



Inhaltsverzeichnis

1	Benutzerdefinition	3
1.1	Benutzer "QSECOFR"	3
1.2	Gruppenprofile (GRPPRF)	4
1.3	Definition von Benutzerprofilen	5
1.3.1	Benutzerprofile	5
1.3.2	Merkmale eines normalen Gruppenprofiles:	6
1.3.3	Merkmale eines normalen GISA-Benutzerprofiles:	6
1.3.4	Berechtigung der Outqueues für allgemeine Ausdrücke	6
1.3.5	Berechtigung der Outqueues für vertrauliche Ausdrücke	6
1.4	weitere Definitionen	6
1.4.1	Verzeichniseintragung	6
1.4.2	Benutzer in anderen Modulen	6
1.4.3	Systemwerte betreffend Kennwort	6
1.4.4	Konzept für Kennwörter	6
1.5	Berechtigungs-Modul	6

1 Benutzerdefinition

1.1 Benutzer "QSECOFR"

Der Benutzer "QSECOFR" ist → Sicherheitsbeauftragter mit der Benutzerklasse ***SECOFR**

Die oberste Priorität im iSeries hat der Benutzer "QSECOFR". Er hat die Berechtigung, auf fast alle Daten im iSeries sowie auf viele systemnahe Funktionen, die nur er ausführen darf. Dies gilt für alle Benutzer "QSECOFR" oder für die Benutzer mit der Benutzerklasse *SECOFR.

Für den Fall, dass ein Benutzer sein Passwort verliert, muss der QSECOFR ihm ein neues zuweisen. Er hat aber nicht die Möglichkeit Passwörter anzusehen. Kann der QSECOFR einem Benutzer ein neues Passwort zuweisen, so hat er auch die Möglichkeit, sich mit dem ihn nun bekannten Passwort als dieser Benutzer anzumelden und somit vertrauliche Daten zu erhalten.

Sich als QSECOFR anmelden, soll nur eine Person können, die volles Vertrauen genießt!

Die Berechtigung

Um einen Benutzer oder ein Gruppenprofil erfassen oder ändern zu können, müssen Sie sich mit dem Benutzer "QSECOFR" anmelden. Nur der Benutzer "QSECOFR" ist berechtigt, alle Benutzer zu ändern.

Anmerkung: Ist einem Benutzerprofil die Benutzerklasse *SECADM zugewiesen, so könnte auch dieses Benutzerprofil die ändern Benutzerprofile ändern oder erfassen.



Bemerkung:

*Es sollte nicht mit dem Benutzer "QSECOFR" oder einem Benutzer mit der Benutzerklasse *SECOFR im GISA gearbeitet werden!*

Ebenfalls sollte kein Benutzer mit dem Namen "GISA" und dem Kennwort "GISA" oder dem Namen "QSECOFR" und dem Kennwort "QSECFR" auf Ihrem System vorhanden sein! Überhaupt sollte das Kennwort nie mit dem Benutzernamen identisch sein.

Empfehlung!

Für den Fall, dass das Kennwort des Profils QSECOFR nicht mehr bekannt ist, sollte ein spezielles Benutzerprofil (z. B. QSECOFR1) angelegt werden. Mit diesem Profil wird nicht gearbeitet, es dient lediglich für den Notfall. Das Profil wird so eingerichtet, dass das Kennwort nie abläuft. Das Kennwort wird an einem sicheren Ort aufbewahrt. Wenn man mit diesem Profil angemeldet ist, kann das Kennwort des QSECOFR neu definiert werden.

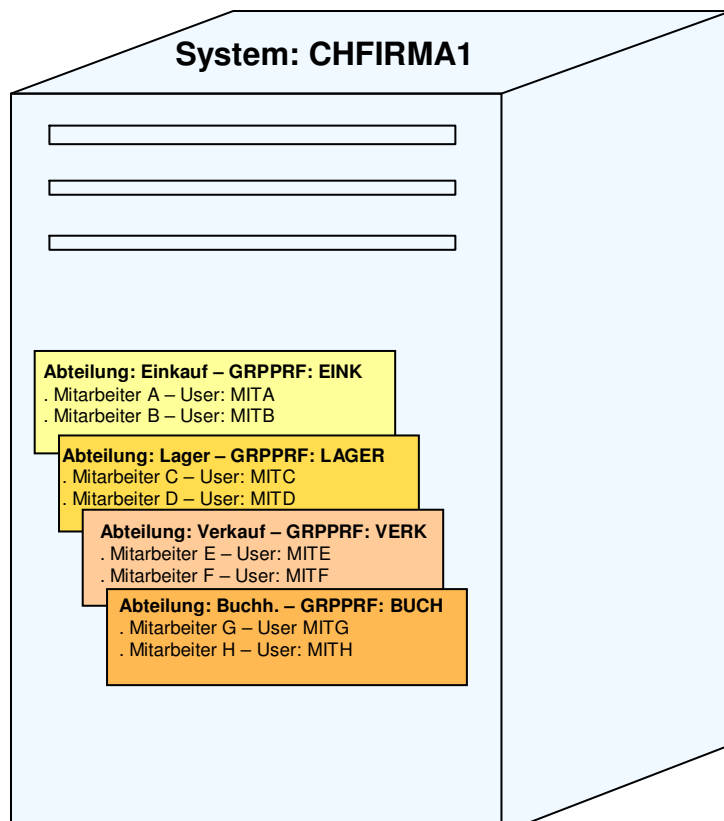
1.2 Gruppenprofile (GRPPRF)

Wir empfehlen Ihnen, Ihre Benutzer in Gruppen zusammenzufassen und die entsprechenden Gruppenprofile im iSeries zu eröffnen, damit die Berechtigung ausschliesslich anhand der Gruppenprofile vergeben werden kann.

Gruppenprofile sind statisch und orientieren sich nach der Aufbauorganisation der Firma. Jeder Benutzer ist in seinem Abteilungs-Gruppenprofil eingetragen.

Bei einem Personalwechsel kann so der neue Benutzer eröffnet werden und mit der Zuweisung des entsprechenden Gruppenprofiles ist er sofort für sein Einsatzgebiet berechtigt.

Ein Gruppenprofil wird ebenfalls in den Benutzerprofilen erfasst.



1.3 Definition von Benutzerprofilen

Für die Definition Ihrer Benutzer respektive für die Definition der Berechtigung empfehlen wir Ihnen folgendes Vorgehen:

1. Teilen Sie Ihre Mitarbeiter in Gruppen ein und definieren Sie bei jedem Benutzerprofil das entsprechende Gruppenprofil.
2. Definieren Sie ein Benutzerprofil für jeden Ihrer Mitarbeiter, welcher auf Ihrem System arbeitet.
3. Nun kann für jede Gruppe ein separates Menü erstellt werden. Auf diesem Menü befinden sich die Programme, welche für die betreffende Gruppe benötigt werden.
4. Muss die Berechtigung noch weiter aufgeteilt werden, so kann das Berechtigungs-Modul vom GISA eingesetzt werden.

1.3.1 Benutzerprofile

Um ein Gruppenprofil oder ein Benutzerprofil zu erstellen, muss mit dem Benutzer: QSECOFR gearbeitet werde.

Mit dem Befehl **go cmdusrprf** erhalten Sie das Menü mit den Befehlen für die Benutzerprofile.

```
CMDUSRPRF          Benutzerprofilbefehle
Auswahlmöglichkeiten:
  Befehle
  1. Benutzerprofil ändern           CHGUSRPRF
  2. Benutzerprofil erstellen       CRTUSRPRF
  3. Benutzerprofil löschen         DLTUSRPRF
  4. Benutzerprofil anzeigen       DSPUSRPRF
  5. Interne Druckprofildaten      PRTPRFINT
  6. Benutzerprofile zurückspeich.  RSTUSRPRF
  7. Benutzerprofil auffinden      RTVUSRPRF
  8. Anpassungsdaten festlegen     SETCSTDTA
  9. Mit Benutzerprofilen arbeiten  WRKUSRPRF
  Zugehörige Befehlsmenüs
  10. Abrechnungsbefehle           CMDACG
  Weitere ...
Auswahl oder Befehl
==> _
```

Wählen Sie den Befehl "9. Mit Benutzerprofilen arbeiten", kann anschliessen mit der Auswahl

- 1 = Erstellen
- 2 = Ändern
- 3 = Kopieren
- 4 = Löschen
- 5 = Anzeigen
- 12 = mit Objekten eines Eigners arbeiten

gearbeitet werden.

Am Einfachsten ist es natürlich, wenn ein bestehendes Benutzerprofil kopiert werden kann. (Auswahl 3 = kopieren)

2. im Benutzerprofil

Benutzerprofil	USRPRF	MITA	Name des Benutzerprofils
Benutzerkennwort	PASSWORD	xxxx	Kennwort für dieses Benutzerprofil
Status	STATUS	*ENABLED	das Benutzerprofil ist aktiv und berechtigt zum Anmelden
Benutzerklasse	USRCLS	*USER	
Text "Beschreibung"	TEXT	Mitarbeiter A	Beschreibung des Profils
Sonderberechtigung	SPCAUT	*JOBCTL	damit die GISA-Funktionen gewährleistet sind, brauchen die Benutzer die Sonderberechtigung *JOBCTL
<p>Achtung: es darf nie, die Sonderberechtigung *ALLOBJ zugeordnet werden, da der Benutzer sonst auf ALLE Daten Zugriff hat. es darf auch nie, die Sonderberechtigung *SPLCTL (siehe auch nachfolgende Beschreibung „Berechtigung der Outqueues für allgemeine und vertrauliche Ausdrücke“) zugeordnet werden, da der Benutzer sonst Zugriff auf ALLE Spooldateien hat.</p>			
Gruppenprofil	GRPPRF	EINKAUF	dieser Benutzer hat die Berechtigung der Gruppe EINKAUF
Eigner	OWNER	*GRPPRF	der Besitzer eines Objektes, welches durch das Gruppenprofil erstellt wird, gehört der Gruppe

1.3.3 Merkmale eines normalen GISA-Benutzerprofils:

- Kennwort xxxx
- Status *ENABLED
- UserClass *USER
- Sonderberechtigung *JOBCTL

- mit Gruppenprofil
- Eigner *GRPPRF

1.3.4 Berechtigung der Outqueues für allgemeine Ausdrücke

Bemerkung:

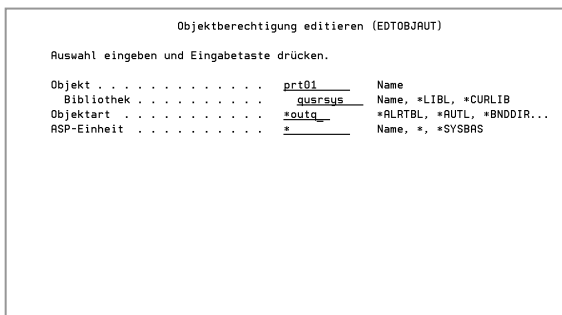
In der Sonderberechtigung (SPCAUT) kann die Berechtigung *SPLCTL (Spool control) aktiviert werden. Diese Sonderberechtigung wird **nicht** empfohlen, da der Benutzer mit dieser Berechtigung Zugriff auf **alle** Spooldateien hat. Vielmehr sollte in den normalen Outqueues die Berechtigung ***PUBLIC mit *CHANGE** definiert sein.

Mit dem Befehl EDTOBJAUT (Objektberechtigung editieren) kann eine Outqueue geändert werden.

Beispiel:

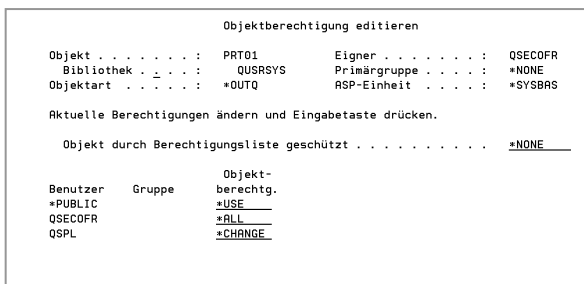
1. Bild:

Objekt gewünschte Outqueue z.B. **PRT01**
 Bibliothek **QUSRSYS**
 Objektart ***OUTQ**



2. Bild

Benutzer *Gruppe* *Objektberechtigung*
***PUBLIC** ***CHANGE**



Mit dem Befehl WRKOUTQ erhalten Sie eine Liste Ihrer Drucker resp. Ihrer Outqueues. Mit der Auswahl "2" ändern, können die Felder „vom Bediener gesteuert“ **OPRCTL** auf „*NO“ und „Berechtigung prüfen“ **AUTCHK** auf **"*DTAAUT"** angepasst werden.

OPRCTL → *NO bedeutet: Diese Warteschlange und ihre Einträge können von einem Benutzer mit Jobsteuerungsberechtigung nicht manipuliert oder geändert werden, es sei denn, er hat auch andere spezielle Berechtigungen.

AUTCHK → *DTAAUT bedeutet: „jeder Benutzer mit Hinzufüge-, Lese- und Löschberechtigung für die Ausgabewarteschlange kann alle Spooldateien in der Warteschlange steuern". Spooldateien gehören dem Profil, welches die Spooldatei erstellt hat.

```

Ausgabewarteschlange ändern (CHGOUTQ)

Auswahl eingeben und Eingabetaste drücken.

Text 'Beschreibung' . . . . . TEXT          'Standardausgabewarteschlange f
ür Drucker PRT03'

-----
Zusätzliche Parameter

Jede Datei anzeigen . . . . . DSPDTR      =NO
Jobtrennungen . . . . . JOBSEP           0
Vom Bediener gesteuert . . . . . OPRCTL   =NO
Datenwarteschlange . . . . . DTAQ        =NONE
Bibliothek . . . . .                      _____
Berechtigung prüfen . . . . . AUTCHK     =DTAAUT

-----
F3=Verlassen  F4=Bedienerf.  F5=Aktualisieren  F12=Abbrechen
F13=Verwendung der Anzeige  F24=Weitere Tasten

Ende
    
```

Alle Outqueues, über welche normale Listen und Dokumente (Lieferscheine, etc.) abgewickelt werden, sind wie soeben beschrieben zu definieren.

1.3.5 Berechtigung der Outqueues für vertrauliche Ausdrücke

Für vertrauliche Listen, wie z.B. Lohnabrechnungen, sind spezielle Outqueues einzurichten.

```

Objektberechtigung editieren

Objekt . . . . . : PRT11      Eigner . . . . . : QSECOFR
Bibliothek . . . . : QUSRSYSALT Primärgruppe . . . . : *NONE
Objektart . . . . . : *OUTQ    ASP-Einheit . . . . : *SYSBAS

Aktuelle Berechtigungen ändern und Eingabetaste drücken.

Objekt durch Berechtigungsliste geschützt . . . . . *NONE

-----
Benutzer  Gruppe  Objekt-
*PUBLIC   Gruppe  berechtig.
QSECOFR   _____ *EXCLUDE
QSPL      _____ *ALL
           _____ *CHANGE

-----
F3=Verlassen  F6=Benutzer hinzufügen  F12=Abbrechen  F24=Weitere Tasten

Ende
    
```

Benutzer *PUBLIC → Berechtigung auf *EXCLUDE

Mit dem Befehl WRKOUTQ das Feld "Berechtigung prüfen" **AUTCHK** → auf ***OWNER** setzen. ***OWNER** bedeutet:

Der Benutzer muss über die Eigenerberechtigung für die Ausgabewarteschlange verfügen, um die Berechtigungsprüfung für die Ausgabewarteschlange zu bestehen. Der Benutzer besitzt die Eigenerberechtigung, wenn er Eigner der Ausgabewarteschlange ist oder ein Gruppenprofil gemeinsam mit dem Warteschlangeneigner benutzt oder ein Programm ausführt, das die Eigenerberechtigung übernimmt.

1.4 weitere Definitionen

1.4.1 Verzeichniseintragung

Wird ein neuer Benutzer im iSeries eröffnet, dann muss für diesen Benutzer auch der Befehl ADDDIRE durchgeführt werden.

Die Verzeichniseintragung wird z.B. benötigt für den Befehl CPYFRMSTMF, welcher u.a. im Programm „VESR einlesen“ (DEB032V*) verwendet wird.

Geben Sie den Befehl ADDDIRE ein und ergänzen Sie folgende Felder:

Benutzer-ID	USRID	MITA	Name des Benutzerprofils
Adresse		CHFIRMA	Name des Systems
Benutzerbeschreibung	USRD	Mitarbeiter A	Beschreibung des Profils

1.4.2 Benutzer in anderen Modulen

Bei einigen Applikationen muss ein Benutzer zusätzlich im Modul definiert werden. Werden folgende Module eingesetzt muss ein Benutzer für das Modul definiert werden:

- . InfoStore
- . IRIS
- . FINANZ
- . PROFIT
- . FAX-Modul
- . GISA (wenn Berechtigungs-Modul verwendet wird)

1.4.3 Systemwerte betreffend Kennwort

Weiter gilt zu beachten, dass für die Definition des Kennwortes auch Systemwerte vorhanden sind. Folgende Systemwerte müssen berücksichtigt werden:

Systemwert	Beschreibung		Wert
QPWDEXPITV	Intervall für Kennwortverfall	Intervall in Tagen	*NOMAX, 1-366
QPWDLMTAJC	Zusammenhängende Ziffern in Kennwort begrenzen	Angrenzende Ziffern	0 = zulässig, 1 = nicht zulässig
QPWDLMTCHR	Zeichen in Kennwort begrenzen	Zeichen in Kennwort nicht zulässig	*NONE
QPWDLMTREP	Zeichenwiederholung in Kennwort begrenzen	Zeichen in Kennwort	0 = kann wiederholt werden 1 = kann nicht wiederholt werden 2 = kann nicht sequentiell wiederholt werden
QPWDLVL	Kennwortstufe	Kennwortstufe	0 = für die Benutzerprofile werden Kennwörter von 1-10 Zeichen unterstützt 1 = für die Benutzerprofile werden die Kennwörter von 1-10 Zeichen unterstützt. AS/400 NetServer-Kennwörter für Windows 95/98/ME Clients werden aus dem System entfernt. 2 = für die Benutzerprofile werden Kennwörter von 1-128 Zeichen unterstützt. 3 = für die Benutzerprofile werden Kennwörter von 1-128 Zeichen unterstützt. AS/400 NetServer-Kennwörter für Windows 95/98/ME Clients werden aus dem System entfernt.
QPWDMAXLEN	Maximale Länge des Kennworts	Maximale Kennwortlänge	1-128
QPWDMINLEN	Mindestlänge des Kennworts	Minimale Kennwortlänge	1-128
QPWDPOSDIF	Zeichenpositionen in Kennwort begrenzen	Zeichenpositionen im Kennwort	0 = können gleich sein 1 = können nicht gleich sein
QPWDRQDDGT	Ziffer in Kennwort erforderlich	Ziffer in Kennwort	0 = nicht erforderlich 1 = erforderlich
QPWDRQDDIF	Kontrolle für doppelte Kennwörter	neues Kennwort	0 = kann gleiches Kennwort wie zuvor sein 1 = darf nicht gleich der letzten 32 sein 2 = darf nicht gleich der letzten 24 sein 3 = darf nicht gleich der letzten 18 sein 4 = darf nicht gleich der letzten 12 sein 5 = darf nicht gleich der letzten 10 sein 6 = darf nicht gleich der letzten 8 sein 7 = darf nicht gleich der letzten 6 sein 8 = darf nicht gleich der letzten 4 sein
QPWDLDPGM	Gültigkeitsprüfung für Kennwort	Kennwortprüfprogramm Bibliothek	Name, *REGFAC, *NONE Name

Bemerkung:

wird im System **QPWDLVL** (Kennwortstufe) der Wert 0 oder 1 gesetzt, wird die Gross- und Kleinschreibung nicht berücksichtigt, wird jedoch der Wert 2 oder 3 gesetzt, das heisst, die Kennwörter sind über 10 Zeichen lang, muss auf die Gross- und Kleinschreibung geachtet werden. Die Gross- und Kleinschreibung innerhalb des Kennwortes wird berücksichtigt.

1.4.4 Konzept für Kennwörter

Damit die oben erwähnten Systemwerte definiert werden können, sollte für das Definieren von Kennwörtern ein Konzept vorhanden sein.

Hier ein Artikel aus der Zeitschrift "Midrange MAGAZIN, November 2000"

Tipps für den Umgang mit Passwörtern

kLykotten*mUmpel gegen Anja

Wir leben in einer Zeit der Passwort-Inflation.

Wo früher "geheime Parolen" nur berechtigten bekannt waren, herrscht heute mehr und mehr ein nachlässiger Umgang damit. Die auf Informationstechnik spezialisierte Sicherheitsberatung TÜV NORD SECURITY GmbH aus Hamburg gibt praktische Tipps zum Umgang mit den kleinen Wörtern.

"Wo ist denn der aktuelle Projektstatus für den Umzug unserer Filiale in Bauzen? Der Chef braucht ihn dringend!" ertönt es morgens um 10.00 Uhr in einem Bankunternehmen in Frankfurt.

"Den hat der Mayer zusammengestellt. Aber der ist heute krank." "Hast Du das Passwort für den Computer?" "Warte mal, der hat doch ein Segelboot. Auf dem Foto da steht auch der Name: Probier's mit Serendipity." "Passt nicht!" "Dann den Namen seiner Frau – Anja. Ist ja praktischer, weil kürzer." "Bingo! Danke Kollege!"

Eine Situation, wie sie täglich vorkommt: Passwörter werden nach Praktikabilität gewählt – Namen von Ehefrauen und –männern, Kindern,

Hunden, Katzen, Booten oder einfache Tastaturkombinationen wie QWERTZ. Zudem gelten die Wörter meist sehr lange, weil keiner daran denkt, sie zu wechseln.

Gefahr durch Social Hacking

Nach der Erfahrung der Hamburger IT-Sicherheitsberatung TÜV NORD SECURITY müssen für den Passwortklauf nicht immer aufwendige Techniken eingesetzt werden. Vielmehr werden PINs grosszügig weitergegeben, im Supermarkt am EC-Kassenterminal allzu offensichtlich eingetippt. In Firmen sind sie häufig dem Zimmerkollegen bekannt oder leicht zu erraten. Hier gelten strikte Regeln: Ein Passwort, das mehr als eine Person kennt, ist wertlos. Ein Passwort, das Bezug auf die eigene Person hat, ist wertlos. Hacker-Profis gehen systematisch vor: Mit so genannten Sniffer-Programmen, die Informationen im Netz abfragen, Tastaturrecordern, die unbemerkt auf einem PC installiert werden und alle Tastaturanschläge speichern oder Passwort-Decodern werden unverschlüsselte oder schwach verschlüsselte Passwörter aus den Systemdateien ausgelesen.

Ein zusätzlicher Sicherheitsfaktor ist das regelmässige Wechseln der Passwörter, da selbst leistungsstarke Rechner einige Zeit benötigen, um Millionen von Begriffen zu scannen: Ein Passwort, das nicht monatlich gewechselt wird, ist wertlos.

Sicherheit durch Fantasie

Die Sicherheitsstrategie eines Unternehmens muss konkrete Anweisungen für die Passwortfindung geben, die entweder von Systemadministratoren oder den Anwendern selbst umzusetzen sind. Um letzteres sicherzustellen, können in Servern Vorgaben gespeichert werden, die nur Passwörter akzeptieren, die ganz bestimmte Anforderungen erfüllen – so etwa Länge, Sonderzeichen, gemischte Schreibweise, kleine reine Zahlenkombination u. a.

Auf den ersten Anblick mögen die Bedingungen verwirren, aber wer sagt, dass sich ein User nicht den Begriff "kLykotten*mUmpel" merken kann?"

Weiter kann beispielsweise auf der Internetseite www.datenschutz.ch unter **Passwort-Check** die Sicherheit Ihrer Kennwörter geprüft werden.

Sichere Passwörter

- sind mindestens 8 Zeichen lang
- bestehen nicht nur aus Zahlen
- enthalten Klein- und Grossbuchstaben in "unlogischer" Anordnung
- enthalten mindestens ein Sonderzeichen (* + # \$ % & / () = ! " -)
- enthalten nicht die selben Zeichen mehrfach hintereinander
- kombinieren mehrere Begriffe miteinander
- sind keine Namen, keine Produktbezeichnungen oder Begriffe aus dem Arbeitsumfeld
- haben keinen sachlichen Bezug zum Inhaber, seiner Familie, seiner Arbeit oder seinen Hobbys
- bezeichnen kein Objekt, das am Arbeitsplatz ins Auge fällt
- enthalten keinen Begriff, der in irgendwelchen Wörterbüchern oder Nachschlagewerken vorkommt oder vorkommen könnte
- enthalten keine Sprichwörter, Phrasen o. ä.
- sind keine Tastaturmuster wie etwa "qwertz"

Kennwörter regelmässig (mindestens alle 30 Tage) ändern!

1.5 Berechtigungs-Modul

Für Berechtigungen auf der Ebene "Programme" empfehlen wir Ihnen unser Berechtigungs-Modul. Mit dem Berechtigungs-Modul besteht die Möglichkeit von Security-Definitionen auf Ebene Firma und/oder Programmen. Es können für bestimmte Gruppenprofile oder für einzelne Benutzer Programme oder Funktionen berechtigt respektive gesperrt werden.

Im Berechtigungs-Modul kann sowohl ein Benutzer als auch ein Gruppenprofil erfasst werden. Sie können also für eine Gruppe gewünschte Programme oder Funktionen berechtigen oder sperren und/oder für einen Benutzer gewünschte Programme oder Funktionen berechtigen oder sperren.

Somit ist es auch möglich, dass eine Gruppe für ein Programm oder eine Funktion nicht berechtigt ist, ein einzelner Benutzer aus dieser Gruppe jedoch eine Berechtigung erhält.