УДК 311.34

РЕАЛЬНОСТЬ, ОСНОВАННАЯ НА УПРАВЛЕНИИ УЧЕТНЫМИ ДАННЫМИ

М. Фюллер
Университет прикладных наук, Ной-Ульм, Германия
E-mail: marlon.fueller@hs-neu-ulm.de

Необходимость повышения безопасности и соблюдения требований подталкивает бизнес к созданию достоверного управления учетными данными в своих ИТ системах. Как связь между организационной структурой компаний и ERP системой (Enterprise Resource Planning) процесс управления идентификацией подвергается изменениям с обеих сторон. Использование требований реального времени с учетом регламентированных разрешений отвечает на эти изменения. Но на самом деле очень немногие компании после сдачи системы в эксплуатацию стараются вносить коррективы в свои системы аккуратно в режиме реального времени, в результате чего они перестают отвечать требованиям.

Эти отклонения от требований снижают качество бизнес-процессов, нарушают соглашения о безопасности и ведут к дополнительным затратам на проведение необходимого анализа с целью правильного отражения информации об идентификации пользователей.

Современные ERP системы, основанные на СУБД класса In-Memory, обладают широким арсеналом аналитических инструментов. Эти возможности следует использовать для удовлетворения потребностей компании в управлении идентификацией, что обеспечит необходимый уровень информационной безопасности компании и сократит расходы на процесс управления лицензиями.

С учетом исходно выверенной концепции авторизации даже при возникновении прецедентов, которые выходят за ее рамки, система управления идентификацией, основанная на данных реального времени, позволит улучшить временные параметры бизнеса и/или обеспечит точное соблюдение регламентов производственной деятельности.

Ключевые слова: соответствие требованиям, ERP системы, управление идентификацией, СУБД класса In Memory, управление лицензиями.

REALITY BASED IDENTITY MANAGEMENT IS READY FOR LEADERSHIP. A PROSPERING PERSPECTIVE FOR SECURITY AND BUSINESS PREMISED ON IDENTITY MANAGEMENT ANALYTICS & IN-MEMORY-DATABASES

M. Fuller
University of Applied Sciences Neu-Ulm, Neu-Ulm, Germany
E-mail: marlon.fueller@hs-neu-ulm.de

Mounting security and compliance demands are pushing businesses to implement accurate identity management in their IT systems. As an interface between the company`s organizational structure and an ERP (Enterprise Resource Planning) system, identity management is subjected to change on both sides. Keeping real-life requirements in line with configured authorizations means responding to these changes. But in reality, very few companies bother to make thorough, real-time adjustments to their systems after implementation – with far-reaching consequences: their concepts become incompatible with their requirements.

These kinds of discrepancies reduce the quality of business processes, compromise security and drive up costs – making reality-based identity management based on an extensive usage analysis imperative. Up-to-date ERP systems based on in-memory-databased are gifted with integrated analytic capabilities. These capabilities properly used are the key instrument to align identity management to company needs, providing a transparent, lasting security concept and reduce costs throuth accurate license management. In close cooperation with a formerly aligned authorization concept, the use case even goes beyond: a reality based identity management will be enabled wich can be realized as leading control system – with in-time indicators for business and/or compliance issues – to ensure accurate business activities.

Keywords: compliance, Enterprise-Resource-Planning, Identity Management, In-Memory-Database, License Management.

Introduction

Mounting security and compliance demands are pushing businesses to implement accurate identity management in their IT systems. As an interface between the company's organizational structure and an ERP (Enterprise Resource Planning) system, identity management is subjected to change on both sides. Keeping real-life requirements in line with configured authorizations means responding to these changes. But in reality, very few companies bother to make thorough, real-time adjustments to their systems after implementation – with far-reaching consequences: their concepts become incompatible with their requirements.

Many companies use ERP or ERPII systems like SAP ERP or SAP Business Suite. Particularly with the growing number of employees, they are applying contemporary and integrated solutions.

Continuous improvement becomes more and more significant. It is replacing the implementation as the central issue in companies. Here, the authorization design has been and still is the essential prerequisite and should support and exactly represent the IT business processes. Irrespective of the underlying architecture, the authorization concept controls which employees can access which functions in the ERP system.

1. Respecting principles

Apart from the typical criteria like security, privacy, segregation of duties or task qualification, the authorization design and maintenance must consider two elementary principles. These principles of the role-based access control (RBAC) significantly influence the authorization assignment:

– The primary focus in the authorization conception lies on function- or transaction-oriented authorization bundles, the so-called roles. Their assignment and allocation take place based on economic criteria, which are based on the management area or the position or job of the employee (economic principle) [FERR07, p. 62 and p. 214].

– The least privilege principle additionally demands that a user only receives the authorizations they require for the everyday accomplishment of their work [FERR92, p. 9]. Less authorization would impede the work process, and too many would pose a security risk.

2. Authorizations in the status QUO

A sector-independent investigation by the IBIS Prof. Thome AG shows that companies are far from an ideal state, as far as authorizations are concerned. On average, employees have far more authorizations than they actually need. Around 23 percent proved to be unnecessary. In the investigated companies, an average of 5000 unnecessary functions or transactions is assigned to the employees. These deficits lead to an uncontrollable freedom of action. The consequence is unregulated activities in the ERP system.

Apart from qualitative effects on the business processes, this has a considerable influence on the data security and not least on the costs.

The main idea of the RBAC approach is that access authorizations are transferred depending on the current organizational position and responsibility. The users' role in the organization, as well as their necessary freedom of action are central. The role is between the users and the function- or transaction- oriented execution authorization. Image 1 shows the complex interaction of technical and organizational areas in the SAP authorization system.

3. Realistic redesign of the authorizations

If the deviations from a defined target concept or the real situation in the company are too high, the deficits require a redesign. The advantages resulting from a productively applied ERP solution should be used here, since it provides all relevant information. Starting in a 'green field' is therefore neither advantageous nor recommended.

The respective user's actual requirements are elementary for the reconception by the least privilege principle. These are reflected in the used functions or transactions, which must be evaluated by a usage analysis of the ERP solution. However, this conception based on real requirements demands an abstraction from the authorizations already introduced. In addition to this, a valid investigation does not require day or ad-hoc analyses, but a consolidated data pool which contains several months. As shown in image 2, these active and necessary function-oriented authorizations serve as a basis for a redesign. The productive system analytics must fully consider the ERP system visualized in image 1. Therefore, it has to allow a complete overview of the current situation, including composite roles, individual roles, division

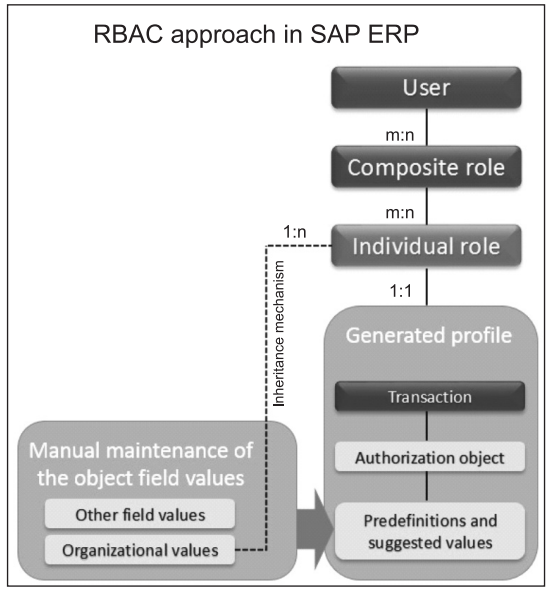

Fig. 1. Function-oriented authorization assignment in SAP ERP (according to [BEYE03, p. 56])

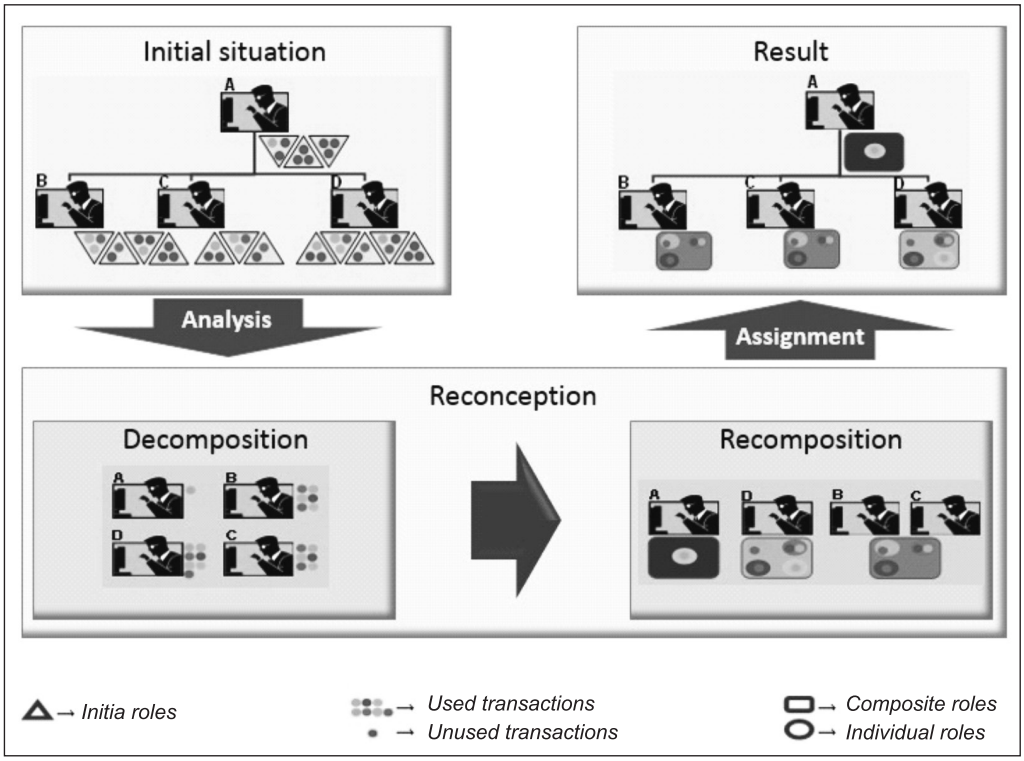

Fig. 2. Redesign based on usage analysis

functions, profiles, authorization objects and values, as well as other role contents, such as links. Furthermore, exceptions like sporadic use or inactive employees can be identified via the usage analysis.

If the economic principle of role conception is considered apart from the least privilege principle, information must be provided which enables a transferal of the user function designation to the composite and individual role system. Again, the users' system usage is considerable. It reflects the required activity areas due to the area of responsibility. In a consolidated observation – over several months and users – the obtained data trigger the creation of new authorization roles. While composite roles have an organizational focus, a basis of module- or subject-specific individual roles allows a higher flexibility and reutilization (see image 2). Resulting from a systematic redesign based on an integrated analyses which respects the RBAC principles and the authorization logic (see image 1), the IT managers benefit from the promptly implemented authorizations which also correspond to the real situation in the company and facilitate the administration with a comprehensible system.

Conclusion

Collaboration and speed, as well as flexibility, belong to the critical success factors in the successful company management. Apart from the corporate culture or the change management, the information technology has to be particularly accommodated. It must be designed to support the company with all

changes it may go through in a secure, effective and efficient way. It is therefore recommended to continuously adapt the new authorization concept to the changed circumstances. Only like this is it possible to avoid possible discrepancies.

While the existing roles are abstracted from during a reconception, they become central in the continuous adaptation. They form the starting point for the examination for deviations from the ideal state. The basis for both phases – redesign and adaptation – is real-time and objective information about the actual state which corresponds to the real situation in the company. To accommodate the time criterion, manual examinations must be abandoned. A software-based examination is recommended, which allows a periodic check, and moreover visualization and automatic processing. Therefor reality-based identity management based on an extensive usage analysis is imperative. Up-to-date ERP systems like SAP S4/HANA based on in-memory-databases are gifted with integrated analytic capabilities. These capabilities properly used are the key instrument to align identity management to company needs, providing a transparent, lasting security concept and reduce costs through accurate license management. In close cooperation with a formerly aligned authorization concept, the use case even goes beyond: a reality based identity management will be enabled which can be realized as leading control system – with in-time indicators for business and/or compliance issues – to ensure accurate business activities. A prospering perspective for security and business grounded on reality based identity management and in-memory databases.

References

1. *Beyer S.-A. et al*. SAP Berechtigungswesen. Design und Realisierung von Berechtigungskonzepten für SAP ERP und SAP Enterprise Portal. Galileo, Bonn, 2003.
2. *Ferraiolo D., Kuhn R*. Role-Based Access Control. Reprinted from 15th National Computer Security Conference (1992), Baltimore MD. P. 554–563. URL: http://csrc.nist.gov/rbac/ferraiolo-kuhn-92.pdf, Erstellungsdatum, 1992.
3. *Ferraiolo D. et al*. Role-Based Access Control. 2nd Edition, Artech House, Norwood, 2007.

Bibliography

1. *Beyer S.-A. et al*. SAP Berechtigungswesen. Design und Realisierung von Berechtigungskonzepten für SAP ERP und SAP Enterprise Portal. Galileo, Bonn, 2003.
2. *Ferraiolo D., Kuhn R*. Role-Based Access Control. Reprinted from 15th National Computer Security Conference (1992), Baltimore MD. P. 554–563. URL: http://csrc.nist.gov/rbac/ferraiolo-kuhn-92.pdf, Erstellungsdatum, 1992.
3. *Ferraiolo D. et al*. Role-Based Access Control. 2nd Edition, Artech House, Norwood, 2007.