

**ipg rolmine® 1.1****Product Report****© Kuppinger Cole + Partner, Digital ID Analysis + Evaluation, 2008****Autor: Martin Kuppinger****1 Executive Summary**

---

Die aktuellen Marktanalysen von Kuppinger Cole machen deutlich, dass sich das Rollenmanagement in den vergangenen drei Jahren zu einem Kernthema für das Identity und Access Management und das neu entstandene Marktsegment GRC (Governance, Risk Management, Compliance) entwickelt hat. In kaum einem anderen Teilbereich sind so viele Projekte geplant.

Die effiziente Umsetzung von Rollenmodellen setzt aber neben der Top-Down-Modellierung auch eine Analyse der vorhandenen Berechtigungsstrukturen, das so genannte Role Mining, voraus. Dafür braucht es spezielle Analysewerkzeuge, die aber auch das kontinuierliche Rollenmanagement unterstützen müssen.

Die Schweizer ipg AG liefert mit rolmine® eine solche Lösung, die alle wesentlichen Anforderungen unterstützt. Zusätzlich kann sie auch für die Verbesserung der Datenqualität von Identitätsdaten eingesetzt werden. Das Produkt kann wesentlich dazu beitragen, die Prozesse für die Erstellung und Pflege von Rollenmodellen zu vereinfachen und zu optimieren und damit einen wichtigen Wertbeitrag für diese Kernherausforderung der IT leisten.

**2 Kernpunkte der Analyse**

---

- |                                                                                      |                                                                                                              |
|--------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------|
| ➤ Unterstützt das Role Mining und ein kontinuierliches Rollenmanagement.             | ➔ Noch sehr wenige Partner, Partner-Infrastruktur aber im Aufbau.                                            |
| ➤ Einfach nutzbare grafische Schnittstellen.                                         | ➤ Berücksichtigt Organisationsstrukturen bei den Vorschlägen für Kandidatenrollen.                           |
| ➔ Nur manuelle, aber gut dokumentierte Import- und Exportschnittstellen.             | ➔ Derzeit nur ein unterstützter Strukturbaum.                                                                |
| ➤ Unterstützt auch die Optimierung der Datenqualität von Identitätsdaten.            | ➔ Ergebnisse des Role Minings sind gut, aber nicht ausreichend mit statistischen Informationen dokumentiert. |
| ➤ Verwendeter Algorithmus ist leistungsfähig und liefert eine hohe Ergebnisqualität. |                                                                                                              |
| ➤ Steuerungsparameter für das Role Mining sind unzureichend.                         |                                                                                                              |
| ➤ Geringer Ressourcenbedarf.                                                         |                                                                                                              |
| ➤ Gute Ergebnisqualität.                                                             |                                                                                                              |
| ➤ Unterstützt auch Abstimmungsprozesse mit Rollenbesitzern.                          |                                                                                                              |

### **3 Produktkategorie**

---

Das Produkt rolmine® der Schweizer ipg AG gehört zur Gruppe der Rollenmanagement-Werkzeuge, wobei der Schwerpunkt auf dem Role Mining liegt, also der Analyse bestehender Berechtigungen, um auf dieser Basis neue Rollen zu generieren. Rollenmanagement-Lösungen sind wiederum ein Teilbereich der generischen GRC-Tools (Governance, Risk Management, Compliance). Diese unterstützen bei der Umsetzung der GRC-Anforderungen. Dabei haben Business- und IT-Rollen eine zentrale Bedeutung, weil wesentliche GRC-Anforderungen nur mit Hilfe von rollengestützten Verwaltungsansätzen effizient umzusetzen sind. Dazu zählen das Autorisierungsmanagement, also die Vergabe von Autorisierungen (Berechtigungen, Entitlements) ebenso wie die Steuerung von SoDs (Segregation of Duties, sich gegenseitig ausschließende Berechtigungen) oder die Attestierung von Autorisierungen.

Die effiziente Umsetzung von GRC-Anforderungen, sei es mit speziellen GRC-Werkzeugen als steuernde und kontrollierende Instanz oberhalb von Provisioning-Lösungen oder direkt mit Hilfe von Provisioning-Systemen mit Rollenunterstützung, ist daher auf optimierte Rollenmodelle angewiesen.

Um diese Modelle zu entwickeln, arbeitet man in der Regel mit einem Prozess, bei dem sowohl Top-Down- als auch Bottom-Up-Ansätze genutzt werden. In diesem Prozess wird zunächst ein einfaches, grundlegendes Rollenmodell, gegebenenfalls auch nur für einen Teilbereich der Organisation, entwickelt, um es dann schrittweise zu verfeinern.

Bei der Top-Down-Vorgehensweise werden Informationen wie die Organisations- und Projektstrukturen, Job-Beschreibungen und weitere Ausgangsdaten genutzt, um ein Rollenmodell zu definieren. Der Bottom-Up-Ansatz basiert dagegen auf vorhandenen Berechtigungen in angeschlossenen Systemen und versucht darin Ähnlichkeiten zu ermitteln. Für diese Fälle werden so genannte Kandidatenrollen (Candidate Roles) vorgeschlagen.

Die Kombination beider Ansätze ist sinnvoll, um einerseits die vorhandenen Informationen berücksichtigen zu können, sie aber nicht unreflektiert zu übernehmen, sondern in optimierter Weise auf die Organisation umzusetzen.

Nach Ansicht von Kuppinger Cole setzt ein effizientes Role Mining sogar voraus, dass man die beiden Ansätze miteinander verbindet und beispielsweise die Organisationsstrukturen bei der Modellierung von Kandidatenrollen einbezieht, um auch sinnvoll umsetzbare Vorschläge zu erhalten. Wenn beispielsweise eine Kandidatenrolle Mitarbeiter aus unterschiedlichen Organisationseinheiten umfasst, ist sie oft schon deshalb nicht umsetzbar, weil es keine einheitliche Verantwortung und damit Zuordnungsmöglichkeit für die Rolle gibt. Allerdings sollte auch die Bildung übergeordneter Rollen beispielsweise für einen Teil der Berechtigungen zugelassen werden, wobei Konflikte und Überschneidungen zwischen den Berechtigungen zu vermeiden sind.

Trotz der aktuellen Entwicklung, innerhalb von generischen GRC-Lösungen immer mehr Funktionen für das Rollenmanagement einschließlich des Role Minings zu integrieren, sehen wir auch weiterhin einen eigenständigen Markt für solche Werkzeuge als Ergänzung zu den (vielen) GRC- und Provisioning-Produkten, die noch nicht mit eigenständigen Funktionen in diesem Bereich ausgestattet sind.

**Product Report: ipg rolmine® 1.1**

---

**4 Produktbeschreibung**

---

Das Produkt rolmine® ist eine Web-Anwendung, die einen integrierten Web-Server und eine integrierte Datenbank nutzt. Python spielt für die Implementierung eine wesentliche Rolle. Es gibt insgesamt vier wesentliche Schnittstellen:

- Die Web-Schnittstelle, die von Anwendern für die Definition von Rollen verwendet wird.
- Die Administrationsschnittstelle, die für Grundfunktionen wie den Import und Export von Daten genutzt wird.
- Utility-Funktionen für spezielle administrative Aufgaben.
- Eine Konfigurationsdatei für die Parameter, die das Verhalten des Systems insbesondere beim Role Mining steuern.

Die Anwendung läuft auf allen gängigen Betriebssystemen, wobei unter Windows sowohl Windows-Arbeitsstationen als auch Server-Systeme unterstützt werden. Die Systemvoraussetzungen sind vergleichsweise gering, was aber vor allem in der spezialisierten Funktion begründet liegt. Für komplexe Analysen ist dennoch ein erheblicher Bedarf an Hauptspeicher und Rechenzeit einzukalkulieren.

Bei der Analyse werden zunächst vorhandene Informationen wie HR-Daten zu den Benutzern und Organisationsstrukturen, zu Berechtigungen und bereits definierten Rollen eingelesen. Diese werden in die Datenbank übernommen und bilden die Grundlage des Role Minings. Die vorbereitenden Schritte werden über die administrative Schnittstelle durchgeführt.

Die Analyse der Daten, die Bearbeitung der Kandidatenrollen und die Umsetzung in die gewünschten Rollen erfolgt dagegen über die Benutzerschnittstelle. Hier kann eine sehr differenzierte Bearbeitung durchgeführt werden, bei der unter anderem auch sicherheitssensitive Rollen in gesonderter Weise bearbeitet werden.

Die Ergebnisse können wiederum über Exportschnittstellen ausgegeben werden, um anschließend Eingangsdaten von GRC- und Provisioning-Produkten zu bilden. Derzeit gibt es zwar aus Projekten heraus vordefinierte Lösungen zur Integration, aber noch keine Standardanbindung für eine automatisierte Übergabe der Informationen an nachgelagerte Systeme.

Damit ist rolmine® eine Offline-Lösung, die isoliert betrieben wird und werden kann. Da es sich bei der Rollenanalyse und dem Rollenmanagement um eine sehr spezielle Aufgabenstellung handelt, ist eine solche direkte Integration auch nicht unbedingt zwingend – umso mehr, als es normalerweise keine Notwendigkeit gibt, Änderungen am Rollenmodell unmittelbar in die Produktionssysteme zu übernehmen.

## **5 Role Mining**

---

Die Kernfunktionalität von rolmine® ist das Role Mining, also die Analyse von Informationen über vorhandenen Berechtigungen, Rollen und andere Daten nach Übereinstimmungen, um darauf basierend mögliche sinnvolle Rollen vorzuschlagen.

Der erste Schritt ist dabei eine Bereinigung der Informationen, auch als Cleansing bezeichnet. Dabei werden beispielsweise verwaiste Benutzerkonten und Berechtigungen mit nicht mehr vorhandenen Benutzern entdeckt. Diese speziellen Informationen können über gesonderte Berichte ausgegeben werden. Das Produkt geht damit über die normalen Funktionen des Rollenmanagements und der Analyse hinaus und kann mit diesen Berichten auch im Vorfeld von Provisioning-Projekten beziehungsweise vor der Einbindung weiterer Systeme eingesetzt werden, um eine Bereinigung der Daten durchzuführen.

Beim Wechsel zur administrativen Schnittstelle kann anschließend eine Analyse auf der Ebene von Organisationseinheiten oder Teilbäumen der Organisation durchgeführt werden. Eine Abbildung der Organisation ist also in jedem Fall erforderlich.

Etwas umständlich sind die Steuerungsmöglichkeiten für die Analyse. Parameter wie beispielsweise die Mindestzahl der Benutzer in einer vorgeschlagenen Rolle oder Einstellungen, die die „Schärfe“ der Analyse im Sinne der Übereinstimmungen zwischen den Benutzern in einer Kandidatenrolle steuern, lassen sich entweder nicht oder nur über die Konfigurationsdatei anpassen, aber nicht differenziert pro Analysevorgang durchführen. Hier gibt es noch Verbesserungspotenzial, um flexibler unterschiedliche Vorschläge für Kandidatenrollen erstellen, speichern, miteinander zu vergleichen und anschließend nutzen zu können.

Der verwendete Algorithmus des Produkts ist nicht dokumentiert, wird aber auf Anfrage genannt. Er liefert sehr gute Ergebnisse in der Analysequalität. Allerdings gilt hier auch, dass eine Kenntnis des Algorithmus ohnehin nur für Experten und bei Verfügbarkeit einer größeren Zahl von Anpassungsparametern für das Feintuning relevant ist. Der Algorithmus ist der so genannte „genetische Optimierungsalgorithmus“.

Generell gilt, dass die Analyseergebnisse eine gute und sinnvolle Grundlage für das weitere Rollenmanagement darstellen, auch wenn man sich weitere einfach zu nutzende Stellschrauben wünschen würde.

Bei der Analyse werden die organisatorischen Zusammenhänge berücksichtigt und nur unter diesem Aspekt sinnvolle Kandidatenrollen gebildet. Diese können allerdings später zu übergeordneten Rollen zusammengefasst werden, falls ein gemeinsames Management doch Sinn macht. Diese werden von ipg als Super-Rollen bezeichnet.

Die in übergeordneten Rollen verwalteten Rechte – es müssen nicht alle Berechtigungen sein - verschwinden automatisch in den untergeordneten Rollen, um Redundanzen und Konflikte zu vermeiden.

## **6 Role Engineering**

---

Auf Basis der automatischen Analyseergebnisse kann anschließend die Bearbeitung der Rollen erfolgen. Im Vergleich zur ersten Version wurde die grafische Schnittstelle schon wesentlich verbessert, so dass man auch bei Organisationseinheiten mit vielen Benutzern und bei komplexeren Gruppen sehr gut arbeiten kann. Etwas mehr Varianten bei den Darstellungen, insbesondere für größere Datenmengen, und die Möglichkeit für den Anwender, frei zu entscheiden, ab welchen Benutzerzahlen er zwischen welchen Darstellungsformen wechselt, wäre aber auch hier nicht nachteilig.

Eine weitere Schwachstelle ist, dass derzeit nur eine Organisationsstruktur oder Projektstruktur abgebildet werden kann, also nur eine Variante eines Strukturbaums. Damit lassen sich beispielsweise nicht parallel die eigentliche Aufbauorganisation, eine parallele Projektorganisation und geografische Strukturen von Unternehmen darstellen - zumindest nicht ohne „Kunstgriffe“ wie der Umsetzung dieser Informationen als parallele Strukturen innerhalb eines übergeordneten Organisationsbaums. Für die nächste Version ist die Unterstützung mehrerer solcher Strukturbäume geplant.

Dennoch ist die Anwendbarkeit gut. Auf Basis der ermittelten Informationen lassen sich sowohl übergeordnete Business-Rollen als auch Systemrollen mit unterschiedlichen Detailberechtigungen erstellen. Der Detaillierungsgrad ist dabei letztlich nur von der Granularität und dem Umfang der importierten Daten abhängig.

Hilfreich wäre es allerdings, wenn es bei den vorgeschlagenen Kandidatenrollen ergänzende statistische Informationen gäbe wie den Übereinstimmungsgrad. Das hilft, schnell die wirklich sinnvollen und zu präferierenden Rollen zu selektieren.

Positiv ist, dass Rollen sowohl als statische wie auch als dynamische Rollen definiert werden können. Außerdem wird neben der Analyse von Rollen im Role Mining und der Nachbearbeitung der vorgeschlagenen Kandidatenrollen auch eine manuelle Definition von Rollen unterstützt.

Die Entstehungsgeschichte des Produkts in Projekten wird bei den sauberen Schnittstellen für die abschließende Beschreibung und Vereinbarung über Rollen deutlich. Die ipg AG ist ein Unternehmen, das das Thema Rollenmanagement über Prozessberatungsprojekte entwickelt hat. Dazu zählen eben auch definierte Prozesse für die Dokumentation der Rollen und ihre Abstimmung mit den Fachbereichen und Rolleneignern.

Wichtig ist noch einmal festzuhalten, dass sowohl die Definition und Umsetzung von Business-Rollen als auch die von IT-Rollen unterstützt werden.

## **7 Benutzerschnittstellen**

---

Die beiden grafischen Benutzerschnittstellen des Produkts für die Administration und für die eigentliche Rollenverwaltung wurden bereits erwähnt. Die administrative Schnittstelle ist dabei sehr einfach, aber durchaus übersichtlich strukturiert und unterstützt wesentliche Grundfunktionen wie den Import und Export sowie die Aktualisierung, Sicherung und Wartung der verwendeten Datenbank. Die Funktionen sind auf dieser Ebene mit wenig Einarbeitungsaufwand nutzbar. Allerdings setzt der Import die Kenntnis der definierten Datenformate voraus. Die Eingabedaten müssen in einem vorgeschriebenen Format vorliegen. Die Erzeugung der entsprechenden Datenstrukturen ist aber grundsätzlich mit gängigen Werkzeugen – angefangen bei Microsoft Excel – einfach.

Die zweite grafische Schnittstelle richtet sich an den Endbenutzer im Sinne der Verantwortlichen für das eigentliche Rollenmanagement, also das Design von Rollen basierend auf den Ergebnissen des Role Minings. Diese Schnittstelle bietet einen deutlich größeren Funktionsumfang und ist einfach nutzbar. Trotz einiger bereits angesprochener Verbesserungspotenziale lässt sich über sie das Rollenmanagement mit einem sehr geringen Einarbeitungsaufwand und einem hohen Maß an Effizienz durchführen.

## **8 Integrationsschnittstellen**

---

Rollenmanagement-Produkte wie rolmine® werden nicht isoliert eingesetzt. Sie arbeiten eng mit GRC- und Provisioning-Lösungen zusammen. Gleichzeitig setzen sie aber auch auf Ist-Daten aus den Zielsystemen auf. Daher spielen die Schnittstellen sowohl zu den Systemen, deren Berechtigungsstrukturen die Ausgangsbasis für das Rollenmanagement bilden als auch zu den übergeordneten Provisioning- und GRC-Lösungen eine wichtige Rolle.

Bei rolmine® wird mit Import- und Export-Schnittstellen für die Übergabe der Informationen gearbeitet, wobei es genau definierte Dateiformate gibt. Es gibt standardmäßig keine Online-Verbindung zu anderen Systemen. Das ist allerdings auch nicht zwingend, weil es in der Praxis kein Erfordernis für eine Realtime-Kopplung gibt. Änderungen an Rollen müssen in der Regel in einem längeren Prozess definiert und freigegeben werden, bevor sie in die produktiven Systeme umgesetzt werden.

Die Aufbereitung der Daten, die für das Role Mining verwendet werden, muss ebenfalls pro System erfolgen. Die meisten angeschlossenen Systeme bieten aber standardmäßig geeignete Export-Funktionen an, mit denen die Daten ausgegeben werden können. Eine Umsetzung in die von rolmine® benötigten Datenstrukturen ist einfach. Zudem verfügen die ipg AG und ihre Partner inzwischen auch über eine breite Projekterfahrung bei der Extraktion der erforderlichen Informationen. Die Bereitstellung spezieller Connectoren in diesem Bereich wäre zwar denkbar, ist aber insgesamt wenig sinnvoll, da es wie ausgeführt in der Regel Tools für die Extraktion gibt und sich dieser einmalige Prozess daher gut auf die beschriebene Weise bewältigen lässt.

Interessanter wären solche Standard-Schnittstellen für die Kopplung zwischen rolmine® und den konsumierenden GRC- und Provisioning-Produkten. Hier gibt es aus Projekten entstandene Anbindungen beispielsweise an den B HOLD, BMC Control-SA und Siemens DirX. Hier wären aber Erweiterungen wünschenswert, wobei auch an dieser Stelle keine Online-Kopplung erforderlich ist, sondern nur standardisierte Übergabeschnittstellen an die von den Zielsystemen definierten Interfaces.

## **9 Einsatzbereich und Nutzenpotenziale**

---

Der Haupteinsatzbereich von rolmine® liegt in der Analyse und Modellierung von Rollen, wobei die Funktionalität über das reine Role Mining (im Sinne der Bottom-Up-Analyse) hinausgeht und das Rollenmanagement einschließlich der Top-Down-Modellierung adressiert wird. Insofern ist der Produktname etwas einschränkend.

Eine solche standardisierte Modellierung von Rollen ist sowohl für Provisioning- als auch GRC-Projekte unverzichtbar, da effiziente Implementierungen auf Rollenmodellen für die Steuerung der Berechtigungsvergabe, die Definition von SoD-Regeln und die Attestierung aufsetzen.

Richtig umgesetzt reduzieren Rollenprojekte dabei den administrativen Aufwand erheblich, weil mit den Business- und IT-Rollen als zusammenfassenden Konstrukten gearbeitet werden kann, statt Einzelberechtigungen zu vergeben.

Neben dieser Kernfunktionalität sind auch noch die Fähigkeiten des Produkts zum Data Cleansing erwähnenswert. Hier liegt ein zusätzlicher Nutzen, da die Schaffung einer hohen Datenqualität bei Identitätsdaten in jedem Identity Management-Projekt ein zentraler, vorgeschalteter Schritt ist, der allerdings auch beim Anschluss weiterer Systeme immer wieder durchgeführt werden muss.

Dabei werden verschiedene wichtige Funktionen unterstützt wie die Analyse der Daten beim Ladevorgang und die Erkennung von fehlerhaften Informationen. Diese Informationen werden auch im Role Mining-Prozess nicht berücksichtigt, können aber als Basis für die Bereinigung der ursprünglichen Datenquelle berücksichtigt werden.

Durch diese kontinuierlichen Aufgaben, insbesondere natürlich das Rollenmanagement, ist rolmine® definitiv ein Werkzeug, das über die initialen Phasen von Projekten und für den dauerhaften Einsatz sinnvoll ist.

**Product Report: ipg rolmine® 1.1**

---

**10 Partner-Infrastruktur**

---

Gerade bei Unternehmen, die relativ neu in einem Markt sind, stellt sich die Frage nach den Partnern, mit denen dieser Markt adressiert wird. Im Fall der ipg AG steht hinter dem Produkt zwar ein etabliertes Schweizer IT-Beratungsunternehmen. Spätestens bei internationalen Projekten stößt man aber hier an die Grenzen.

Zum aktuellen Zeitpunkt gibt es erste Partnerschaften sowohl mit Integrationspartnern wie der Schweizer Skypro AG und SOLVIS ltd als auch auf der Produktebene mit B HOLD. Außerdem sind nach Aussagen des Unternehmens verschiedene Partnerschaften sowohl mit Systemintegratoren als auch mit Produktherstellern in Arbeit, sowohl in der Schweiz als auch in Deutschland und anderen Ländern. Es ist daher davon auszugehen, dass sich die Situation in diesem Bereich relativ zügig verbessert.

**11 Die Sicht von Kuppinger Cole**

---

Mit rolmine® 1.1 hat die Schweizer ipg AG ein interessantes und leistungsfähiges Produkt für die Rollenanalyse (Role Mining) und das Rollenmanagement auf den Markt gebracht. Durch die stark steigende Bedeutung des Rollenmanagements, das zu den führenden Investitionsthemen im Bereich Identity Management und GRC gehört, handelt es sich dabei um ein stark wachsendes Marktsegment.

Im Vergleich zur ersten Version zeigt sich das Release 1.1 deutlich gereift. Einige der derzeit noch vorhandenen Einschränkungen wie beispielsweise die Abbildung mehrerer Organisationsstrukturbäume sollen zudem mit der nächsten Version beseitigt werden. Die genannten Verbesserungsmöglichkeiten sind aber durchweg akzeptabel und lassen sich durch gangbare Workarounds adressieren.

In der Praxis erweist sich das Werkzeug als funktionale Lösung, die einen erheblichen Nutzenbeitrag sowohl für Rollenmodellierung und –management als auch für die Erhöhung der Datenqualität von Identitätsdaten leisten kann.

Daher empfiehlt sich in GRC- und Provisioning-Projekten, bei denen die geplanten oder eingesetzten Lösungen kein Role Mining unterstützen, eine Evaluation von rolmine® als ergänzendem Werkzeug.

Zitieren von Informationen und Daten von Kuppinger Cole + Partner: In internen Dokumenten und Präsentationen dürfen einzelne Sätze und Abschnitte für die ausschließlich interne Kommunikation in Unternehmen ohne explizite Erlaubnis von Kuppinger Cole + Partner verwendet werden. Die Verwendung großer Abschnitte oder des vollständigen Dokuments setzt die vorherige schriftliche Zustimmung von Kuppinger Cole + Partner voraus und kann die Zahlung von Lizenzgebühren einschließen. Die externe Publikation von Dokumenten und Informationen von Kuppinger Cole + Partner in der Werbung, Pressemeldungen oder anderen Marketing-Materialien erfordert generell eine vorherige schriftliche Zustimmung von Kuppinger Cole + Partner. Ein Entwurf des entsprechenden Dokuments sollte vorgelegt werden. Kuppinger Cole + Partner behalten sich das Recht vor, die externe Verwendung aus jedwedem Grund zu untersagen. © Kuppinger Cole + Partner 2004-2008. Vervielfältigung verboten, falls nicht autorisiert. Für zusätzliche Kopien kontaktieren Sie bitte [service@kuppingercole.de](mailto:service@kuppingercole.de).