INSTITUT FÜR SYSTEM-MANAGEMENT

Generische Prozess-Modelle

Prio	Gruppe	Core Prozess	spezielle Ausprägungen	Ziel / Inhalt	Auslöser
	Wechselprozesse des Users				
X		Mitarbeitereintritt		Neue Mitarbeiter erhalten in einem automatisierten Prozess alle erforderlichen (Basis-)Rechte, um im Prinzip arbeiten und an dem System und seinen Prozessen teilnehmen zu können. Sie können dann auch weitere Rollen beantragen (siehe Antragsverfahren).	Neuer Mitarbeiter wird im IAM System eingetragen über autom. Userimport (z.B. aus SAP) oder manuelle dezentrale Erfassung (z.B. für Externe)
X		Mitarbeiteraustritt		Ein GPM steuert den geordneten Mitarbeiteraustritt mit den verschiedenen Möglichkeiten der Rechtereduzierung und unterschiedlichen zeitlichen Abstufungen (sog. Nachlaufzeiten).	Das Austrittsdatum wird erreicht oder der User-Status im IAM System auf "ausgetreten" gesetzt.
			Sofortiges Usersperren	Kritische Austritte eines Users erfordern die sofortige Sperrung der wichtigsten Zugangssysteme für diesen User. Dies muss u.U. deutlich vor dem arbeitsrechtlichen Austritt erfolgen. Die Sperre kann aber auch in den regulären Austrittsprozeß übergehen.	Anweisung vom P-Leitung, die Zugangssysteme werden in den Status "gesperrt" gesetzt oder regulärer MA-Austritt
X		Wechsel im Unternehmen		Bei einer Rollenänderung (z.B. durch OE-Wechsel) können die Berechtigungen nicht schlagartig wechseln. Dazu existieren sog. Vor- und Nachlaufzeiten und entsprechende konfigurierbare Regeln. Wechselprozesse sind komplex und dienen dazu, das ein Mitarbeiter nicht nur zusätzliche Rechte bekommt sondern ihm auch nicht mehr erforderliche Rechte entzogen werden.	Änderungen am User (z.B. neue OE-Zuordnung) lösen den Prozess aus

			Wiedereintritt innerhalb des Konzerns	In Konzernen mit weitgehend eigenständigen Unternehmen ist ein Mitarbeiterwechsel formal ein Austritt und Eintritt eines neuen Mitarbeiters. In den dazu führenden P-Systemen hat der Mitarbeiter dann auch eine neue Identität d.h. eine neue Personal-Nummer. Aus IAM-Sicht ist dies aber kein neuer Mitarbeiter, sondern ein komplexer Wechselprozess desselben Mitarbeiters. Um dies zu erkennen, ist in dem IAM-System eine Dublettenkontrolle unverzichtbar	vorhandener Mitarbeiter wird erneut aus P-Systemen geliefert und als Dublette erkannt
			Shadow User (User in einer weiteren OE)	Der User wird einer weiteren Organisationseinheit zugeordnet. Für ihn können jetzt durch den zuständigen Leiter weitere Rechte (Rollen) beantragt werden	
	Antrags- und Provisioning-Verfahren				
X		Antragsverfahren Rollen		Abhängig von bestimmten technischen User-Attributen kann ein User bzw. ein für diesen User Berechtigter (z.B. der Leiter) Fachrollen beantragen.	Antrag des Users oder zuständigen Leiters
X			Automatische regelbasierte Rollenzuteilung	Die Rollenzuteilung erfolgt nach Antragstellung automatisch, wen für die Rolle und die dazu festgelegten Systemprofile keine zusätzlichen Genehmigungen erforderlich sind.	Antrag des Users oder zuständigen Leiters
			Richtlinienabhängiges Provisioning	Bestimmte System- oder auch Rollenzuordnungen werden in einem GPM mit der Bestätigung einer Benutzer-Richtlinie verbunden. Ohne die Bestätigung dieser Richtlinie wird dem User die Berechtigung nicht erteilt. Seine Bestätigung ist nachweisbar.	Bestimmte Systeme / Rollen sind als richtlinienabhängig gekennzeichnet

			Nachträgliche Änderung techn. Attribute an der Rolle	Änderungsantrag für technische Attribute zu bereits beim User vergebenen Rollen	manueller Antrag des Users
			Mit differenzierter Beibringung der Attribute	Antrag auf eine neue Rolle für den User, die technischen Attribute werden je nach Festlegung einzeln durch verschiedene Akteure im Prozess eingetragen.	Antrag auf neue Rolle
		Teamrollen		Teammitgliedern (z.B. in Projektteams) werden zeitlich begrenzt Rechte für die Projektarbeit zugeteilt. GPM ist noch in der Spezifizierung	User wird Mitglied eines Teams
X		Allgemeiner dokumentenbasierter Antrags-Prozess		Für Anträge, die sich nicht in die genannten GPM einordnen lassen, ist ein allgemeiner Antrags-Prozess zu nutzen, der sich auf Dokumentvorlagen stützt. Dabei kann das allg. Modell so angepasst werden, das der Prozessablauf den Erfordernissen des jeweiligen Dokuments entspricht, z.B. einen mehrstufigen Genehmigungsprozess abbildet. Für jede Dok.-Vorlage wird ein separates Prozess-Modell hinterlegt.	Antrag des Users oder zuständigen Leiters
			Sonderfall: kein Prozess definiert	Der User will eine bestimmten Berechtigung / Ressource anfordern, für deren Zuteilung es keinen Prozess gibt. Eine spezielle Dok.-Vorlage ermöglicht die Anfrage dazu nach definiertem Ablauf in einem Trouble-Shooting.	Antrag des Users oder zuständigen Leiters
		dokumentenbasierter Antrag nach SDI Verfahren (Secure Document Interchange)		Für dokumenetenbasierte Anträge nach SDI-Verfahren ist **ein** Modell hinterlegt, die Adressaten werden über Indizierung (auf Rollen, OE, Teams…) zur jeweiligen Dokumentenvorlage festgelegt. Der Versender erhält Infos zum Abruf und Bestätigung des Dokuments durch die Adressaten, das Dokument wird an einen Final User zur Ausführung weitergeleitet.	SDI-Session wird vom Versender gestartet, nachdem er das Dokument im Dok-Server hinterlegt hat

X		Antrag für allgemeine Applikationen		Bestimmte Systeme werden allen Usern oder definierten Teilmengen der User zum Antrag bereitgestellt. In der Regel sind das lizenzpflichtige oder ressourcenintensive Anwendungen (z.B. Graphik-Tool oder Adobe,…), deren Nutzung beantragt und genehmigt werden soll. Diese Applikationen haben keine differenzierte Rechtestruktur	Antrag des Users oder zuständigen Leiters
		Signatur-Management in PKI		GPM ist in der Spezifizierung	
	Wiederholungs-freigaben				
		Re-Lizensierung (regelmäßige Bestätigung einer bereits erteilten Lizenz)		Im Zuge der Lizenzoptimierung müssen bestimmte Systeme regelmäßig neu bestätigt werden, um die bereits erteilte Lizenz zu erneuern	Erreichen des zentralen Re-Lizenzierungsdatums für alle erteilten Rechte zu einem lizenzpflichtigen System
X		Re-Zertifizierung (regelmäßige Bestätigung eines bereits erteilten Nutzungsrechts)		Zur Sicherung der Compliance (SOX, 8. EU-Richtlinie,..) bedürfen bereits erteilte Nutzungsrechte einer regelmäßige Bestätigung durch den Leiter	Ablauf des Zertifizierungszeitraums für alle erteilten Rechte zum jeweiligen System beim User
		Re-Validierung		Bestätigung der Existenz eines Users und dessen Status (intern, extern..)	Ablauf des Validierungszeitraums für den User
	Nebengelagerte Prozesse				

		Antrag auf einen Arbeitsplatz		Ein definierter Prozess ermöglicht es dem Leiter, für einen Mitarbeiter einen Arbeitsplatz zu beantragen, zu reservieren oder freizugeben. Dieser IPM-Prozess erfordert die Verwaltung von FM-Daten im IAM System	Antrag des zuständigen Leiters
			Antrag auf Änderung der Arbeitsplatzausstattung		Antrag des Useres oder zuständigen Leiters
		Rollenbasierter Antrag auf eine Zutrittsberechtigung		Bestimmte Rollen können mit Zutrittsrechten verbunden werden. Beispiel: Ein Unix-Admin hat nicht nur die Rechte auf den Unix-Systemen sondern auch das Zutrittsrecht zu den	Antrag auf eine Rolle, die mit Zutrittsberechtigung verbunden ist
		Antrag zur Abwesenheit		Dieser Antrag (Urlaubsantrag) ermöglicht es, nach Genehmigung die Abwesenheiten im IAM-System zu erfassen, diese Abwesenheiten steuern in anderen GPM die Aufgabenverteilung und können, wenn erforderlich, das vorübergehende Sperren von Zutrittssystemen auslösen.	Antrag des Users oder zuständigen Leiters
			Antrag zum Urlaub	siehe Antrag zur Abwesenheit	Antrag des Users
	Serviceprozesse				
		Password Self-Service		Bei Problemen mit fehlenden Berechtigungen ist ein IPM-Prozess für eine allgemeine Nachfrage definiert. Z.B. ein User meint, dass er fehlende Rechte hat, um seine Arbeit tun zu können, kann das Problem aber nicht näher beschreiben.	manuller (mündlicher) Antrag des Users beim Leiter
		Allgemeine Supportanfrage		Bei Problemen mit fehlenden Berechtigungen ist ein IPM-Prozess für eine allgemeine Nachfrage definiert. Z.B. ein User meint, dass er fehlende Rechte hat, um seine Arbeit tun zu können, kann das Problem aber nicht näher beschreiben.	manuller Antrag des Users
	Interne Prozesse				

		Antrag für neue Rollen		Einen neue Rolle soll designed im Rollenmodell hinterlegt werden.	
		Antrag zur Rollen-Änderng		Eine vorhandene Rolle soll im Rollenmodell geändert werden.	
			Technische Attribute	Änderung in der Definition von technischen Attributen	
			Berechtigungattribute	Änderung in der Definition von Berechtigungsattributen in der Rolle	
		Antrag für Modellierungs-änderungen		Modellierungsänderungen im IAM System	
		Freigaben im gesicherten Betriebskonzept		neue oder geänderte Modellierungen sind getestet und werden z.B. von der Revision für die Nutzng im produktiven System freigegeben.	
		Analytische Rollenmodellierung SoP		Das System unterbreitet nach mathematischer Analyse der vorhandenen Rechte (Näherungsverfahren, Ähnlichkeitsmaß) Vorschläge zur Rollenmodellierung (synthetische Rollen). Diese können automatiosche in das Reollenmodell übernommen und ggf. noch angepasst werden.	