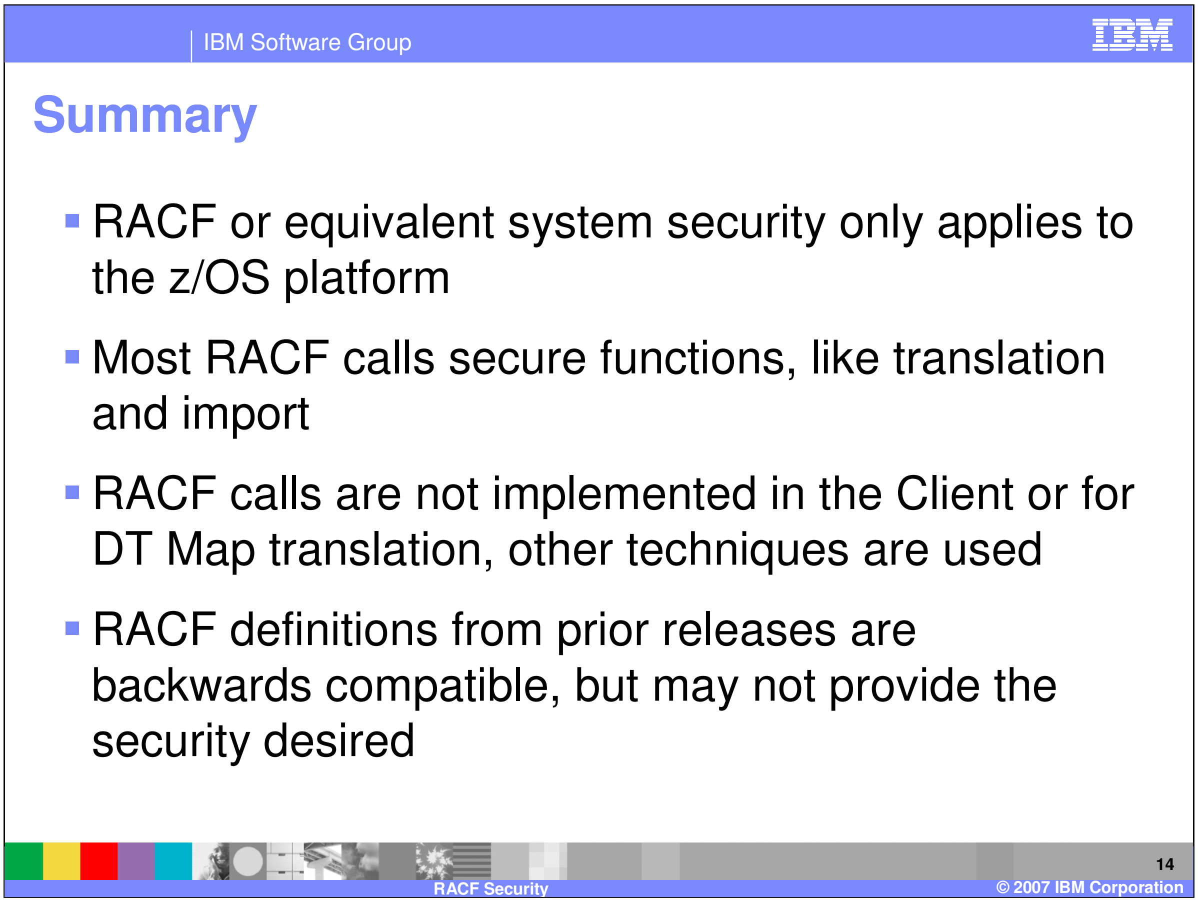
d. Press Enter. The RACF - Add General Resource Profile panel is displayed.

3. Press Enter to accept the information supplied on the Add panel. The RACF - General Resources Services panel is redisplayed.

4. Select option 4 to grant users access to the resource you just defined. The RACF - Maintain General Resource Access List - Add panel is displayed.

5. Grant ALTER access rights for the resource SYSTEM.DIENU. The owner, USERA, always has access. Enter the IDs of all other users you want to grant ALTER access to this resource.

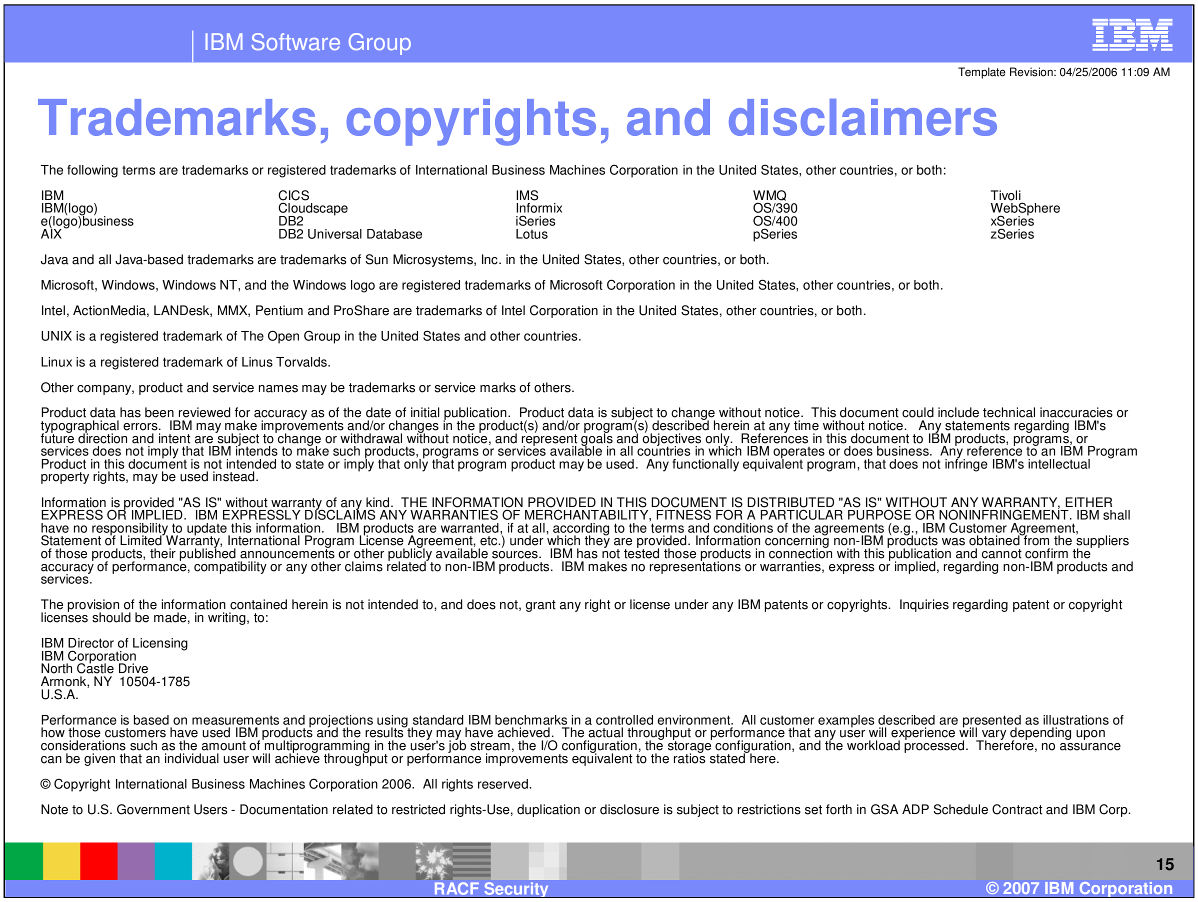
6. Press Enter to accept the information supplied.



Summary

- RACF or equivalent system security only applies to the z/OS platform
- Most RACF calls secure functions, like translation and import
- RACF calls are not implemented in the Client or for DT Map translation, other techniques are used
- RACF definitions from prior releases are backwards compatible, but may not provide the security desired

RACF or equivalent system security only applies to the z/OS platform. Most RACF calls secure functions, like translation and import. RACF calls are not implemented in the Client or for Data Transformation (DT) Map translation, other techniques are used. RACF definitions from prior releases are backwards compatible, but may not provide the security desired.



Template Revision: 04/25/2006 11:09 AM

Trademarks, copyrights, and disclaimers

The following terms are trademarks or registered trademarks of International Business Machines Corporation in the United States, other countries, or both:

IBM
IBM(logo)
e(logo)business
AIX
CICS
Cloudscape
DB2
DB2 Universal Database
IMS
Informix
iSeries
Lotus
WMQ
OS/390
OS/400
pSeries
Tivoli
WebSphere
xSeries
zSeries

Java and all Java-based trademarks are trademarks of Sun Microsystems, Inc. in the United States, other countries, or both.

Microsoft, Windows, Windows NT, and the Windows logo are registered trademarks of Microsoft Corporation in the United States, other countries, or both.

Intel, ActionMedia, LANDesk, MMX, Pentium and ProShare are trademarks of Intel Corporation in the United States, other countries, or both.

UNIX is a registered trademark of The Open Group in the United States and other countries.

Linux is a registered trademark of Linus Torvalds.

Other company, product and service names may be trademarks or service marks of others.

Product data has been reviewed for accuracy as of the date of initial publication. Product data is subject to change without notice. This document could include technical inaccuracies or typographical errors. IBM may make improvements and/or changes in the product(s) and/or program(s) described herein at any time without notice. Any statements regarding IBM's future direction and intent are subject to change or withdrawal without notice, and represent goals and objectives only. References in this document to IBM products, programs, or services does not imply that IBM intends to make such products, programs or services available in all countries in which IBM operates or does business. Any reference to an IBM Program Product in this document is not intended to state or imply that only that program product may be used. Any functionally equivalent program, that does not infringe IBM's intellectual property rights, may be used instead.

Information is provided "AS IS" without warranty of any kind. THE INFORMATION PROVIDED IN THIS DOCUMENT IS DISTRIBUTED "AS IS" WITHOUT ANY WARRANTY, EITHER EXPRESS OR IMPLIED. IBM EXPRESSLY DISCLAIMS ANY WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE OR NONINFRINGEMENT. IBM shall have no responsibility to update this information. IBM products are warranted, if at all, according to the terms and conditions of the agreements (e.g., IBM Customer Agreement, Statement of Limited Warranty, International Program License Agreement, etc.) under which they are provided. Information concerning non-IBM products was obtained from the suppliers of those products, their published announcements or other publicly available sources. IBM has not tested those products in connection with this publication and cannot confirm the accuracy of performance, compatibility or any other claims related to non-IBM products. IBM makes no representations or warranties, express or implied, regarding non-IBM products and services.

The provision of the information contained herein is not intended to, and does not, grant any right or license under any IBM patents or copyrights. Inquiries regarding patent or copyright licenses should be made, in writing, to:

IBM Director of Licensing
IBM Corporation
North Castle Drive
Armonk, NY 10504-1785
U.S.A.

Performance is based on measurements and projections using standard IBM benchmarks in a controlled environment. All customer examples described are presented as illustrations of how those customers have used IBM products and the results they may have achieved. The actual throughput or performance that any user will experience will vary depending upon considerations such as the amount of multiprogramming in the user's job stream, the I/O configuration, the storage configuration, and the workload processed. Therefore, no assurance can be given that an individual user will achieve throughput or performance improvements equivalent to the ratios stated here.

Note to U.S. Government Users - Documentation related to restricted rights-Use, duplication or disclosure is subject to restrictions set forth in GSA ADP Schedule Contract and IBM Corp.