stromwerken

# Berechtigungsreports

## Bereich AD/WinNt

### #200 AD/WinNT - User mit allen Parametern

Zeigt die AD/WinNT-User, sortiert nach Benutzerkennungen, mit ihrem letzten Login-Datum an.

### #201 AD/WinNT - User letzte Anmeldung und PW-Wechsel (Matrix)

Zeigt die AD/WinNT-User, sortiert nach Benutzerkennungen, mit ihrem letztem Anmelde und Passwortwechsel-Datum an.

Die letzte Anmeldung im AD wird aus dem jüngeren Datum der AD-Variablen lastLogon und lastLogonTimestamp gebildet.

Erläuterung: lastLogon und lastLogonTimestamp unterscheiden sich dadurch, dass lastLogon nicht zwischen den Domänencontrollern repliziert wird, lastLogonTimestamp schon (allerdings erst nach 9-14 Tagen). Der jüngere Werte ist also der "richtigere", wobei der genaue Wert der letzten Anmeldung in der Domäne tatsächlich erst nach 9-14 Tagen im AD über die Variable lastLogonTimestamp ausgelesen werden kann.

### #202 AD/WinNT - User in Gruppen (Matrix)

Zeigt die AD/WinNT-User sowie die Gruppen der AD/WinNT-User als Matrix an. Es kann nur eine bestimmte Anzahl an Gruppen angezeigt werden, sollten mehr Gruppen vorhanden sein, bricht der Report mit einem Fehler ab. Reduzieren Sie dann die User oder die anzuzeigenden Gruppen.

### #203 AD-User in Gruppen

Zeigt die AD-User sowie die Gruppen der AD-User als Liste an.

### #204 AD/WinNT - User mit Parametern (Matrix)

Zeigt die AD/WinNT-User, sortiert nach Benutzerkennungen, und deren Attribute an.

ACHTUNG: Es wird von jedem Parameter eines Users immer nur der erste Wert angezeigt. Nutzen Sie zur Anzeige mehrerer Parameter die entsprechenden Reports.

### #205 Letzter RACF-PW-Wechsel jünger als letzte Anmeldung am AD

Der Report zeigt alle User an, deren Passwortwechsel in RACF jünger als die letzte Anmeldung in Windows (AD) ist. Die letzte Anmeldung im AD wird aus dem jüngeren Datum der AD-Variablen lastLogon und lastLogonTimestamp gebildet. Der Download der Daten aus RACF und AD muss vom gleichen Tag sein, sonst kann der Report nicht ausgeführt werden.

WICHTIG: Es werden nur Anmeldungen betrachtet, die Älter als 14 Tage sind, da das AD-Attribut lastLogonTimestamp erst nach 14 Tagen auch definitiv zwischen den Domänen-Controllern repliziert wurde. Ferner werden RACF-Daten derzeit nur Samstags in der IIB aktualisiert.

Erläuterung: lastLogon und lastLogonTimestamp unterscheiden sich dadurch, dass lastLogon nicht zwischen den Domänencontrollern repliziert wird, lastLogonTimestamp schon (allerdings erst nach 9-14 Tagen). Der jüngere Werte ist also der "richtigere", wobei der genaue Wert der letzten Anmeldung in der Domäne tatsächlich erst nach 9-14 Tagen im AD über die Variable lastLogonTimestamp ausgelesen werden kann.

### #206 AD-User mit letztem Passwortwechsel >= X Tage

Zeigt alle User an, die vor mehr als X Tagen zum letzten Mal das Passwort gewechselt haben.

### #207 WinNT-User mit maximaler Passwortwechselzeit >= X Tage

Zeigt alle WinNT-User an, deren Passwort-Wechsel-Zeit länger als X Tage ist.

### #208 Aktive AD-User mit PW-Wechsel oder letzter Anmeldung >= X Tage

Zeigt alle User an, die vor mehr als X Tagen zum letzten Mal das Passwort gewechselt oder sich zum letzten Mal angemeldet haben und deren Konto aktiv ist. Gesperrte Konten und Konten, deren Passwort nie abläuft, werden nicht angezeigt.

### #209 AD-User mit allen Flags

Zeigt alle User an mit ihren Flags an (z.B. Account gesperrt etc.).

SCRIPT - Das Anmeldeskript wird ausgeführt.

### #209 AD-User mit allen Flags

ACCOUNTDISABLE - Das Benutzerkonto wird deaktiviert.

HOMEDIR_REQUIRED - Basisverzeichnis erforderlich.

PASSWD_NOTREQD - Es ist kein Kennwort erforderlich.

PASSWD_CANT_CHANGE - Der Benutzer kann das Kennwort nicht ändern. Dies ist eine Berechtigung für das Objekt des Benutzers. Informationen zur Festlegung dieser Berechtigung per Programm finden Sie auf folgender Website: (http://msdn.microsoft.com/library/default.asp?url=/library/en-us/adsi/adsi/modifying_user_cannot_change_password_ldap_provider.asp)

ENCRYPTED_TEXT_PASSWORD_ALLOWED - Der Benutzer kann ein verschlüsseltes Kennwort senden.

TEMP_DUPLICATE_ACCOUNT - Konto für Benutzer, deren primäres Konto sich in einer anderen Domäne befindet. Dieses Konto gewährt den Zugriff des Benutzers auf diese Domäne, jedoch nicht auf Domänen, die dieser Domäne vertrauen. Dies wird manchmal als "lokales Benutzerkonto" bezeichnet.

NORMAL_ACCOUNT - Standardkontotyp für einen typischen Benutzer.

INTERDOMAIN_TRUST_ACCOUNT - Konto für ein Vertrauenskonto einer Domäne, die anderen Domänen vertraut.

WORKSTATION_TRUST_ACCOUNT - Computerkonto für einen Computer mit Microsoft Windows NT 4.0 Workstation, Microsoft Windows NT 4.0 Server, Microsoft Windows 2000 Professional oder Windows 2000, der Mitglied dieser Domäne ist.

SERVER_TRUST_ACCOUNT - Computerkonto für einen Domänencontroller, der Mitglied dieser Domäne ist.

DONT_EXPIRE_PASSWD - Kennwort, das für dieses Konto nie ablaufen sollte.

MNS_LOGON_ACCOUNT - "Majority Node Set" (MNS) Anmeldekonto. Mit MNS kann man einen "Multi-Node Windows Cluster" konfigurieren, ohne eine "Common Shared Disk" zu verwenden.

SMARTCARD_REQUIRED - Wenn dieses Kennzeichen gesetzt ist, wird der Benutzer gezwungen, sich über eine Smartcard anzumelden.

TRUSTED_FOR_DELEGATION - Wenn dieses Kennzeichen gesetzt ist, wird dem Dienstkonto (dem Benutzer- oder Computerkonto), unter dem ein Dienst ausgeführt wird, für Kerberos-Delegierungszwecke vertraut. Jeder derartige Dienst kann die Identität eines Clients annehmen, der den Dienst anfordert. Sie müssen dieses Flag für die Eigenschaft userAccountControl des Dienstkontos setzen, um einen Dienst für die Kerberos-Delegierung zu aktivieren.

NOT_DELEGATED - Wenn dieses Kennzeichen gesetzt ist, wird der Sicherheitskontext des Benutzers nicht an einen Dienst delegiert, auch dann nicht, wenn das Dienstkonto als "für Delegierungszwecke vertraut" definiert ist.

USE_DES_KEY_ONLY - (Windows 2000/Windows Server 2003) Beschränken Sie diesen Prinzipal auf DES-Verschlüsselungstypen für Schlüssel (DES = Data Encryption Standard).

DONT_REQUIRE_PREAUTH - (Windows 2000/Windows Server 2003) Dieses Konto setzt keine Kerberos-Vorauthentifizierung für die Anmeldung voraus.

PASSWORD_EXPIRED - (Windows 2000/Windows Server 2003) Das Kennwort des Benutzers ist abgelaufen.

TRUSTED_TO_AUTH_FOR_DELEGATION - (Windows 2000/Windows Server 2003) Dem Konto wird für Delegierungszwecke vertraut. Dies ist eine sicherheitskritische Einstellung. Konten, bei denen diese Option aktiviert ist, sollten genau kontrolliert werden. Diese Einstellung ermöglicht einem Dienst, der unter diesem Konto ausgeführt wird, die Identität des Clients anzunehmen

### #210 AD-Kennungen, die keinen Passwortwechsel erfordern

Zeigt alle Kennungen im AD an, bei denen das Passwort nicht geändert werden muss.

SCRIPT - Das Anmeldeskript wird ausgeführt.

### #210 AD-Kennungen, die keinen Passwortwechsel erfordern

ACCOUNTDISABLE - Das Benutzerkonto wird deaktiviert.

HOMEDIR_REQUIRED - Basisverzeichnis erforderlich.

PASSWD_NOTREQD - Es ist kein Kennwort erforderlich.

PASSWD_CANT_CHANGE - Der Benutzer kann das Kennwort nicht ändern. Dies ist eine Berechtigung für das Objekt des Benutzers. Informationen zur Festlegung dieser Berechtigung per Programm finden Sie auf folgender Website: (http://msdn.microsoft.com/library/default.asp?url=/library/en-us/adsi/adsi/modifying_user_cannot_change_password_ldap_provider.asp)

ENCRYPTED_TEXT_PASSWORD_ALLOWED - Der Benutzer kann ein verschlüsseltes Kennwort senden.

TEMP_DUPLICATE_ACCOUNT - Konto für Benutzer, deren primäres Konto sich in einer anderen Domäne befindet. Dieses Konto gewährt den Zugriff des Benutzers auf diese Domäne, jedoch nicht auf Domänen, die dieser Domäne vertrauen. Dies wird manchmal als "lokales Benutzerkonto" bezeichnet.

NORMAL_ACCOUNT - Standardkontotyp für einen typischen Benutzer.

INTERDOMAIN_TRUST_ACCOUNT - Konto für ein Vertrauenskonto einer Domäne, die anderen Domänen vertraut.

WORKSTATION_TRUST_ACCOUNT - Computerkonto für einen Computer mit Microsoft Windows NT 4.0 Workstation, Microsoft Windows NT 4.0 Server, Microsoft Windows 2000 Professional oder Windows 2000, der Mitglied dieser Domäne ist.

SERVER_TRUST_ACCOUNT - Computerkonto für einen Domänencontroller, der Mitglied dieser Domäne ist.

DONT_EXPIRE_PASSWD - Kennwort, das für dieses Konto nie ablaufen sollte.

MNS_LOGON_ACCOUNT - "Majority Node Set" (MNS) Anmeldekonto. Mit MNS kann man einen "Multi-Node Windows Cluster" konfigurieren, ohne eine "Common Shared Disk" zu verwenden.

SMARTCARD_REQUIRED - Wenn dieses Kennzeichen gesetzt ist, wird der Benutzer gezwungen, sich über eine Smartcard anzumelden.

TRUSTED_FOR_DELEGATION - Wenn dieses Kennzeichen gesetzt ist, wird dem Dienstkonto (dem Benutzer- oder Computerkonto), unter dem ein Dienst ausgeführt wird, für Kerberos-Delegierungszwecke vertraut. Jeder derartige Dienst kann die Identität eines Clients annehmen, der den Dienst anfordert. Sie müssen dieses Flag für die Eigenschaft userAccountControl des Dienstkontos setzen, um einen Dienst für die Kerberos-Delegierung zu aktivieren.

NOT_DELEGATED - Wenn dieses Kennzeichen gesetzt ist, wird der Sicherheitskontext des Benutzers nicht an einen Dienst delegiert, auch dann nicht, wenn das Dienstkonto als "für Delegierungszwecke vertraut" definiert ist.

USE_DES_KEY_ONLY - (Windows 2000/Windows Server 2003) Beschränken Sie diesen Prinzipal auf DES-Verschlüsselungstypen für Schlüssel (DES = Data Encryption Standard).

DONT_REQUIRE_PREAUTH - (Windows 2000/Windows Server 2003) Dieses Konto setzt keine Kerberos-Vorauthentifizierung für die Anmeldung voraus.

PASSWORD_EXPIRED - (Windows 2000/Windows Server 2003) Das Kennwort des Benutzers ist abgelaufen.

TRUSTED_TO_AUTH_FOR_DELEGATION - (Windows 2000/Windows Server 2003) Dem Konto wird für Delegierungszwecke vertraut. Dies ist eine sicherheitskritische Einstellung. Konten, bei denen diese Option aktiviert ist, sollten genau kontrolliert werden. Diese Einstellung ermöglicht einem Dienst, der unter diesem Konto ausgeführt wird, die Identität des Clients anzunehmen

### #211 AD-Kennungen, bei denen kein Passwort angegeben werden muss

Zeigt alle Kennungen im AD an, bei denen das Passwort "leer" sein kann. Meist sind diese Konten über Smartcards abgesichert (Anmeldung nur über Smartcard möglich - SMARTCARD_REQUIRED)

### #211 AD-Kennungen, bei denen kein Passwort angegeben werden muss

SCRIPT - Das Anmeldeskript wird ausgeführt.

ACCOUNTDISABLE - Das Benutzerkonto wird deaktiviert.

HOMEDIR_REQUIRED - Basisverzeichnis erforderlich.

PASSWD_NOTREQD - Es ist kein Kennwort erforderlich.

PASSWD_CANT_CHANGE - Der Benutzer kann das Kennwort nicht ändern. Dies ist eine Berechtigung für das Objekt des Benutzers. Informationen zur Festlegung dieser Berechtigung per Programm finden Sie auf folgender Website: (http://msdn.microsoft.com/library/default.asp?url=/library/en-us/adsi/adsi/modifying_user_cannot_change_password_ldap_provider.asp)

ENCRYPTED_TEXT_PASSWORD_ALLOWED - Der Benutzer kann ein verschlüsseltes Kennwort senden.

TEMP_DUPLICATE_ACCOUNT - Konto für Benutzer, deren primäres Konto sich in einer anderen Domäne befindet. Dieses Konto gewährt den Zugriff des Benutzers auf diese Domäne, jedoch nicht auf Domänen, die dieser Domäne vertrauen. Dies wird manchmal als "lokales Benutzerkonto" bezeichnet.

NORMAL_ACCOUNT - Standardkontotyp für einen typischen Benutzer.

INTERDOMAIN_TRUST_ACCOUNT - Konto für ein Vertrauenskonto einer Domäne, die anderen Domänen vertraut.

WORKSTATION_TRUST_ACCOUNT - Computerkonto für einen Computer mit Microsoft Windows NT 4.0 Workstation, Microsoft Windows NT 4.0 Server, Microsoft Windows 2000 Professional oder Windows 2000, der Mitglied dieser Domäne ist.

SERVER_TRUST_ACCOUNT - Computerkonto für einen Domänencontroller, der Mitglied dieser Domäne ist.

DONT_EXPIRE_PASSWD - Kennwort, das für dieses Konto nie ablaufen sollte.

MNS_LOGON_ACCOUNT - "Majority Node Set" (MNS) Anmeldekonto. Mit MNS kann man einen "Multi-Node Windows Cluster" konfigurieren, ohne eine "Common Shared Disk" zu verwenden.

SMARTCARD_REQUIRED - Wenn dieses Kennzeichen gesetzt ist, wird der Benutzer gezwungen, sich über eine Smartcard anzumelden.

TRUSTED_FOR_DELEGATION - Wenn dieses Kennzeichen gesetzt ist, wird dem Dienstkonto (dem Benutzer- oder Computerkonto), unter dem ein Dienst ausgeführt wird, für Kerberos-Delegierungszwecke vertraut. Jeder derartige Dienst kann die Identität eines Clients annehmen, der den Dienst anfordert. Sie müssen dieses Flag für die Eigenschaft userAccountControl des Dienstkontos setzen, um einen Dienst für die Kerberos-Delegierung zu aktivieren.

NOT_DELEGATED - Wenn dieses Kennzeichen gesetzt ist, wird der Sicherheitskontext des Benutzers nicht an einen Dienst delegiert, auch dann nicht, wenn das Dienstkonto als "für Delegierungszwecke vertraut" definiert ist.

USE_DES_KEY_ONLY - (Windows 2000/Windows Server 2003) Beschränken Sie diesen Prinzipal auf DES-Verschlüsselungstypen für Schlüssel (DES = Data Encryption Standard).

DONT_REQUIRE_PREAUTH - (Windows 2000/Windows Server 2003) Dieses Konto setzt keine Kerberos-Vorauthentifizierung für die Anmeldung voraus.

PASSWORD_EXPIRED - (Windows 2000/Windows Server 2003) Das Kennwort des Benutzers ist abgelaufen.

TRUSTED_TO_AUTH_FOR_DELEGATION - (Windows 2000/Windows Server 2003) Dem Konto wird für Delegierungszwecke vertraut. Dies ist eine sicherheitskritische Einstellung. Konten, bei denen diese Option aktiviert ist, sollten genau kontrolliert werden. Diese Einstellung ermöglicht einem Dienst, der unter diesem Konto ausgeführt wird, die Identität des Clients anzunehmen

### #212 WinNT-Kennungen, deren Passwort nicht abläuft

Zeigt alle WinNT-Kennungen an, bei denen das Passwort nie abläuft.

# Berechtigungsreports

## Bereich AD/WinNt

### #213 WinNT-User mit letztem Passwortwechsel >= X Tage

Zeigt alle WinNT-User an, deren letzter Passwort-Wechsel länger als X Tage zurück liegt.

### #214 Gesperrte / deaktivierte Konten

Zeigt alle AD- und WinNT-Konten an, die gesperrt oder deaktiviert sind.

### #215 AD-Kennungen, deren Passwort noch nie geändert wurde

Zeigt alle Kennungen, deren Passwort noch nie verändert wurde (Datum <= 01.01.1900)

### #216 AD-Kennungen ohne Anmeldung

Zeigt alle Kennungen die sich noch nie angemeldet haben (Datum <= 01.01.1900)

### #250 AD-User ohne KURS-User

Zeigt AD-User an, die in KURS keinen User haben.

ACHTUNG: Bitte bedenken Sie, dass das KURS-Datum und das AD-Download-Datum voneinander abweichen können! Es kann also durchaus sein, dass Sie unterschiedliche Zeiträume betrachten!

### #252 AD-User ohne WinNT-User

Zeigt AD-User an, die in WinNT keinen User haben.

### #253 WinNT-User ohne AD-User

Zeigt WinNT-User an, die in AD keinen User haben.

### #254 WinNT-User ohne KURS-User

Zeigt WinNT-User an, die in KURS keinen User haben.

ACHTUNG: Bitte bedenken Sie, dass das KURS-Datum und das WinNT-Download-Datum voneinander abweichen können! Es kann also durchaus sein, dass Sie unterschiedliche Zeiträume betrachten!

# Berechtigungsreports

## Bereich Berechtigungen

### #2 Anzahl zugewiesene Profile / Berechtigungen

Der Report zeigt in Zahlen an, wie viele Berechtigungen / Profile wo (OE, Stelle, Mitarbeiter) zugewiesen wurden.

### #3 Profile / Berechtigungen - Soll/Ist-Matrix (Excel)

Erzeugt einen Excel-Report, bei dem alle Berechtigungen und Profile in einer Matrix angezeigt werden (ohne Feindefinitionen, Eigenschaften/Kompetenzen). Ab Version 1.3 wird zusätzlich eine Matrix für zugewiesene Profile und direkt zugewiesene Berechtigungen an Stellen, OEs und Mitarbeitern angezeigt. Die Mitarbeiter werden mit der Rolle PLANSTELLE ausgewertet. Es werden ausschließlich Profile der Profilart 0 (Berechtigungsprofil) berücksichtigt.

Differenzen zwischen Soll und ist werden wie folgt dargestellt:

I (rot): Berechtigung im Ist vorhanden, nicht aber im SOLL
S (orange): Berechtigung im Soll vorhanden, nicht aber im IS
IS (grau): Übereinstimmung

Zu Attributen (z.B. Ändern / Löschen) werden Texteinträge erzeugt, z.B. 'KURS_ADMI (Ä)'.

### #4 Anzahl zugewiesene Profile / Berechtigungen mit Details

Der Report zeigt in Zahlen an, wie viele Berechtigungen / Profile wo (OE, Stelle, Mitarbeiter) zugewiesen wurden. Zusätzlich werden noch die Objekte (OE, Stelle, Mitarbeiter) aufgeführt, denen die Berechtigungen / Profile zugewiesen wurden. Berechtigungen in Profilen werden in diesem Report nicht angezeigt.

### #5 OE / Mitarbeiter / Berechtigungen / Feindefinitionen

Der Report zeigt alle Berechtigungen einzelner Mitarbeiter inklusive Feindefinitionen an, und zwar nach der OE sortiert.

Technischer User RZ erben keine Berechtigungen des Instituts oder von Stellen / OEs.

Hinweis: Der Report zeigt administrierte konkurrierende Berechtigungen farbig an, wenn sowohl die führende Berechtigung als auch die abhängige konkurrierende Berechtigung nicht durch Filterung im Report ausgeschlossen wurden.

### #6 Profile / Berechtigungen / Feindefinitionen / Eigenschaften

Der Report erzeugt eine Übersicht aller Profile und den darin enthaltenen Berechtigungen inkl. Kompetenzen.

### #7 Mitarbeiter / Abgelaufene Profile

Hier werden alle Profile, die in Mitarbeiter in der Vergangenheit hatte, die ihm aber inzwischen wieder entzogen wurden, angezeigt.

### #8 OE / Mitarbeiter / Berechtigungen

Der Report zeigt alle Berechtigungen einzelner Mitarbeiter an, und zwar nach der OE sortiert. Feindefinitionen und Eigenschaften werden nicht angezeigt.

Technischer User RZ erben keine Berechtigungen des Instituts oder von Stellen / OEs.

Hinweis: Der Report zeigt administrierte konkurrierende Berechtigungen farbig an, wenn sowohl die führende Berechtigung als auch die abhängige konkurrierende Berechtigung nicht durch Filterung im Report ausgeschlossen wurden.

### #9 Entzogene Berechtigungen nach Datum

Zeigt alle Berechtigungen, die ablaufen bzw. bereits abgelaufen sind, an. So kann man z.B. prüfen, ob Berechtigungen terminiert sind; wenn man beispielsweise das heutige Datum eingibt, sieht man, welche Profile zukünftig ablaufen.

### #10 Direkt an Mitarbeiter vergebene Berechtigungen

In OSP ist es möglich, Mitarbeitern direkt Berechtigungen zuzuweisen (also nicht über Profile). Dieser Report zeigt alle Berechtigungen inkl. Feindefinitionen / Eigenschaften / Kompetenzen, die direkt an einen Mitarbeiter vergeben sind.

### #11 Direkt vergebene Berechtigungen inkl. Eigenschaften

In OSP ist es möglich, Mitarbeitern, Stellen und OEs direkt Berechtigungen zuzuweisen (also nicht über Profile). Dieser Report zeigt alle Berechtigungen, die direkt vergeben wurden.

# Berechtigungsreports

## Bereich Berechtigungen

### #11 Direkt vergebene Berechtigungen inkl. Eigenschaften

### #13 MA / alle Stellen / Berechtigungen / FDef / Eigenschaften

Der Report zeigt alle Berechtigungen einzelner Mitarbeiter inklusive Feindefinitionen und Eigenschaften / Kompetenzen an. Pro Mitarbeiter werden alle Berechtigungen dargestellt, die sich für Stellen, auf der sich der Mitarbeiter anmelden kann, ergeben.

Technischer User RZ erben keine Berechtigungen des Instituts oder von Stellen / OEs.

Hinweis: Der Report zeigt administrierte konkurrierende Berechtigungen farbig an, wenn sowohl die führende Berechtigung als auch die abhängige konkurrierende Berechtigung nicht durch Filterung im Report ausgeschlossen wurden.

### #14 FDef / MA / alle Stellen / Berechtigungen / Eigenschaften

Der Report zeigt alle Berechtigungen einzelner Mitarbeiter, bei denen Feindefinitionen zugewiesen sind, an und zwar nach Feindefinitionen sortiert. Zusätzlich werden pro Mitarbeiter die Feindefinitionen / Berechtigungen dargestellt, die sich für Stellen, auf der sich der Mitarbeiter anmelden kann, ergeben.

### #15 Zeitraum: MA / alle Stellen / Berechtigungen / F-Def / Eig.

ACHTUNG: Dieser Report sollte nur mit einzelnen Berechtigungen genutzt werden; da er Daten über einen Zeitraum hinweg darstellt, kann er sehr mächtig werden. Mit diesem Report kann z.B. geprüft werden, ob Mitarbeiter in einem gegebenen Zeitraum zu irgend einem Zeitpunkt eine bestimmte Berechtigung hatten.

Der Report zeigt alle Berechtigungen einzelner Mitarbeiter inklusive Feindefinitionen und Eigenschaften / Kompetenzen an in einem bestimmten Zeitraum an. Pro Mitarbeiter werden alle Berechtigungen dargestellt, die sich für Stellen, auf der sich der Mitarbeiter anmelden kann, ergeben.

Berechtigungen / Profile / Stellenzuordnungen (von Profilen oder Berechtigungen), die im gegebenen Zeitraum Ihre Gültigkeit verloren / gewonnen haben, werden gesondert im Report markiert.

Technischer User RZ erben keine Berechtigungen des Instituts oder von Stellen / OEs.

Hinweis: Der Report zeigt administrierte konkurrierende Berechtigungen farbig an, wenn sowohl die führende Berechtigung als auch die abhängige konkurrierende Berechtigung nicht durch Filterung im Report ausgeschlossen wurden.

### #16 Hinzugefügte und entzogene Feindefinitionen

Zeigt alle hinzugefügten und entzogenen Feindefinitionen in einem bestimmten Zeitraum, nach Datum sortiert, an.

### #17 Profile mit Negierungen

Der Report erzeugt eine Übersicht aller Profile, in denen Negierungen enthalten sind.

### #23 Entzogene Berechtigungen nach Mitarbeitern

Zeigt alle Berechtigungen von Mitarbeitern an, die ablaufen bzw. bereits abgelaufen sind, an. So kann man z.B. prüfen, ob Berechtigungen terminiert sind, und zwar nach Namen sortiert; wenn man beispielsweise das heutige Datum eingibt, sieht man, welche Profile zukünftig ablaufen.

### #26 Berechtigungen / Anzahl Mitarbeiter

Der Report zeigt die zu einem bestimmten Zeitpunkt vergebenen Berechtigungen mit der Anzahl der Mitarbeiter, die diese Berechtigungen besitzen, an. "Geerbte" Berechtigungen (z.B. von Stellen) werden hier mit berücksichtigt. Ferner zeigt der Report die Anzahl der Mitarbeiter differenziert nach dem Attribut "Negiert" an.

### #28 Profile / Berechtigungen - Ist-Matrix (Excel)

Erzeugt einen Excel-Report, bei dem alle Berechtigungen und Profile in einer Matrix angezeigt werden. Ab Version 1.3 wird zusätzlich eine Matrix für zugewiesene Profile und direkt zugewiesene Berechtigungen an Stellen, OEs und Mitarbeitern angezeigt. Die Mitarbeiter werden mit der Rolle PLANSTELLE ausgewertet. Es werden ausschließlich Profile der Profilart 0 (Berechtigungsprofil) berücksichtigt.

Zusätzlich wird bei allen Berechtigungen, die etwa Einzelaspekte wie 'Löschen' oder 'Ändern' gesetzt haben, Zusatzinformationen erzeugt. Wenn beispielsweise bei KURS_ADMI 'Ändern' individuell festgelegt wurde, erzeugt das

### #28 Profile / Berechtigungen - Ist-Matrix (Excel)

Programm einen Eintrag mit dem Text 'KURS_ADMI (Ä)'.

### #29 Profile / Berechtigungen - Soll/Ist-Matrix (Excel, filterbar)

Erzeugt einen Excel-Report, bei dem alle Berechtigungen und die selektierten Profile in einer Matrix angezeigt werden (ohne Feindefinitionen, Eigenschaften/Kompetenzen). Zusätzlich wird eine Matrix für zugewiesene Profile und direkt zugewiesene Berechtigungen an Stellen, OEs und Mitarbeitern angezeigt. Die Mitarbeiter werden mit der Rolle PLANSTELLE ausgewertet. Es werden ausschließlich Profile der Profilart 0 (Berechtigungsprofil) berücksichtigt.

Die Übersicht für Profile / Privilegien kann nach Profilen gefiltert werden, die OE-Übersicht wird vollständig angezeigt. ACHTUNG: SOLL-Profile die im aktuellen IST-Bestand nicht mehr vorhanden sind (also z.B. alte Profile, die inzwischen gelöscht wurden) sind NICHT filterbar und werden auch NICHT angezeigt. Wenn alle gelöschten SOLL-Profile angezeigt werden sollten muss der Report #3 verwendet werden.

Differenzen zwischen Soll und ist werden wie folgt dargestellt:

I (rot): Berechtigung im Ist vorhanden, nicht aber im SOLL
S (orange): Berechtigung im Soll vorhanden, nicht aber im IS
IS (grau): Übereinstimmung

Zu Attributen (z.B. Ändern / Löschen) werden Texteinträge erzeugt, z.B. 'KURS_ADMI (Ä)'.

### #31 OE / Mitarbeiter / negierte Berechtigungen

Der Report zeigt alle negierten Berechtigungen einzelner Mitarbeiter an, und zwar nach der OE sortiert.

### #32 Kompetenzen / Eigensch. / MA / alle Stellen / Berechtigungen

Der Report zeigt alle Berechtigungen einzelner Mitarbeiter, denen Eigenschaften / Kompetenzen zugewiesen sind, an und zwar nach Eigenschaft sortiert. Zusätzlich werden pro Mitarbeiter die Eigenschaften / Kompetenzen dargestellt, die sich für Stellen des Filters 'OE-Stellen-Zuordnungsart', ergeben. Berechtigungen ohne Eigenschaften / Kompetenzen werden nicht angezeigt.

### #33 Profilabweichungen

Der Report zeigt die Anzahl der Abweichungen aller Profile untereinander an. Dadurch lassen sich Redundanzen bzw. geringfügige Abweichungen identifizieren, die dann durch Anpassung der Profile aufgehoben werden können. Der Report berücksichtigt Attribute, alle Feindefinitionen sowie alle zugewiesenen Eigenschaften.

Geben Sie hier die maximalen Anzahl der Unterschiede zwischen Profilen an, die angezeigt werden sollen. Wenn Sie 2 Profile (oder auch mehrere einzelne) vergleichen wollen, geben Sie am besten einen sehr hohen Wert für "Anzahl" an, damit die Unterschiede auch im Report aufgeführt werden.

Je höher "Anzahl" (bei Selektion aller Profile), um so länger dauert die Berechnung, da jedes Profil mit jedem verglichen wird und erst bei "Anzahl" Unterschieden der Vergleich abgebrochen wird.

Als 1 Unterschied gilt: 1 Berechtigung, 1 bis alle Attribute einer Berechtigung, 1 Feindefinition, 1 bis alle Attribute auf Feindefinitionsebene, 1 Eigenschaft

### #34 Profile OHNE bestimmte Berechtigungen

Der Report zeigt Profile an, in denen bestimmte Berechtigungen NICHT vorhanden sind.

### #35 Profile ohne Berechtigungen

Der Report zeigt alle Profile an, denen überhaupt keine Berechtigungen zugeordnet sind. Es werden keine Menüprofile mit ausgegeben.

### #36 Direkt zugewiesene Profile mit weniger als X Mitarbeitern

Der Report zeigt Profile an, die weniger als X Mitarbeitern direkt zugewiesen sind. (OE- und Stellen-Zuweisungen werden nicht berücksichtigt)

### #37 OE / MA / Berechtigungen / Feindefinitionen / Eigenschaften

Der Report zeigt alle Berechtigungen einzelner Mitarbeiter inklusive Feindefinitionen an, und zwar nach der OE sortiert.

# Berechtigungsreports

## Bereich Berechtigungen

### #37 OE / MA / Berechtigungen / Feindefinitionen / Eigenschaften

Zusätzliche werden alle zugeschlüsselten Eigenschaften wie z.B. Kompetenzen angezeigt.

Technischer User RZ erben keine Berechtigungen des Instituts oder von Stellen / OEs.

Hinweis: Der Report zeigt administrierte konkurrierende Berechtigungen farbig an, wenn sowohl die führende Berechtigung als auch die abhängige konkurrierende Berechtigung nicht durch Filterung im Report ausgeschlossen wurden.

### #43 OE-Übersicht der Profile und direkt. zug. Berechtigungen

Der Report zeigt alle Profile und direkt zugewiesenen Berechtigungen der selektierten Orgeinheiten und der darin enthaltenen Stellen an. Es werden nur die Orgeinheiten und Stellen angezeigt, denen auch Profile oder Berechtigungen zugewiesen wurden.

### #44 Mitarbeiter mit negierten und nicht negierten Berecht.

Der Report zeigt Zuweisungen bestimmter Berechtigungen zu einem bestimmbaren Zeitpunkt an, die einer Person direkt oder über Vererbung (über Profil, Stelle oder OE) zugewiesen wurden. Dabei werden nur solche User angezeigt, die gleichzeitig eine Berechtigung mit Negierung und ohne Negierung erhalten. Der Report zeigt nur Mitarbeiter an, die Stellen über Rollen (z.B. HIER TÄTIG, PLANSTELLE) auch tatsächlich zugewiesen sind.

Das Institutsprofil wird hier nicht gesondert berücksichtigt, da es allen Mitarbeitern zugeschlüsselt ist (nutzen Sie hierfür ggf. Report #6).

### #46 Personen, die Profile über mehrere Ursprünge erhalten

Profilgruppen gibt es in OSP selbst nicht. Eine Profilgruppe stellt die Summe aller Profile dar, die einem Mitarbeiter zugewiesen sind. Sollte ein anderer Mitarbeiter die gleichen Profile besitzen, so gehört er zur gleichen Profilgruppe.

Im Report werden solche Personen angezeigt, die ein Profil über unterschiedliche Ursprünge (Mitarbeiter, Stelle, OE) erhalten haben.

Der Report wertet alle Profile aus, auch solche, die an der Stelle oder an der OE hängen aus. Da der Mitarbeiter an einem Tag auf mehreren Stellen zugeordnet sein (wenn er z.B. den Platz wechselt wie bei Springern), stellt dies nur die Profilgruppen der angegebenen "Sekunde" dar.

### #48 Hinzugefügte Berechtigungen nach Datum

Zeigt alle Berechtigungen, die in einem bestimmten Zeitraum vergeben wurden.

### #49 Hinzugefügte Berechtigungen nach Mitarbeitern

Zeigt alle Berechtigungen nach Mitarbeiternamen sortiert an, die in einem bestimmten Zeitraum vergeben wurden.

### #50 Berechtigungen an Mitarbeitern / Profilen / Stellen / OEs

Der Report zeigt Zuweisungen bestimmter Berechtigungen zu einem bestimmbaren Zeitpunkt an, die einer Person direkt oder über Vererbung (über Profil, Stelle oder OE) zugewiesen wurden. Der Report zeigt nur Mitarbeiter an, die Stellen über Rollen (z.B. HIER TÄTIG, PLANSTELLE) auch tatsächlich zugewiesen sind.

Das Institutsprofil wird hier nicht gesondert berücksichtigt, da es allen Mitarbeitern zugeschlüsselt ist (nutzen Sie hierfür Report #86, dort wird zusätzlich das Institutsprofil mit ausgegeben).

### #52 Profile an Mitarbeitern / Stellen / OEs

Der Report zeigt alle Zuweisungen bestimmter Profile zu einem Zeitpunkt an, die einer Person, einer Stelle oder einer OE direkt oder indirekt zugewiesen wurde.

Hinweis: Es werden nur solche Oes und Stellen angezeigt, denen auch User über die eingestellte Zuordnungsart zugewiesen sind. Wenn z.B. in den Stellen einer OE keine User zugewiesen ist, wird die OE nicht aufgeführt. Nutzen Sie dafür den Report #53.

### #53 OE / Stelle / Profil / Berechtigungen

Der Report zeigt alle über die OE / Stelle und dort zugeordnete Profile / Berechtigungen.

# Berechtigungsreports

## Bereich Berechtigungen

### #54 Nirgends zugewiesene Profile

Der Report zeigt Profile an, die aktuell nicht verwendet werden. Es werden Berechtigungsprofile (IST), Menüprofile und Funktionsprofile (SOLL) angezeigt.

### #55 Profil- / Berechtigungsvergleich Mitarbeiter

Vergleicht die zugewiesenen Berechtigungen und Profile zweier Mitarbeiter. Attribute auf Feindefinitionsebene oder Eigenschaften werden nicht berücksichtigt.

### #58 Hinzugefügte und entzogene Berechtigungen nach Datum

Zeigt alle hinzugefügten und entzogenen Berechtigungen in einem bestimmten Zeitraum, nach Datum sortiert, an.

### #59 Hinzugefügte und entzogene Berechtigungen nach Mitarbeitern

Zeigt alle Berechtigungen und Profile nach Mitarbeiternamen sortiert an, die in einem bestimmten Zeitraum vergeben oder entzogen wurden.

### #60 Änderungsbearbeitung für das Gesamthaus und alle TIDs

Der Report zeigt alle User an, die für das Gesamthaus (OE 0000000 bis 9999999) alle Tätigkeits-ID (00000 bis 99999) prüferisch tätig sein können (Berechtigung: AEND-BEARB). Über den OE-Stellen-Zuordnungsart kann festgelegt werden, welche Zuordnungsarten angezeigt werden.

### #69 Direkt an Mitarbeiter vergebene Profile

Dieser Report zeigt alle Profile an, die direkt an einen Mitarbeiter vergeben sind.

### #75 OSP-Funktionsprofile / Berechtigungen / Fdef. / Eigenschaften

Der Report erzeugt eine Übersicht aller Funktionsprofile und den darin enthaltenen Berechtigungen inkl. Kompetenzen.

### #78 Abweichungen OSP-Funktionsprofile / Ist-Profile nach Profilnr.

Der Report vergleicht die aktuell eingestellten Funktionsprofile in KURS mit den IST-Profilen und zeigt ausschließlich Abweichungen an. Es wird nach Profilnummern verglichen.

### #79 User mit direkt zugewiesenen negierten Berechtigungen

Der Report erzeugt eine Übersicht aller User, denen direkt negierte Berechtigungen zugewiesen wurden.

### #81 Kompetenzen / Eigensch. / MA / nur PLANSTELLE / Berechtigungen

Der Report zeigt alle Berechtigungen einzelner Mitarbeiter, bei denen Eigenschaften / Kompetenzen zugewiesen sind, an und zwar nach Eigenschaft sortiert. Es wurden nur die PLANSTELLEN angezeigt. Berechtigungen ohne Eigenschaften / Kompetenzen werden nicht angezeigt.

### #84 Eigenschaften von Anwendungssystemen

Zeigt die Eigenschaften von Anwendungssystemen, für die in KURS Rechte vergeben werden können, an..

### #85 Zuordnung von Anwendungssystemen zu Berechtigungen

Zeigt alle Berechtigungen an, die ein Anwendungssystem zur Verfügung stellt.

### #86 Berechtigungen an MA / Profilen / Stellen / Oes inkl. Inst-Prof

Der Report zeigt Zuweisungen bestimmter Berechtigungen zu einem bestimmbaren Zeitpunkt an, die einer Person direkt oder über Vererbung (über Profil, Stelle oder OE) zugewiesen wurden. Der Report zeigt nur Mitarbeiter an, die Stellen über Rollen (z.B. HIER TÄTIG, PLANSTELLE) auch tatsächlich zugewiesen sind.

### #87 Hinzugefügte / entzogene Eigenschaften / Kompetenzen

Der Report zeigt hinzugefügte und entfernte Kompetenzen / Eigenschaften in einem bestimmten Zeitraum an.

### #88 Konkurrierende Berechtigungen

Zeigt eine Liste der konkurrierenden Berechtigungen an. Konkurrierende Berechtigungen wirken sich nur auf Berechtigungen aus, die das Attribut Ändern gesetzt haben.

Der Berechtigungs-Filter wirkt auf die führende Berechtigung.

# Berechtigungsreports

## Bereich Berechtigungen

### #88 Konkurrierende Berechtigungen

### #89 Hinzugefügte / entzogene konkurrierende Berechtigungen

Zeigt eine Liste hinzugefügter und entzogener konkurrierenden Berechtigungen in einem bestimmbaren Zeitraum an. Konkurrierende Berechtigungen wirken sich nur auf Berechtigungen aus, die das Attribut Ändern gesetzt haben.

### #90 OE / MA / Profile + direkt zugewiesene Berechtigungen

Der Report zeigt alle Profile von Mitarbeitern sowie die direkt zugewiesenen Berechtigungen inklusive Feindefinitionen an, und zwar nach der OE sortiert. Zusätzliche werden alle zugeschlüsselten Eigenschaften wie z.B. Kompetenzen angezeigt. Alle ggf. mehrfach direkt zugewiesene Berechtigungen (z.B an Stelle und User) werden angezeigt. Menüprofile werden nicht angezeigt.

Technischer User RZ erben keine Berechtigungen des Instituts oder von Stellen / OEs.

Hinweis: Konkurrierende Berechtigungen können in diesem Report nicht berücksichtigt werden, da nur die Profile und nicht die Einzelberechtigungen ausgegeben werden!

### #91 Kompetenz- und Eigenschaftenanzahl

Der Report zeigt gruppiert nach der Anzahl der Bediener beim 4-Augen-Prinzip an, wie häufig Unter- und Obergrenzen von Kompetenzen vergeben wurden. Es werden ausschließlich Kompetenzen von Planstellen mit Mitarbeitern berücksichtigt. Negierte Berechtigungen werden nicht angezeigt!

Wenn beispielsweise für die Berechtigung INL-LASTSCH in unterschiedlichen AZs Kompetenzen vergeben wurden, so zeigt dieser Report dann die Unter- und Obergrenzen der Kompetenzen in den einzelnen AZs an.

### #92 Summen der Profile pro Berechtigungsträger

Der Report zeigt die Summen aller Zuweisungen bestimmter Profile zu einem Zeitpunkt an User an, die einer Person, einer Stelle oder einer OE direkt oder indirekt zugewiesen wurde. Bei OE und Stelle wird immer die Useranzahl ausgegeben, die über eine OE oder eine Stelle ein Profil erhält.

Hinweis: Es werden nur solche Oes und Stellen berücksichtigt, denen auch User über die eingestellte Zuordnungsart zugewiesen sind. Wenn z.B. in den Stellen einer OE keine User zugewiesen ist, wird die OE nicht aufgeführt.

### #93 Art des Berechtigungsträgers / Berechtigungsträger / Profil

Der Report zeigt die Berechtigungsträger mit ihren Profilen, gruppiert nach Berechtigungsart, an. Es wird die Anzahl der Profilzuweisungen gezählt, erhalten mehrere User über eine OE oder Stelle das gleiche Profil, so wird das Profil nur ein mal gezählt.

Hinweis: Es werden nur solche Oes und Stellen berücksichtigt, denen auch User über die eingestellte Zuordnungsart zugewiesen sind. Wenn z.B. in den Stellen einer OE keine User zugewiesen ist, wird die OE nicht aufgeführt.

### #94 Genehmigungen für das Gesamthaus und alle TIDs

Der Report zeigt alle User an, die für das Gesamthaus (OE 0000000 bis 9999999) alle Tätigkeits-ID (00000 bis 99999) Genehmigungen von Berechtigungsvorgängen durchführen können (Berechtigung: KURS_GENEHM). Über den OE-Stellen-Zuordnungsart kann festgelegt werden, welche Zuordnungsarten angezeigt werden.

### #95 Kompetenz- und Eigenschaftenanzahl ohne Unter- und Obergrenze 1

Der Report zeigt gruppiert nach der Anzahl der Bediener beim 4-Augen-Prinzip an, wie häufig Unter- und Obergrenzen von Kompetenzen vergeben wurden. Es werden ausschließlich Kompetenzen von Planstellen mit Mitarbeitern berücksichtigt. Negierte Berechtigungen sowie die Unter- und Obergrenze 1 werden nicht angezeigt!

Wenn beispielsweise für die Berechtigung INL-LASTSCH in unterschiedlichen AZs Kompetenzen vergeben wurden, so zeigt dieser Report dann die Unter- und Obergrenzen der Kompetenzen in den einzelnen AZs an.

### #97 Abweichungen OSP-Funktionsprofile / Ist-Profile nach Profilname

Der Report vergleicht die aktuell eingestellten Funktionsprofile in KURS mit den IST-Profilen und zeigt ausschließlich Abweichungen an. Es wird nach Profilnamen verglichen (nur Bezeichnung 1). Profile mit einer Profilnummer >= 999900000000 und Profile, deren Profilname mit Musterprofil beginnt, werden nicht mit berücksichtigt.

### #98 Berechtigungsübersicht nach OEs

# Berechtigungsreports

## Bereich Berechtigungen

### #98 Berechtigungsübersicht nach OEs

Der Report zeigt die Berechtigungen, Feindefinitionen und Eigenschaften / Kompetenzen der User einer OE inklusive ihrer Stellen an. Dabei werden solche User zusammengefasst dargestellt, deren Berechtigungen identisch sind, unabhängig davon, über welchen Ursprung die User die Berechtigung erhalten (z.B. über eine OE, eine Stelle oder ein Profil). Wenn keine Attribute setzbar sind und Negiert auf N steht werden die Attribute nicht mit ausgegeben.

ACHTUNG: Bitte prüfen Sie vor Ausführung die Zuordnungsart (HIER_TÄTIG, PLANSTELLE etc.)!!!

Sie können diesen Report verwenden, um einzelne OEs bezüglich der aktuellen Rechtevergabe zu validieren bzw. die Rezertifizierung im Sinne der MaRisk durchzuführen. Durch die "komprimierte" Anzeige (gleiche Berechtigungen aller User einer OE werden voran gestellt) wird der Abstimmaufwand reduziert. Ferner können Sie sich durch die Zusammenfassung der User in Gruppen einen Überblick darüber verschaffen, welche User ein gleichartiges Kompetenz- und Rechtegfüge aufweisen.

Sollten User mit gleichen Funktionen / Stellenbeschreibungen in unterschiedlichen Gruppen erscheinen, so wäre zu prüfen, warum und wie sich diese User von den Usern der anderen Gruppe unterscheiden und ob dies sachgerecht ist.

Der Report berücksichtigt die die Berechtigungskategorisierung des R4Plus, vorausgesetzt diese wurde importiert. Dies gibt Ihnen die Möglichkeit, den Report auf risikorelevante Berechtigungen zu reduzieren.

ACHTUNG: Im Normalfall können Sie das Instituts-Profil hier ausschließen! Bitte wählen Sie im Reiter KURS-Details die für Sie relevanten Berechtigungsträger aus.

### #99 Direkt an Mitarbeiter vergebene Berechtigungen nach OE

In OSP ist es möglich, Mitarbeitern direkt Berechtigungen zuzuweisen (also nicht über Profile). Dieser Report zeigt alle Berechtigungen inkl. Feindefinitionen / Eigenschaften / Kompetenzen an, die direkt an einen Mitarbeiter vergeben sind. Die Ausgabe wird nach OE (3 Stellen) sortiert.

### #100 Berechtigungen / Anzahl Mitarbeiter / R4Plus-Erläuterung

Der Report zeigt die zu einem bestimmten Zeitpunkt vergebenen Berechtigungen mit der Anzahl der Mitarbeiter, die diese Berechtigungen besitzen, an. "Geerbte" Berechtigungen (z.B. von Stellen) werden hier mit berücksichtigt. Ferner zeigt der Report die Anzahl der Mitarbeiter differenziert nach dem Attribut "Negiert" an.

Falls der R4Plus-Rahmen importiert wurde werden die R4Plus-Informationen mit ausgegeben.

Sie können in diesem Report auch nach User-Typen filtern, sodass Sie gezielt auch technische User abfragen können. Bitte beachten Sie, dass nur User angezeigt werden, die auch per Zuordnungsart Stellen zugeordnet sind.

### #101 Nicht verwendete Berechtigungen

Der Report zeigt alle in OPS sichtbaren Berechtigungen an, die zum gewählten Zeitpunkt NICHT verwendet werden. Berechtigungen an Stellenfunktionen bzw. Funktionsprofilen werden ausgenommen, d.h. wenn Berechtigungen ausschließlich Stellenfunktionen bzw. Funktionsprofilen zugewiesen sind, gelten diese als "nicht verwendet".

### #102 Berechtigungsübersicht für mehrere Oes

Der Report zeigt die Berechtigungen, Feindefinitionen und Eigenschaften / Kompetenzen der User mehrerer OEs inklusive ihrer Stellen an. Dabei werden solche User zusammengefasst dargestellt, deren Berechtigungen identisch sind, unabhängig davon, über welchen Ursprung die User die Berechtigung erhalten (z.B. über eine OE, eine Stelle oder ein Profil). Wenn keine Attribute setzbar sind und Negiert auf N steht werden die Attribute nicht mit ausgegeben.

ACHTUNG: Bitte prüfen Sie vor Ausführung die Zuordnungsart (HIER_TÄTIG, PLANSTELLE etc.)!!!

Sie können diesen Report verwenden, um mehrere OEs bezüglich der aktuellen Rechtevergabe zu validieren (z.B. mehrere Markt-Oes) bzw. die Rezertifizierung im Sinne der MaRisk durchzuführen. Durch die "komprimierte" Anzeige (gleiche Berechtigungen aller User einer OE werden voran gestellt) wird der Abstimmaufwand reduziert. Ferner können Sie sich durch die Zusammenfassung der User in Gruppen einen Überblick darüber verschaffen, welche User ein gleichartiges Kompetenz- und Rechtegfüge aufweisen.

Sollten User mit gleichen Funktionen / Stellenbeschreibungen in unterschiedlichen Gruppen erscheinen, so wäre zu prüfen, warum und wie sich diese User von den Usern der anderen Gruppe unterscheiden und ob dies sachgerecht ist.

Der Report berücksichtigt die die Berechtigungskategorisierung des R4Plus, vorausgesetzt diese wurde importiert. Dies

# Berechtigungsreports

## Bereich Berechtigungen

### #102 Berechtigungsübersicht für mehrere Oes

gibt Ihnen die Möglichkeit, den Report auf risikorelevante Berechtigungen zu reduzieren.

ACHTUNG: Im Normalfall können Sie das Instituts-Profil hier ausschließen! Bitte wählen Sie im Reiter KURS-Details die für Sie relevanten Berechtigungsträger aus.

### #103 Technische User inkl. Änderungsvorgangsprüfkennzeichen

Der Report zeigt die technischen User an.

Das Merkmal "Änderungsvorgänge in der Änderungs-DB prüffrei stellen bzw. im Kontrollradar berücksichtigen" kann folgende Werte haben:
norm-mKR = normale Prüfung, mit Kontrollradar
prüffrei-oKR = prüffrei, ohne Kontrollradar
prüffrei-mKR = prüffrei, mit Kontrollradar
norm-oKR = normale Prüfung, ohne Kontrollradar

### #104 Stellen mit Profilen, Funktionsprof. und direkt. zug. Berecht.

Der Report zeigt alle Profile, Funktionsprofile und direkt zugewiesenen Berechtigungen der Stellen (Soll und Ist) und Usern (Ist der PLANSTELLE) der selektierten Orgeinheiten an. Es werden nur Stellen angezeigt, denen auch Profile oder Berechtigungen zugewiesen wurden.

### #105 Stellenfunktionen ohne Stellen

Der Report zeigt alle Stellenfunktionen an, die keiner Stelle zugewiesen sind.

### #106 Stellenfunktionen ohne Inhalte

Der Report zeigt alle Stellenfunktionen an, die keine zugewiesenen Berechtigungen oder Profile haben.

### #107 Funktionsprofile ohne Berechtigungen

Der Report zeigt alle Funktionsprofile an, denen überhaupt keine Berechtigungen zugeordnet sind.

### #108 Nirgends zugewiesene Funktionsprofile

Der Report zeigt Funktionsprofile an, die aktuell nicht verwendet werden.

### #109 Soll/Ist-Vergleich nach Stellen

Vergleicht das SOLL einer Stelle mit dem IST. Hierbei werden die Berechtigungen des Mitarbeiters, der eine Planstelle besetzt, mit den Soll-Werten der Stellenfunktion verglichen.

### #110 Soll-Berechtigungsübersicht nach Oes

Der Report zeigt die Soll-Berechtigungen, -Feindefinitionen und -Eigenschaften / -Kompetenzen der User einer OE inklusive ihrer Stellen an. Dabei werden solche User zusammengefasst dargestellt, deren Soll-Berechtigungen identisch sind. Wenn keine Attribute setzbar sind und Negiert auf N steht werden die Attribute nicht mit ausgegeben.

ACHTUNG: Bitte prüfen Sie vor Ausführung die Zuordnungsart (HIER_TÄTIG, PLANSTELLE etc.)!!!

Sie können diesen Report verwenden, um einzelne OEs bezüglich der aktuellen Soll-Rechtevergabe zu validieren bzw. die Rezertifizierung im Sinne der MaRisk durchzuführen. Durch die "komprimierte" Anzeige (gleiche Berechtigungen aller User einer OE werden voran gestellt) wird der Abstimmaufwand reduziert. Ferner können Sie sich durch die Zusammenfassung der User in Gruppen einen Überblick darüber verschaffen, welche User ein gleichartiges Kompetenz- und Rechtegfüge aufweisen. Der Report lässt sich sehr gut mit Report #109 kombinieren: Nutzen Sie 110 um das Soll zu rezertifiziereund und 109 um dann den Soll-Ist-Abgleich durchzuführen.

Sollten User mit gleichen Funktionen / Stellenbeschreibungen in unterschiedlichen Gruppen erscheinen, so wäre zu prüfen, warum und wie sich diese User von den Usern der anderen Gruppe unterscheiden und ob dies sachgerecht ist.

Der Report berücksichtigt die die Berechtigungskategorisierung des R4Plus, vorausgesetzt diese wurde importiert. Dies gibt Ihnen die Möglichkeit, den Report auf risikorelevante Berechtigungen zu reduzieren.

### #111 Soll-Berechtigungsübersicht für mehrere Oes

Der Report zeigt die Soll-Berechtigungen, Feindefinitionen und Eigenschaften / Kompetenzen der User mehrerer OEs

# Berechtigungsreports

## Bereich Berechtigungen

### #111 Soll-Berechtigungsübersicht für mehrere Oes

inklusive ihrer Stellen an. Dabei werden solche User zusammengefasst dargestellt, deren Soll-Berechtigungen identisch sind. Wenn keine Attribute setzbar sind und Negiert auf N steht, werden die Attribute nicht mit ausgegeben.

ACHTUNG: Bitte prüfen Sie vor Ausführung die Zuordnungsart (HIER_TÄTIG, PLANSTELLE etc.)!!!

Sie können diesen Report verwenden, um mehrere OEs bezüglich der aktuellen Rechtevergabe zu validieren (z.B. mehrere Markt-Oes) bzw. die Rezertifizierung im Sinne der MaRisk durchzuführen. Durch die "komprimierte" Anzeige (gleiche Soll-Berechtigungen aller User einer OE werden voran gestellt) wird der Abstimmaufwand reduziert. Ferner können Sie sich durch die Zusammenfassung der User in Gruppen einen Überblick darüber verschaffen, welche User ein gleichartiges Kompetenz- und Rechtegfüge aufweisen. Der Report lässt sich sehr gut mit Report #109 kombinieren: Nutzen Sie 110 um das Soll zu rezertifiziereund und 109 um dann den Soll-Ist-Abgleich durchzuführen.

Sollten User mit gleichen Funktionen / Stellenbeschreibungen in unterschiedlichen Gruppen erscheinen, so wäre zu prüfen, warum und wie sich diese User von den Usern der anderen Gruppe unterscheiden und ob dies sachgerecht ist.

Der Report berücksichtigt die die Berechtigungskategorisierung des R4Plus, vorausgesetzt diese wurde importiert. Dies gibt Ihnen die Möglichkeit, den Report auf risikorelevante Soll-Berechtigungen zu reduzieren.

### #112 Anzahl Berechtigungen in OSP-Funktionsprofilen (Neu)

Der Report zeigt die Anzahl der Berechtigungen in Funktionsprofilen an

### #113 Berechtigungen inkl. Attribute / Anzahl Mitarbeiter (Neu)

Der Report zeigt die zu einem bestimmten Zeitpunkt vergebenen Berechtigungen mit der Anzahl der Mitarbeiter, die diese Berechtigungen besitzen, an. "Geerbte" Berechtigungen (z.B. von Stellen) werden hier mit berücksichtigt. Ferner zeigt der Report die Anzahl der Mitarbeiter differenziert nach allen Attributen an.

### #114 Abweichungen Funktionsprofil / Berechtigungsprofil (Neu)

Der Report vergleicht ein auswählbares Funktionsprofil mit einem auswählbaren Berechtigungsprofil und zeigt ausschließlich Abweichungen an.

### #117 Berechtigungskritikalitäten und R4-Plus-Einschätzung (Neu)

Der Report zeigt die in OSP erfasste Kritikalität und die hinterlegte R4-Plus-Einschätzung von Berechtigungen an. Es werden nur solche Berechtigungen angezeigt, die im Downloadzeitreim verwendet wurden.

### #119 Stellen / Funktionsprofile / Berecht. an Stellenfunktionen (Neu)

Der Report zeigt alle Stellen / Stellenfunktionen und deren Funktionsprofile / Berechtigungen an Stellenfunktionen der selektierten Orgeinheiten an. Es werden nur Stellen angezeigt, denen auch Funktionsprofile oder Soll-Berechtigungen zugewiesen wurden.

### #120 OE / Stelle / Stellenfunktion / Mitarbeiter / Rolle (Neu)

Der Report zeigt alle Rollen der Mitarbeiter sowie die Stellenfunktion der Stelle an.

### #121 Berechtigungen ohne Kritikalitätseinstufung (Neu)

Der Report zeigt die Berchetigungen an, für die in OSP keine Kritikalität erfasst wurde. Ergänzend werden die R4Plus-Risikoeinschätzungen ausgegeben. Es werden nur solche Berechtigungen angezeigt, die im Downloadzeitreim verwendet wurden.

### #123 Funktionsprofile / Verantwortliche (Neu)

Der Report zeigt alle Funktionsprofile sowie deren Verantwortliche an.

### #124 FP-Verantwortlich / Funktionsprofile (Neu)

Der Report zeigt nach Funktionsprofilverantwortlichen sortiert die zugewiesenen Funktionsprofile an.

### #125 Funktionsprofile ohne Verantwortliche (Neu)

Der Report zeigt Funktionsprofile an, bei denen kein Verantwortlicher hinterlegt ist.

# Berechtigungsreports

## Bereich Berechtigungen

### #126 FP-Verantwortlich / Funktionsprofil / Berecht. / Fdef. / Eigen. (Neu)

Der Report erzeugt eine Übersicht aller Funktionsprofile und den darin enthaltenen Berechtigungen inkl. Kompetenzen, sortiert nach dem Funktionsprofilverantwortlichen.

### #127 STF-Verantw. / Stellen mit Prof+Funktionsprof. u. zug. Berecht. (Neu)

Der Report zeigt alle Profile, Funktionsprofile und direkt zugewiesenen Berechtigungen der Stellen (Soll und Ist) und User (Ist der PLANSTELLE) der selektierten Orgeinheiten an. Es werden nur Stellen angezeigt, denen auch Profile oder Berechtigungen zugewiesen wurden. Die Sortierung erfolgt nach Stellenfunktionsverantwortlichen.

### #128 STF-Verantw. / OE / Stelle / Stellenfkt. / Mitarbeiter / Rolle (Neu)

Der Report zeigt alle Rollen der Mitarbeiter sowie die Stellenfunktion der Stelle an. Die Sortierung erfolgt nach dem Stellenfunktionsverantwortlichen.

### #129 STF-Verantw. / Stellen mit Funktionsprof. Und d. zug. Berecht. (Neu)

Der Report zeigt alle Funktionsprofile und direkt zugewiesenen Berechtigungen der Stellen (Soll und Ist) und User (Ist der PLANSTELLE) der selektierten Orgeinheiten an. Es werden nur Stellen angezeigt, denen auch Profile oder Berechtigungen zugewiesen wurden. Die Sortierung erfolgt nach Stellenfunktionsverantwortlichen.

### #130 Direkt an Stellenfunktionen vergeben Berechtigungen (Neu)

Der Report zeigt alle direkt zugewiesenen Berechtigungen an Stellenfunktionen der selektierten Orgeinheiten an. Die Sortierung erfolgt nach Verantwortlichen.

### #131 Soll-/Ist-Ansicht (Neu)

Der Report zeigt das Soll und Ist der selektierten Orgeinheiten, sortiert nach Verantwortlichen, an. Die Zuordnungen (Soll / Ist) können frei gewählt werden.

### #134 STF-Verantwortlich / Stellenfunktion (Neu)

Der Report zeigt die Stellenfunktionen, sortiert nach Stellenfunktionsverantwortlichem, OE und Stelle an.

# Berechtigungsreports

## Bereich Profil-/Berechtigungsgr.

### #38 Profilgruppen nach OEs

Profilgruppen gibt es in OSP selbst nicht. Eine Profilgruppe stellt die Summe aller Profile dar, die einem Mitarbeiter zugewiesen sind. Sollte ein anderer Mitarbeiter die gleichen Profile besitzen, so gehört er zur gleichen Profilgruppe.

Im Report werden die Profilgruppen, die darin enthaltenen Profile und die Mitarbeiter angezeigt. Mitarbeitern direkt zugewiesene Berechtigungen werden hier nicht berücksichtigt.

Der Report wertet alle Profile aus, auch solche, die an der Stelle oder an der OE hängen aus. Da der Mitarbeiter an einem Tag auf mehreren Stellen zugeordnet sein (wenn er z.B. den Platz wechselt wie bei Springern), stellt dies nur die Profilgruppen der angegebenen "Sekunde" dar.

### #41 Profile in Profilgruppen

Profilgruppen gibt es in OSP selbst nicht. Eine Profilgruppe stellt die Summe aller Profile dar, die einem Mitarbeiter zugewiesen sind. Sollte ein anderer Mitarbeiter die gleichen Profile besitzen, so gehört er zur gleichen Profilgruppe.

Im Report werden die Profilgruppen mit den darin enthaltenen Profilen angezeigt. Direkt zugewiesene Berechtigungen werden hier nicht berücksichtigt.

Der Report wertet alle Profile aus, auch solche, die an der Stelle oder an der OE hängen aus. Da der Mitarbeiter an einem Tag auf mehreren Stellen zugeordnet sein (wenn er z.B. den Platz wechselt wie bei Springern), stellt dies nur die Profilgruppen der angegebenen "Sekunde" dar.

### #42 Profilgruppen nach OEs (Excel, alle Profile)

Profilgruppen gibt es in OSP selbst nicht. Eine Profilgruppe stellt die Summe aller Profile dar, die einem Mitarbeiter zugewiesen sind. Sollte ein anderer Mitarbeiter die gleichen Profile besitzen, so gehört er zur gleichen Profilgruppe.

In diesem Excel-Report werden die Profilgruppen, die darin enthaltenen Profile und die Mitarbeiter mit den entsprechenden Profilgruppen angezeigt. Direkt Personen zugewiesene Berechtigungen werden hier nicht berücksichtigt.

Der Report wertet alle Profile aus, auch solche, die an der Stelle oder an der OE hängen aus. Da der Mitarbeiter an einem Tag auf mehreren Stellen zugeordnet sein (wenn er z.B. den Platz wechselt wie bei Springern), stellt dies nur die Profilgruppen der angegebenen "Sekunde" dar.

### #45 Profilgruppen nach OEs inkl. Ursprung

Profilgruppen gibt es in OSP selbst nicht. Eine Profilgruppe stellt die Summe aller Profile dar, die einem Mitarbeiter zugewiesen sind. Sollte ein anderer Mitarbeiter die gleichen Profile besitzen, so gehört er zur gleichen Profilgruppe.

Im Report werden die Profilgruppen, die darin enthaltenen Profile und die Mitarbeiter angezeigt. Direkt Personen zugewiesene Berechtigungen werden hier nicht berücksichtigt. Zusätzlich wird angezeigt, woher die Mitarbeiter ein bestimmtes Profil erhalten haben (über OE, Stelle oder direkt zugewiesen).

Der Report wertet alle Profile aus, auch solche, die an der Stelle oder an der OE hängen aus. Da der Mitarbeiter an einem Tag auf mehreren Stellen zugeordnet sein (wenn er z.B. den Platz wechselt wie bei Springern), stellt dies nur die Profilgruppen der angegebenen "Sekunde" dar.

### #47 Profilgruppen inkl. Ursprung

Profilgruppen gibt es in OSP selbst nicht. Eine Profilgruppe stellt die Summe aller Profile dar, die einem Mitarbeiter zugewiesen sind. Sollte ein anderer Mitarbeiter die gleichen Profile besitzen, so gehört er zur gleichen Profilgruppe.

Im Report werden die Profilgruppen, die darin enthaltenen Profile und die Mitarbeiter angezeigt. Direkt Personen zugewiesene Berechtigungen werden hier nicht berücksichtigt. Zusätzlich wird angezeigt, woher die Mitarbeiter ein bestimmtes Profil erhalten haben (über OE, Stelle oder direkt zugewiesen).

Der Report wertet alle Profile aus, auch solche, die an der Stelle oder an der OE hängen aus. Da der Mitarbeiter an einem Tag auf mehreren Stellen zugeordnet sein (wenn er z.B. den Platz wechselt wie bei Springern), stellt dies nur die Profilgruppen der angegebenen "Sekunde" dar.

### #70 Berechtigungsgruppenvergleich

Der Report zeigt die Anzahl der Abweichungen aller Berechtigungsgruppen an.

## Bereich Profil-/Berechtigungsgr.

### #70 Berechtigungsgruppenvergleich

WICHTIG: Die Berechtigungsgruppen in diesem Report werden dadurch erzeugt, dass alle Berechtigungen eines Mitarbeiters inkl. Attributen, Feindefinitionen und Eigenschaften / Kompetenzen mit denen der anderen Mitarbeiter verglichen werden.

Es wird wie folgt verglichen:

In der Berechtigungsgruppe wird nach gleichen Berechtigungen gesucht.
1. Wenn eine Berechtigung nicht vorhanden ist, gilt dies als 1 Unterschied. Es wird nicht weiter geprüft, ob noch Eigenschaften/Kompetenzen oder Feindefinitionen vorhanden sind!
2. Wenn die Berechtigungen gleich sind wird zuerst geprüft, ob ein oder mehr Attribute unterschiedlich sind. Wenn ein oder mehr Attribute unterschiedlich sind, gilt dies als 1 Unterschied (auch wenn mehrere unterschiedlich sind!). Nach der Attributsprüfung wird weiter geprüft.
3. Wenn ein Feindefinitionssatz (FDef1, FDef2 und FDef3 einer Berechtigung) abweicht bzw. in der anderen Profilgruppe für diese Berechtigung nicht enthalten ist, gilt dies als 1 Unterschied. Liegen mehrere Feindefinitionssätze vor, so wird jeder geprüft. Ein Feindefinitionssatz gilt dann als identisch, wenn alle Feindefinitionen inkl. Attribute identisch sind. Nach der Feindefinitionsprüfung wird weiter geprüft.
4. Wenn eine Eigenschaft/Kompetenz abweicht bzw. in der anderen Berechtigungsgruppe für diese Berechtigung nicht enthalten ist, gilt dies als 1 Unterschied. Eine Eigenschaft gilt dann als identisch, wenn die Untergrenzen/Obergrenzen, die Kompetenzausübung im 4-Augen-Prinzip und das Ein-/Ausschluss-Kennzeichen identisch sind.

### #71 Berechtigungsgruppenvergleich inkl. Mitarbeiternamen

Der Report zeigt die Anzahl der Abweichungen aller Berechtigungsgruppen inkl. Mitarbeiter an.

WICHTIG: Die Berechtigungsgruppen in diesem Report werden dadurch erzeugt, dass alle Berechtigungen eines Mitarbeiters inkl. Attributen, Feindefinitionen und Eigenschaften / Kompetenzen mit denen der anderen Mitarbeiter verglichen werden.

Es wird wie folgt verglichen:

In der Berechtigungsgruppe wird nach gleichen Berechtigungen gesucht.
1. Wenn eine Berechtigung nicht vorhanden ist, gilt dies als 1 Unterschied. Es wird nicht weiter geprüft, ob noch Eigenschaften/Kompetenzen oder Feindefinitionen vorhanden sind!
2. Wenn die Berechtigungen gleich sind wird zuerst geprüft, ob ein oder mehr Attribute unterschiedlich sind. Wenn ein oder mehr Attribute unterschiedlich sind, gilt dies als 1 Unterschied (auch wenn mehrere unterschiedlich sind!). Nach der Attributsprüfung wird weiter geprüft.
3. Wenn ein Feindefinitionssatz (FDef1, FDef2 und FDef3 einer Berechtigung) abweicht bzw. in der anderen Profilgruppe für diese Berechtigung nicht enthalten ist, gilt dies als 1 Unterschied. Liegen mehrere Feindefinitionssätze vor, so wird jeder geprüft. Ein Feindefinitionssatz gilt dann als identisch, wenn alle Feindefinitionen inkl. Attribute identisch sind. Nach der Feindefinitionsprüfung wird weiter geprüft.
4. Wenn eine Eigenschaft/Kompetenz abweicht bzw. in der anderen Berechtigungsgruppe für diese Berechtigung nicht enthalten ist, gilt dies als 1 Unterschied. Eine Eigenschaft gilt dann als identisch, wenn die Untergrenzen/Obergrenzen, die Kompetenzausübung im 4-Augen-Prinzip und das Ein-/Ausschluss-Kennzeichen identisch sind.

### #72 Berechtigungsgruppenvergleich (Stellen-bezogen)

Der Report zeigt die Anzahl der Abweichungen aller Berechtigungsgruppen an.

WICHTIG: Die Berechtigungsgruppen in diesem Report werden dadurch erzeugt, dass alle Berechtigungen von Stellen inkl. Attributen, Feindefinitionen und Eigenschaften / Kompetenzen mit denen der anderen Stellen verglichen werden. Hierbei ist irrelevant, ob die Stelle von Mitarbeitern besetzt ist.

Es wird wie folgt verglichen:

In der Berechtigungsgruppe wird nach gleichen Berechtigungen gesucht.
1. Wenn eine Berechtigung nicht vorhanden ist, gilt dies als 1 Unterschied. Es wird nicht weiter geprüft, ob noch Eigenschaften/Kompetenzen oder Feindefinitionen vorhanden sind!
2. Wenn die Berechtigungen gleich sind wird zuerst geprüft, ob ein oder mehr Attribute unterschiedlich sind. Wenn ein oder mehr Attribute unterschiedlich sind, gilt dies als 1 Unterschied (auch wenn mehrere unterschiedlich sind!). Nach der Attributsprüfung wird weiter geprüft.
3. Wenn ein Feindefinitionssatz (FDef1, FDef2 und FDef3 einer Berechtigung) abweicht bzw. in der anderen Profilgruppe für diese Berechtigung nicht enthalten ist, gilt dies als 1 Unterschied. Liegen mehrere Feindefinitionssätze vor, so wird

### #72 Berechtigungsgruppenvergleich (Stellen-bezogen)

jeder geprüft. Ein Feindefinitionssatz gilt dann als identisch, wenn alle Feindefinitionen inkl. Attribute identisch sind. Nach der Feindefinitionsprüfung wird weiter geprüft.

4. Wenn eine Eigenschaft/Kompetenz abweicht bzw. in der anderen Berechtigungsgruppe für diese Berechtigung nicht enthalten ist, gilt dies als 1 Unterschied. Eine Eigenschaft gilt dann als identisch, wenn die Untergrenzen/Obergrenzen, die Kompetenzausübung im 4-Augen-Prinzip und das Ein-/Ausschluss-Kennzeichen identisch sind.

# Berechtigungsreports

## Bereich RACF

### #61 RACF-User

Zeigt die existenten RACF-User inkl. Parametern an.

HINWEIS: Eine Anmeldung im Portal führt NICHT zu einem Anmelde-Änderungsdatum in RACF, da durch das Portal "nur" ein Schnellcheck durchgeführt wird.

Bitte bedenken Sie, dass die FI die Tabellen in der IIB nur Samstags aktualisiert.

### #62 RACF-User nach letzter Anmeldung

Zeigt die existenten RACF-User inkl. Parametern sortiert nach letztem Anmeldedatum (vom ältesten zum jüngsten) an.

HINWEIS: Es werden ausschließlich diejenigen User angezeigt, welche sich im Auswertungszeitraum zumindest einmal angemeldet haben. Ferner führt eine Anmeldung im Portal NICHT zu einem Anmelde-Änderungsdatum in RACF, da durch das Portal "nur" ein Schnellcheck durchgeführt wird.

Bitte bedenken Sie, dass die FI die Tabellen in der IIB nur Samstags aktualisiert.

### #63 Gesperrte RACF-User

Zeigt gesperrte RACF-User inkl. Parametern an.

Bitte bedenken Sie, dass die FI die Tabellen in der IIB nur Samstags aktualisiert.

### #64 RACF-User mit Passwortintervall größer gleich X Tage

Zeigt alle User an, bei denen das Passwortintervall größer gleich X Tage ist.

Bitte bedenken Sie, dass die FI die Tabellen in der IIB nur Samstags aktualisiert.

### #65 RACF-User ohne Passwortwechsel

Zeig alle User an, die keinen Passwortwechsel durchführen müssen (Passwortintervall = 0).

Bitte bedenken Sie, dass die FI die Tabellen in der IIB nur Samstags aktualisiert.

### #66 RACF-User ohne KURS-ID

Zeigt alle User an, die in RACF eine User-ID haben, nicht aber in KURS

Bitte bedenken Sie, dass die FI die Tabellen in der IIB nur Samstags aktualisiert.

### #67 KURS-User ohne RACF-ID

Zeigt alle User an, die in KURS eine User-ID haben, nicht aber in RACF

Bitte bedenken Sie, dass die FI die Tabellen in der IIB nur Samstags aktualisiert.

### #68 RACF-User nach Gruppen

Zeigt die existenten RACF-User nach Gruppen inkl. Parametern an. Die Gruppe "SXXX$AAA" wird nicht mit ausgegeben.

Bitte bedenken Sie, dass die FI die Tabellen in der IIB nur Samstags aktualisiert.

### #76 RACF-User mit letztem Passwortwechsel >= X Tage

Zeigt alle User mit Kennungen SXXX#### an, die sich vor mehr als X Tagen zum letzten Mal in RACF angemeldet haben. XXX ist hier die Institutsnummer, #### die User-ID des Users. Beispiel: S9991234. Es werden auch User mit Buchstaben in den letzten 4 Zeichen der Kennung berücksichtigt (Beispiel: S999ABCD)

User mit Passwortintervall 0 und User, die innerhalb des angegebenen Zeitraums angelegt wurden, werden nicht angezeigt. Ein Passwortwechsel gilt als Anmeldung.

HINWEIS: Eine Anmeldung im Portal führt NICHT zu einem Anmelde-Änderungsdatum in RACF, da durch das Portal "nur" ein Schnellcheck durchgeführt wird.

Bitte bedenken Sie, dass die FI die Tabellen in der IIB nur Samstags aktualisiert.

# Berechtigungsreports

## Bereich RACF

### #77 RACF-User mit letztem Passwortwechsel >= X Tage

Zeigt alle User mit Kennungen SXXX#### an, die vor mehr als X Tagen zum letzten Mal das Passwort gewechselt haben. XXX ist hier die Institutsnummer, #### die User-ID des Users. Beispiel: S9991234. Es werden auch User mit Buchstaben in den letzten 4 Zeichen der Kennung berücksichtigt (Beispiel: S999ABCD)

User mit Passwortintervall 0 und User, die innerhalb des angegebenen Zeitraums angelegt wurden, werden nicht angezeigt.

Bitte bedenken Sie, dass die FI die Tabellen in der IIB nur Samstags aktualisiert.

### #205 Letzter RACF-PW-Wechsel jünger als letzte Anmeldung am AD

Der Report zeigt alle User an, deren Passwortwechsel in RACF jünger als die letzte Anmeldung in Windows (AD) ist. Die letzte Anmeldung im AD wird aus dem jüngeren Datum der AD-Variablen lastLogon und lastLogonTimestamp gebildet. Der Download der Daten aus RACF und AD muss vom gleichen Tag sein, sonst kann der Report nicht ausgeführt werden.

WICHTIG: Es werden nur Anmeldungen betrachtet, die Älter als 14 Tage sind, da das AD-Attribut lastLogonTimestamp erst nach 14 Tagen auch definitiv zwischen den Domänen-Controllern repliziert wurde. Ferner werden RACF-Daten derzeit nur Samstags in der IIB aktualisiert.

Erläuterung: lastLogon und lastLogonTimestamp unterscheiden sich dadurch, dass lastLogon nicht zwischen den Domänencontrollern repliziert wird, lastLogonTimestamp schon (allerdings erst nach 9-14 Tagen). Der jüngere Werte ist also der "richtigere", wobei der genaue Wert der letzten Anmeldung in der Domäne tatsächlich erst nach 9-14 Tagen im AD über die Variable lastLogonTimestamp ausgelesen werden kann.

# Berechtigungsreports

## Bereich Rezertifizierung

### #75 OSP-Funktionsprofile / Berechtigungen / Fdef. / Eigenschaften

Der Report erzeugt eine Übersicht aller Funktionsprofile und den darin enthaltenen Berechtigungen inkl. Kompetenzen.

### #105 Stellenfunktionen ohne Stellen

Der Report zeigt alle Stellenfunktionen an, die keiner Stelle zugewiesen sind.

### #106 Stellenfunktionen ohne Inhalte

Der Report zeigt alle Stellenfunktionen an, die keine zugewiesenen Berechtigungen oder Profile haben.

### #107 Funktionsprofile ohne Berechtigungen

Der Report zeigt alle Funktionsprofile an, denen überhaupt keine Berechtigungen zugeordnet sind.

### #108 Nirgends zugewiesene Funktionsprofile

Der Report zeigt Funktionsprofile an, die aktuell nicht verwendet werden.

### #109 Soll/Ist-Vergleich nach Stellen

Vergleicht das SOLL einer Stelle mit dem IST. Hierbei werden die Berechtigungen des Mitarbeiters, der eine Planstelle besetzt, mit den Soll-Werten der Stellenfunktion verglichen.

### #117 Berechtigungskritikalitäten und R4-Plus-Einschätzung (Neu)

Der Report zeigt die in OSP erfasste Kritikalität und die hinterlegte R4-Plus-Einschätzung von Berechtigungen an. Es werden nur solche Berechtigungen angezeigt, die im Downloadzeitreim verwendet wurden.

### #118 Anwendungsschutzbedarf (Neu)

Der Report zeigt die Anwendung inklusive der administrierten Parameter zum Schutzbedarf an.

### #119 Stellen / Funktionsprofile / Berecht. an Stellenfunktionen (Neu)

Der Report zeigt alle Stellen / Stellenfunktionen und deren Funktionsprofile / Berechtigungen an Stellenfunktionen der selektierten Orgeinheiten an. Es werden nur Stellen angezeigt, denen auch Funktionsprofile oder Soll-Berechtigungen zugewiesen wurden.

### #120 OE / Stelle / Stellenfunktion / Mitarbeiter / Rolle (Neu)

Der Report zeigt alle Rollen der Mitarbeiter sowie die Stellenfunktion der Stelle an.

### #121 Berechtigungen ohne Kritikalitätseinstufung (Neu)

Der Report zeigt die Berchetigungen an, für die in OSP keine Kritikalität erfasst wurde. Ergänzend werden die R4Plus-Risikoeinschätzungen ausgegeben. Es werden nur solche Berechtigungen angezeigt, die im Downloadzeitreim verwendet wurden.

### #122 Anwendungen ohne Schutzbedarfseinstufung (Neu)

Der Report zeigt Anwendung an, für die keine Schutzbedarfskategorisierung vorgenommen wurde.

### #123 Funktionsprofile / Verantwortliche (Neu)

Der Report zeigt alle Funktionsprofile sowie deren Verantwortliche an.

### #124 FP-Verantwortlich / Funktionsprofile (Neu)

Der Report zeigt nach Funktionsprofilverantwortlichen sortiert die zugewiesenen Funktionsprofile an.

### #125 Funktionsprofile ohne Verantwortliche (Neu)

Der Report zeigt Funktionsprofile an, bei denen kein Verantwortlicher hinterlegt ist.

### #126 FP-Verantwortlich / Funktionsprofil / Berecht. / Fdef. / Eigen. (Neu)

Der Report erzeugt eine Übersicht aller Funktionsprofile und den darin enthaltenen Berechtigungen inkl. Kompetenzen, sortiert nach dem Funktionsprofilverantwortlichen.

### #127 STF-Verantw. / Stellen mit Prof+Funktionsprof. u. zug. Berecht. (Neu)

# Berechtigungsreports

## Bereich Rezertifizierung

### #127 STF-Verantw. / Stellen mit Prof+Funktionsprof. u. zug. Berecht. (Neu)

Der Report zeigt alle Profile, Funktionsprofile und direkt zugewiesenen Berechtigungen der Stellen (Soll und Ist) und User (Ist der PLANSTELLE) der selektierten Orgeinheiten an. Es werden nur Stellen angezeigt, denen auch Profile oder Berechtigungen zugewiesen wurden. Die Sortierung erfolgt nach Stellenfunktionsverantwortlichen.

### #128 STF-Verantw. / OE / Stelle / Stellenfkt. / Mitarbeiter / Rolle (Neu)

Der Report zeigt alle Rollen der Mitarbeiter sowie die Stellenfunktion der Stelle an. Die Sortierung erfolgt nach dem Stellenfunktionsverantwortlichen.

### #129 STF-Verantw. / Stellen mit Funktionsprof. Und d. zug. Berecht. (Neu)

Der Report zeigt alle Funktionsprofile und direkt zugewiesenen Berechtigungen der Stellen (Soll und Ist) und User (Ist der PLANSTELLE) der selektierten Orgeinheiten an. Es werden nur Stellen angezeigt, denen auch Profile oder Berechtigungen zugewiesen wurden. Die Sortierung erfolgt nach Stellenfunktionsverantwortlichen.

### #130 Direkt an Stellenfunktionen vergeben Berechtigungen (Neu)

Der Report zeigt alle direkt zugewiesenen Berechtigungen an Stellenfunktionen der selektierten Orgeinheiten an. Die Sortierung erfolgt nach Verantwortlichen.

# Berechtigungsreports

## Bereich Sonstiges

### #12 Menüstruktur Portal

Dieser Report zeigt die Menüstruktur unter OSP-Portal an, auf die der Mitarbeiter anhand der aktuell vergebenen Berechtigungen zugreifen kann. Der Report eignet sich unter anderem, um Profile mit Abteilungsleitern abzustimmen.

### #18 Von SXXX####- abweichende User-IDs

Der Report zeigt alle User-IDs an, die vom Standard abweichen. Im Normalfall steht vor einer User-Kennung ein S und die dreistellige Institutsnummer. Dieser Report zeigt alle Kennungen an, die von diesem Standard, aus welchen Gründen auch immer, abweichen. Er kann somit der Qualitätssicherungen der S-Kennungen und technischer User dienen.

Ab Release 9.0: Der User "Technischer RACF-User" (PNR: 9999001001) wird bei diesem Report nicht angezeigt, da er nur als "Pseudouser" die Unterschiede zwischen RACF und KURS abbildet.

### #19 Berechtigungen

Der Report zeigt alle in OSP vorhandenen Berechtigungen zu einem bestimmten Tag an. Zum Report-Tag nicht mehr gültige Berechtigungen sind gesondert gekennzeichnet.

### #25 In einem Zeitraum zu OSP hinzugefügte Berechtigungen

Der Report zeigt die Berechtigungen an, die von der SI in einem bestimmten Zeitraum neu zu OSP hinzugefügt wurden (Schlüsselverzeichnis PRI).

### #57 OE-Hierarchie-Baum

Erzeugt einen Hierarchiebaum der aktuellen OE-Struktur nach einer bestimmten OE-Rolle.

### #115 OE-Beziehungen (Neu)

Der Report zeigt OE-Beziehungen an. Die OE-Hierarchie-Bäume werden nicht angezeigt, nutzen Sie dafür Report #57.

### #116 Objekt-Beziehungen und Verantwortlichkeiten (Neu)

Der Report zeigt Beziehungen zwischen Objekten in OSP an, z.B. wer verantwortlich ist für bestimmte Berechtigungen oder auch Anwendungen.

### #118 Anwendungsschutzbedarf (Neu)

Der Report zeigt die Anwendung inklusive der administrierten Parameter zum Schutzbedarf an.

### #122 Anwendungen ohne Schutzbedarfseinstufung (Neu)

Der Report zeigt Anwendung an, für die keine Schutzbedarfskategorisierung vorgenommen wurde.

# Berechtigungsreports

## Bereich Stellen / Rollen

### #1 Mitarbeiter ohne OE

Der Report zeigt alle Mitarbeiter an, die zum Auswertungszeitpunkt keiner OE zugewiesen sind.

### #20 Mitarbeiter Vertritt

Der Report zeigt alle Mitarbeiter an, die die Rolle „MA vertritt“ auf Beraterplätze zugewiesen bekommen haben.

### #21 OE / Stelle / Mitarbeiter / Rolle

Der Report zeigt alle Rollen der Mitarbeiter bestimmter OEs an. (hier tätig, Planstelle, MA vertritt).

### #22 Unbesetzte Stellen

Der Report zeigt alle Stellen einer OE an, die unbesetzt sind.

### #24 Mitarbeiter Stellenhistorie

Der Report zeigt an, wann bestimme Mitarbeiter welche Stelle besetzt haben (HIER_TÄTIG).

### #74 Stelle Vertritt Stelle

Der Report zeigt alle Stellen an, die anderen Stelle vertreten.

### #80 Mitarbeiter wird vertreten von

Der Report zeigt die Stellen des Mitarbeiters an, auf denen der Mitarbeiter eine bestimmbare Rolle hat UND für die es Stellvertretungen zu dieser Stelle gibt. Stellen, für die der User eine Rolle hat, für die es aber keine Stellvertretung (MA VERTRITT oder VERTRETUNG) gibt, werden NICHT angezeigt.

### #120 OE / Stelle / Stellenfunktion / Mitarbeiter / Rolle (Neu)

Der Report zeigt alle Rollen der Mitarbeiter sowie die Stellenfunktion der Stelle an.

### #128 STF-Verantw. / OE / Stelle / Stellenfkt. / Mitarbeiter / Rolle (Neu)

Der Report zeigt alle Rollen der Mitarbeiter sowie die Stellenfunktion der Stelle an. Die Sortierung erfolgt nach dem Stellenfunktionsverantwortlichen.

# Berechtigungsreports

## Bereich User

### #39 Hinzugefügte und entfernte KURS-User nach Name

Zeigt alle hinzugefügten und entfernten (abgelaufenen) User in einem bestimmten Zeitraum, nach Name sortiert, an.

### #40 Hinzugefügte und entfernte KURS-User nach Datum

Zeigt alle hinzugefügten und entfernten (abgelaufenen) User in einem bestimmten Zeitraum an. Es wird nach dem Hinzufüge- / Ablaufdatum sortiert, je nachdem, was relevant ist. Wenn ein User im gegebenen Zeitraum hinzugefügt und entfernt wurde, wird er unter dem "Hinzufüge-Datum" aufgeführt.

Es werden auch User aufgeführt, die "umbenannt" oder deaktiviert wurden.

### #82 User aus Excel-Liste ohne KURS-User

Zeigt die User aus einer frei definierbaren Excel-Liste an, die keinen KURS-User haben.

### #83 KURS-User ohne User aus Excel-Liste

Zeigt die User aus KURS an, die in einer frei definierbaren Excel-Liste fehlen..

### #132 KURS User (Neu)

Der Report zeigt alle User mit Von-Bis-Datum, Eintritts- und Austrittsdatum, User-Typ, Gesperrt (durch Admin, nicht durch Falscheingabe Passwort), Mitarbeitergruppe und Mitarbeiterstatus im selektierten Zeitraum an.

### #250 AD-User ohne KURS-User

Zeigt AD-User an, die in KURS keinen User haben.

ACHTUNG: Bitte bedenken Sie, dass das KURS-Datum und das AD-Download-Datum voneinander abweichen können! Es kann also durchaus sein, dass Sie unterschiedliche Zeiträume betrachten!

### #251 KURS-User ohne AD-User

Zeigt KURS-User an, die keinen AD-User haben.

ACHTUNG: Bitte bedenken Sie, dass das KURS-Datum und das AD-Download-Datum voneinander abweichen können! Es kann also durchaus sein, dass Sie unterschiedliche Zeiträume betrachten!

### #252 AD-User ohne WinNT-User

Zeigt AD-User an, die in WinNT keinen User haben.

### #253 WinNT-User ohne AD-User

Zeigt WinNT-User an, die in AD keinen User haben.

### #254 WinNT-User ohne KURS-User

Zeigt WinNT-User an, die in KURS keinen User haben.

ACHTUNG: Bitte bedenken Sie, dass das KURS-Datum und das WinNT-Download-Datum voneinander abweichen können! Es kann also durchaus sein, dass Sie unterschiedliche Zeiträume betrachten!

### #255 KURS-User ohne WinNT-User

Zeigt KURS-User an, die in WinNT keinen User haben.

ACHTUNG: Bitte bedenken Sie, dass das KURS-Datum und das WinNT-Download-Datum voneinander abweichen können! Es kann also durchaus sein, dass Sie unterschiedliche Zeiträume betrachten!