GPM Re-Zertifizierung

1 Ziel

Abhängig von der Security-Classification (SC, nach X509) der beim User zugeordneter Rollen und Einzelberechtigungen wird in regelmäßigen Abständen eine Wiederholungsfreigabe (Re-Zertifizierung) eingefordert. Diese Prozesse werden automatisch initiiert
Mit der Re-Zertifizierung werden folgende Funktionen realisiert:

1. Berechtigungsobjekte (Rollen, Systeme), die in bi-Cube einer SC mit Re-Zertifizierungszeitraum unterworfen sind, werden in regelmäßigen Abständen einer Wiederholungsfreigabe durch den Leiter des Users unterworfen.
2. Die SC regelt den Re-Zertifizierungsrhythmus, wenn zur SC ein Zeitraum > 0 (null Monate) eingestellt ist. Eine SC gilt dann als ***rezertifizierungspflichtig***. In der Standard-Konfiguration sind folgende Re-Zertifizierungszeiträume definiert:
   - SC = 5 (top secret) **à** 6 Monate
   - SC = 4 (secret) **à** 6 Monate
   - SC = 3 (confidential) **à** 12 Monate

   Die vordefinierten Zeiträume können nach Einsatzfall geändert werden. Für die SC 0 bis 2 sind im Standard keine Re-Zertifizierungszeiträume definiert, können aber bei Bedarf jederzeit eingerichtet werden.
3. Existieren Systemobjekte mit rezertifizierungspflichtiger SC in einer Rolle, wird nur die Wiederholungsfreigabe lt. SC der Rolle eingefordert, die Re-Zertifizierung des Systems ist dabei inkludiert.
4. Stimmt der Leiter der Re-Zertifizierung zu, wird die nächste Freigabe lt. SC mit entsprechendem Startzeitpunkt für das Berechtigungsobjekt in bi-Cube automatisch initiiert.
5. Lehnt der Leiter die Re-Zertifizierung einer Rolle oder eines direkt zugewiesenen Systems (Einzelberechtigung) ab, werden die Rolle bzw. das Systemobjekt automatisch durch bi-Cube entzogen bzw. deaktiviert.
6. Zum Abschluss des Prozesses erhält der betroffene User eine Information zum Prozess-Verlauf und Ergebnis.

Änderungen zu den Einstellungen der Re-Zertifizierungsrhythmen der einzelnen SC werden wie folgt wirksam:

- Wird für eine SC nachträglich der Zeitraum verlängert oder verkürzt, wirkt sich dies nur für Neuzuweisungen und die automatische Initiierung von Re-Zertifizierungen aus. Bereits initiierte, aber noch nicht gestartete Prozesse laufen zum berechneten Starttermin an.
- Wird für eine SC der Zeitraum nachträglich auf 0 (null) gesetzt (also keine Re-Zertifizierung erforderlich), werden noch nicht gestarteten Prozesse nicht mehr ausgeführt. Bereits laufende Prozesse müssen über den Prozess-Manager im IPM Web-Portal gecancelt werden.
- Wird ein Berechtigungsobjekt, das bereits in bi-Cube verwendet wird (Zuweisungen bei den Usern bereits vorhanden), erstmalig einer SC mit Re-Zertifizierung unterworfen, können die erforderlichen Wiederholungsfreigaben über eine Mengenoperation mit V 7.X.X initiiert werden (verfügbar in einem späteren Release in V7).

2 Modellierungsrichtlinien

Folgende Richtlinien für die Modellierung der Re-Zertifizierung sind zu beachten:

- Die Re-Zertifizierungszeiträume werden kleiner, je höher die ausgewählte SC!
- Die SC im Rollenmodell erfolgt für die Fachrollen.
- Die SC zu den Berechtigungsobjekten (Rolle, System) muss so gesetzt werden, das eine Rolle immer mindestens die gleiche SC aufweist wie das am höchsten eingestufte Systemobjekt in der (Fach-) Rolle. Das bedeutet gleichzeitig, dass eine Rolle immer einer SC unterworfen werden muss, sobald ein Systemobjekt mit rezertifizierungspflichtiger SC zur Rolle gehört. Diese Regel gilt natürlich auch für SC in Systemobjekt-Hierarchien, die in Rollen verwendet werden.
- SC in Systemobjekthierarchien können derart gesetzt werden, das ein untergeordnetes Objekt eine höhere SC besitzt als das Wurzelobjekt (z.B. eine Software innerhalb win, die höher eingestuft ist als Windows selbst).

3 GPM Re-Zertifizierung

Der Prozess zur Re-Zertifizierung wird automatisch gestartet.

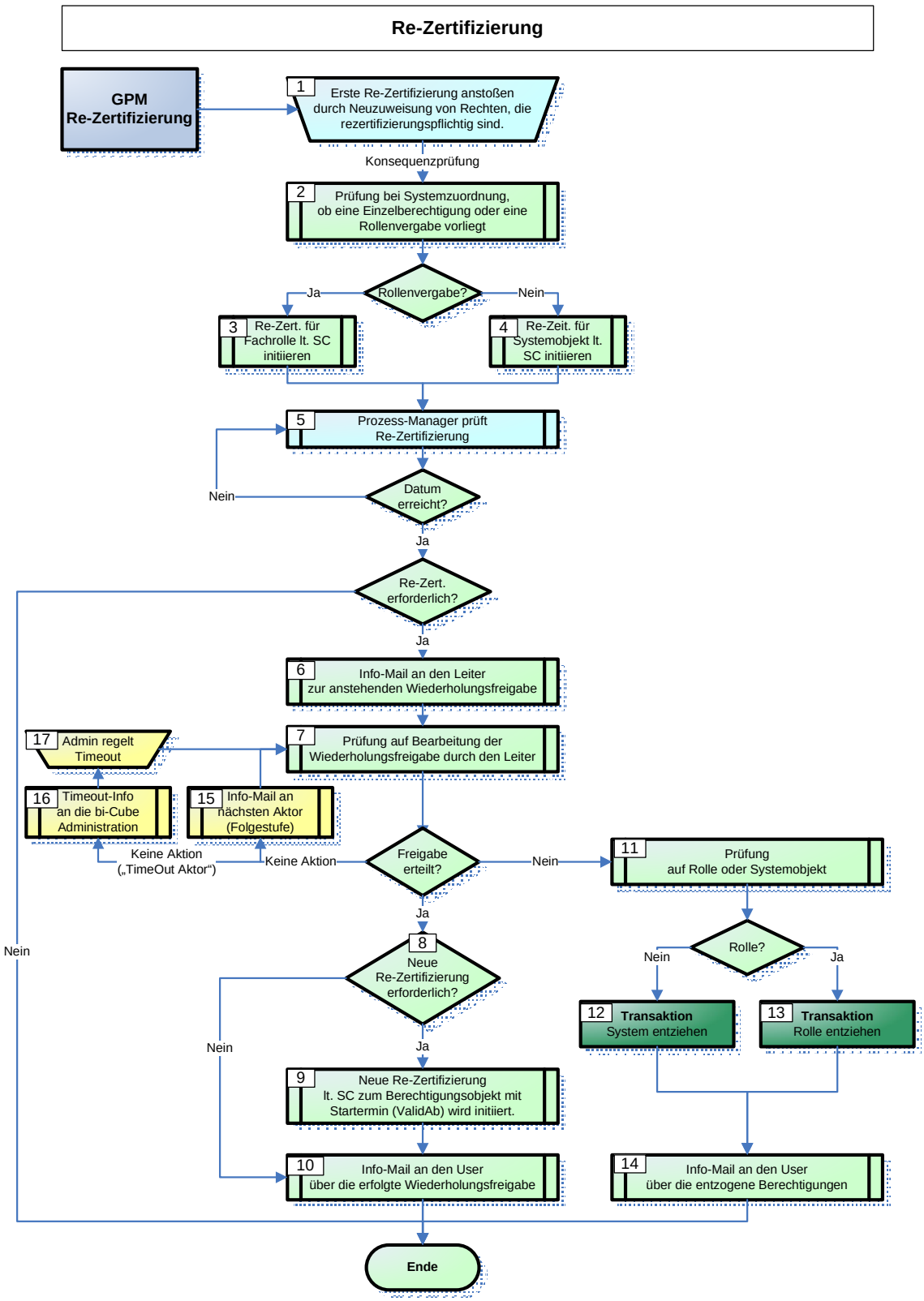

Abbildung 1: GPM Re-Zertifizierung

Erläuterungen zum GPM *Re-Zertifizierung*

1 **Erste Re-Zertifizierung anstoßen:**
Bei Zuweisung rezertifizierungspflichtiger Berechtigungsobjekte (Rollen, Einzelberechtigungen) wird über die Konsequenzprüfung die Re-Zertifizierungs-Schleife für das Objekt angestoßen, siehe Punkt 2.

2 **Prüfung auf Rolle oder Einzelberechtigung:**
Die Konsequenz prüft, ob es sich bei Neuzuweisung eines Systems mit Re-Zertifizierungspflicht um eine Einzelberechtigung oder eine Rollenzuweisung handelt. Je nach Prüfergebnis wird in Punkt 3 oder 4 verzweigt.
Hinweis: Punkt 3 muss nur durchlaufen werden, wenn für die betroffene Rolle noch keine Re-Zertifizierung beim User initiiert ist!

3 **Re-Zert. für Fachrolle:**
Die Prüfung in 2 hat ergeben, das die Systemzuweisung über eine Rolle erfolgt ist. Die Re-Zertifizierung wird ausgehend von der SC der Rolle initiiert, nicht auf Grund der SC des Systems.

4 **Re-Zert. für Einzelberechtigung (Systemobjekt):**
Die Prüfung in 2 hat ergeben, das die Systemzuweisung als Einzelberechtigung (ohne Rolle) erfolgt ist. Die Re-Zertifizierung wird ausgehend von der SC des Systems initiiert.

5 **Re-Zertifizierung starten:**
Der Prozess-Manager startet den eigentlichen Prozess der Re-Zertifizierung genau dann, wenn das Re-Zertifizierungsdatum (ValidAb der Message) erreicht ist. Dabei wird geprüft, ob die SC zum Berechtigungsobjekt noch rezertifizierungspflichitg ist.
D.h. wurde nachträglich der Re-Zertifizierungszeitraum im Customizing für die SC auf 0 (null Monate) gesetzt, wird der Prozess ohne weitere Aktion beendet. Ansonsten stößt der Prozess-Manager die Info-Aktion zur Bearbeitung an, siehe Punkt 6.

6 **Info-Mail an den Leiter:**
Der Aktor (z.B. der Leiter) zur Genehmigung der Wiederholungsfreigabe erhält eine Info per Email, das eine Re-Zertifizierung zur Bearbeitung vorliegt verbunden mit der Aufforderung, diesen Antrag zu bearbeiten.

7 **Prüfung auf Bearbeitung der Re-Zertifizierung:**
Der Aktor (z.B. der Leiter) meldet sich im IPM Web-Portal an und bearbeitet den Antrag zur Wiederholungsfreigabe. Die Überwachung durch den Prozess-Manager kann folgende Ergebnisse erbringen:
Wiederholungsfreigabe bestätigt: Der Leiter hat die Wiederholungsfreigabe für das Berechtigungsobjekt im IPM Web-Portal bestätigt. Der Prozess-Manager leitet weiter zur Initiierung der Folgefreigabe (nächste Re-Zertifizierung des Berechtigungsobjekts), siehe Punkt 8.
Wiederholungsfreigabe abgelehnt: Der Leiter hat die Freigabe abgelehnt. Der Prozess-Manager leitet weiter zum Entzug der Berechtigungen, siehe Punkt 11.
Keine manuelle Aktion: Die Bearbeitung des Auftrags durch den Aktor erfolgte nicht im dafür vorgesehenen Zeitraum. Der Prozess-Manager leitet weiter zur Erinnerung, siehe Punkt 15.

8 **Neue Re-Zertifizierung erforderlich?**
Für das Berechtigungsobjekt wird auf Grundlage der SC geprüft, ob eine erneute Re-Zertifizierung initiiert werden muss:
Ja: Die beim Objekt (Rolle, System) eingestellte SC ist immer noch rezertifizierungspflichtig. Der Prozess-Manager leitet weiter zur Initiierung der Re-Zertifizierung, siehe Punkt 9.
Nein: Lt. SC ist das Berechtigungsobjekt nicht (mehr) rezeritfizierungspflichtig. Der Prozess-Manager leitet weiter zur Abschluss-Info, siehe Punkt 10.

9 **Neue Re-Zertifizierung lt. SC initiieren:**
Nach erfolgter Re-Zertifizierung wird die nächste Wiederholungsfreigabe automatisch initiiert, das auf Grundlage der aktuellen Einstellung für den Re-Zertifizierungszeitraum für die SC am Berechtigungsobjekt. Ist zwischenzeitlich die Definition für die SC auf 0 (null Monate) gesetzt worden, wird keine neue Re-Zertifizierung für das Berechtigungsobjekt (Rolle, System) initiiert. Danach leitet der Prozess-Manager weiter zur Abschluss-Info für die Re-Zertifizierung, siehe Punkt 10.

10 **Info-Mail an den User über Wiederholungsfreigabe:**
Zum Abschluss der erfolgten Re-Zertifizierung wird der betroffene User per Mail über das Ergebnis informiert.

11 **Prüfung auf Rolle oder Systemobjekt:**
Nach Ablehnung der Wiederholungsfreigabe wird geprüft, ob es sich bei dem Berechtigungsobjekt um eine Rolle handelt.
Ja: Das Berechtigungsobjekt ist eine Rolle, es wird weitergeleitet zum Sub-Prozess *Rolle entziehen*, siehe Punkt 13.
Nein: Bei dem Berechtigungsobjekt handelt es sich um eine Einzelberechtigung (Systemobjekt), es wird weitergeleitet zum Sub-Prozess *System entziehen*, siehe Punkt 12.

12 **Transaktion System entziehen (siehe auch Beschreibung der Transaktionen):**
Das zum Entzug vorgesehene System und alle dazu gehörenden Berechtigungen werden dem User entzogen.
Handelt es sich um ein Zugangssystem, dann wird das Zugangssystem gesperrt und je nach Customizing-Einstellung zum Systemobjekt nach einer Nachlaufzeit gelöscht.
Die Transaktionen werden vom Transaktionsmonitor überwacht und Fehlermeldungen aus den Schnittstellen (Connectoren) an die bi-Cube Administration gemeldet. Nach erfolgreichem Abschluss der Transaktionen wird intern zur nächsten Aktion weitergeleitet (siehe Punk 14).

13 **Transaktion Rolle entziehen (siehe auch Beschreibung der Transaktionen):**
Die zum Entzug vorgesehene Rolle und alle dazu gehörenden Berechtigungen werden unter Berücksichtigung der Rollenkonfliktauflösung entzogen.
Befindet sich in der Rolle ein Zugangssystem, das durch keine andere Rolle mehr beim User zugewiesen ist, dann wird das Zugangssystem gesperrt und je nach Customizing-Einstellung zum Systemobjekt nach einer Nachlaufzeit gelöscht.
Die Transaktionen werden vom Transaktionsmonitor überwacht und Fehlermeldungen aus den Schnittstellen (Connectoren) an die bi-Cube Administration gemeldet. Nach erfolgreichem Abschluss der Transaktionen wird intern zur nächsten Aktion weitergeleitet (siehe Punkt 14)

14 **Info-Mail an der User über Berechtigungsentzug:**
Zum Abschluss der nicht bestätigten Re-Zertifizierung wird der betroffene User per Mail über das Ergebnis und den Entzug der Berechtigungen informiert.

15 **Keine manuelle Aktion:**
Die Bearbeitung des Antrags durch den Aktor erfolgte nicht im dafür vorgesehenen Zeitraum. Es wird eine **Info-Mail** an die Stellvertretung des Aktors verschickt (nächste Stufe zur gleichen Aktion) verschickt, damit die die Bearbeitung des Auftrags erfolgt.

16 **Timeout-Info:**
Für die Bearbeitung des Antrags ist das Timeout eingetreten, d.h. es erfolgte keine manuelle Bearbeitung durch einen Aktor im Timeout Zeitfenster. Eine Timeout-Info wird per Email an die bi-Cube Administration verschickt. Diese Timeout-Info kann auch an eine andere Adressatengruppe verschickt werden, einzustellen in der Aktion im Prozess-Modell.

17 **Admin regelt Timeout:**
Bei Timeout-Info muss die bi-Cube Administration eingreifen und z.B. die zuständigen Aktoren auffordern, Ihren Job zu erledigen.