[1.]Mihaela OSACI, [2.]Ana Daniela CRISTEA, [3.]Daniel GHIUZAN, [1.]Diana Adela BERDIE

SAP AUTHORIZATION BASED ON THE FOUR EYES PRINCIPLE

[1.]Politehnica University of Timisoara, Faculty of Engineering Hunedoara, 5 Revolutiei Street, Hunedoara, ROMANIA
[2.] Cellent AG, Ringstraße 70D, Fellbach-Stuttgart, GERMANY
[3.] Flex LTD, DN6 km 5.7, Timişoara, ROMANIA

Abstract: Currently, the implementation of the integrated information systems in companies represents a sine qua non condition for providing higher and more reliable accessibility to the information resources. One of the most used integrated platform, which offer the support for ERP (Enterprise Resources Planning, is SAP Netweaver. This platform is multilingual & multitasking, based on the three-tier client-server technology. The development environment is the Application Server ABAP and/or Java. Web Dynpro technology is the present-day standard to develop Web applications in ABAP (or Java) programming SAP environment. Data security is now an issue of great interest. The standard modality to get a SAP Netweaver authorisation is the role-based authorization, having as foundation the RBAC design pattern (Role Based Access Control). For standalone Web Dynpro applications, being not integrated in the portal, the security shall be programmed into the application. The four eyes principle is a control mechanism designed to achieve a high level of security, especially for critical documents and operations. This principle is based on the fact that at least two persons check independently the same request / transaction / document. This paper presents a way to implement the four eyes principle in SAP Netweaver Application Server.
Keywords: SAP authorization, four eyes principle, SAP Netweaver Application Server

1. THE FOUR EYES PRINCIPLE AND THE STANDARD SAP AUTHORIZATION

The standard modality to get a SAP Netweaver authorisation [1], [2], [3] is the role-based authorization, having as foundation the RBAC design pattern (Role Based Access Control).
This pattern was formalized in 1992 by Ferraiolo and Kuhn [4], in the form in which the users have role-based access to the system resources with permissions, and the roles can inherit permissions from other roles. The class diagram of the RBAC pattern is shown in Figure 1, [5].

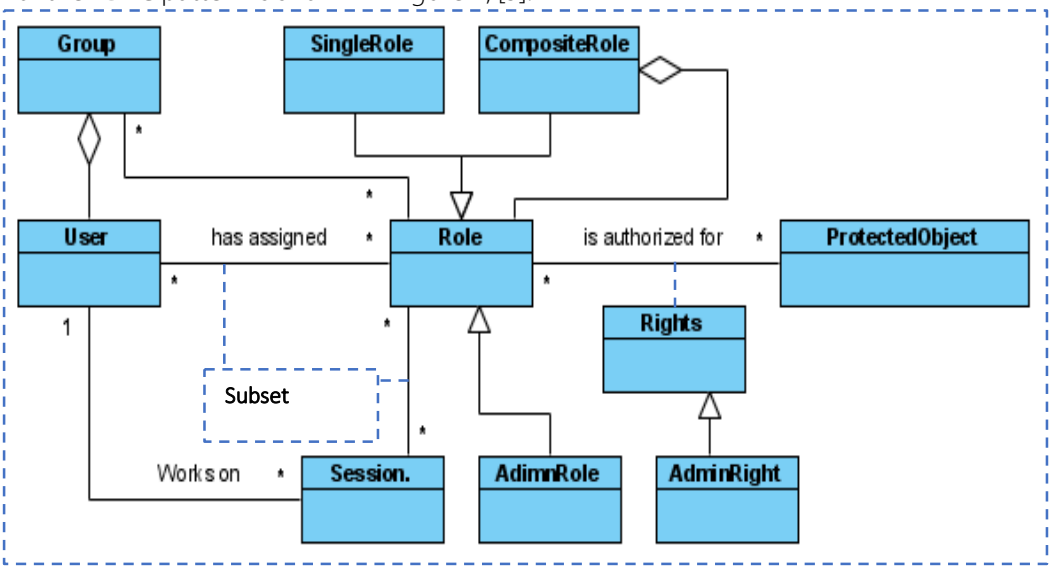

Figure1. The RBAC Design Pattern (Gellert, 2013).

The User class represents the user waiting to access a protected object (transactions, programs, services), and the Role class represents the user's roles. SAP provides a large number of single roles to be used, as well as the possibility to create their own roles. The Rights class describes the access type (deletion, writing, etc.), [5].
So, the users may access the resources / information through the roles (rights) assigned to them by an administrator. An administrator who can solely decide what rights are granted to a user or what users are inserted into / removed from a system can easily produce illegal operations. Therefore, to increase the transparency and security of a system (in our case, the user management), the administrator can use the four eyes principle.

The four eyes principle is a control mechanism designed to achieve a high level of security, especially for critical requests. The four eyes principle ensures that a certain request or transaction is approved by at least two persons. Therefore, each operation intended to change the rights of a user, or to insert or delete a user, will be supervised by at least two other persons.

That's why the below German saying fits very well with this principle:

"Trust is good, but control is better"

The four eyes principle is usually implemented as an extra layer at the top of the system whose security we want to increase. (Figure 2).

This principle is used in an increasingly range of applications and fields. We meet it from information processes to banking processes or even medicine (e.g. in the process of granting organs to the patients).

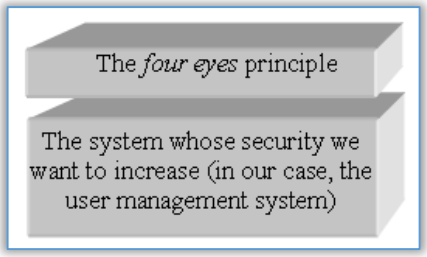

Figure 2. The four eyes principle layer

2. AN EXAMPLE OF SAP USER MANAGEMENT IMPLEMENTATION

We illustrate in this paper a way to implement the four eyes principle, i.e. a case study in which at least two persons must approve a decision [6]-[12].

We started from a school catalogue, for which an administrator can create, delete or change the users. The application administrator can create / delete / change the users who are divided into 3 groups: teachers, students and parents. For example, the students and parents will have only the right to visualize the data included in the school catalogue application. The teachers will have the right to add or remove only the data related to the subject they teach.

To prevent any possible frauds, we introduced at the top of the school catalogue the four eyes principle, implemented on 2 levels (Figure 3). In this way, we ensure, for example, that no student will get the role of a teacher.

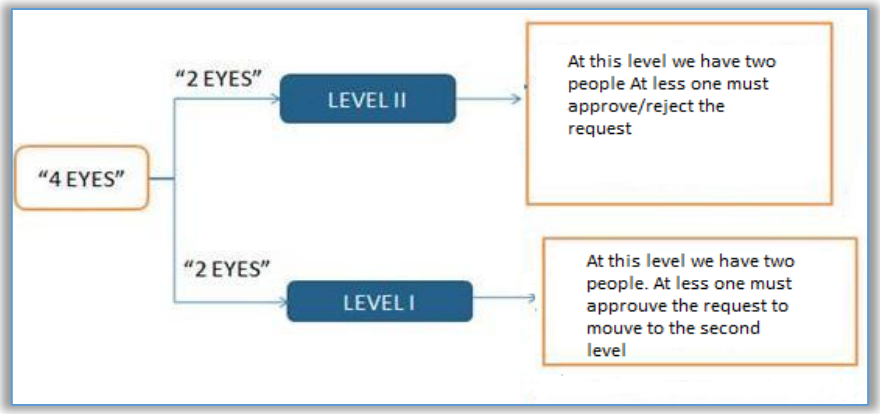

Figure 3. Hierarchical authorization level for the school catalogue

The four eyes policy is usually based on levels. The number of levels can range from 1 to n, and on each level we can have a variable number of people that must approve/reject a request. As approval policy, we can choose that one person on a level to be enough for approving/rejecting a request, or all the people on a level to be required to approve/reject a request. It is recommended that the number of people on a level to be maximum 5 and minimum 2. In this way, if a person is on leave or sick leave, there is always another person who can approve/reject a request. It is not recommended to introduce more than 5 people, because the costs increase with increasing number of people involved. Those people need time to approve/reject a request, thus reducing the time used to fulfill their tasks and perform their everyday work, fact which normally increases the costs. At the same time, we must take into account the fact that not any person may be involved in such process. The selected persons must know when they may accept and when they must reject a request, been responsible for his/her actions.

In our case, we have 2 persons assigned for the first hierarchical level and other 2 persons for the second hierarchical level. Each level needs at least one person to approve/reject a request.

If at less one person from the first level approved the request, all the persons from the second level will automatically receive from the application workflow an email through which they are informed that a request must be approved/rejected. Only after at least one person from the second level approves the request, the user will get the desired rights. In this way, the administrator cannot make any changes until at least two other persons decide whether that change is correct or not.

If one of the persons from the first level rejects the request, the process will be automatically terminated, and the persons from the second level will not be informed anymore. Also, the application workflow will automatically send an email to that user for informing him/her that an administrator requested certain rights for him/her, but the request has been rejected.
An example of four eyes principle application is shown in the diagram presented in Figure 4.

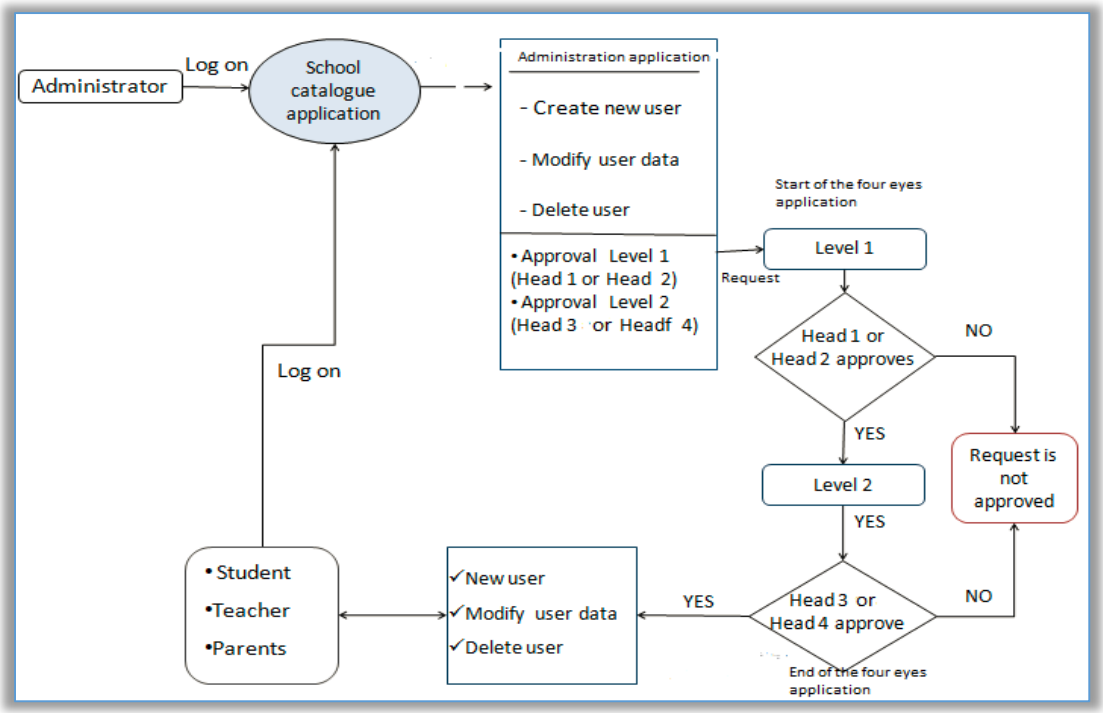

Figure 4. The diagram for implementing the four eyes principle in the case study application
Figure 5 shows the case study application in conjunction with the four eyes application.

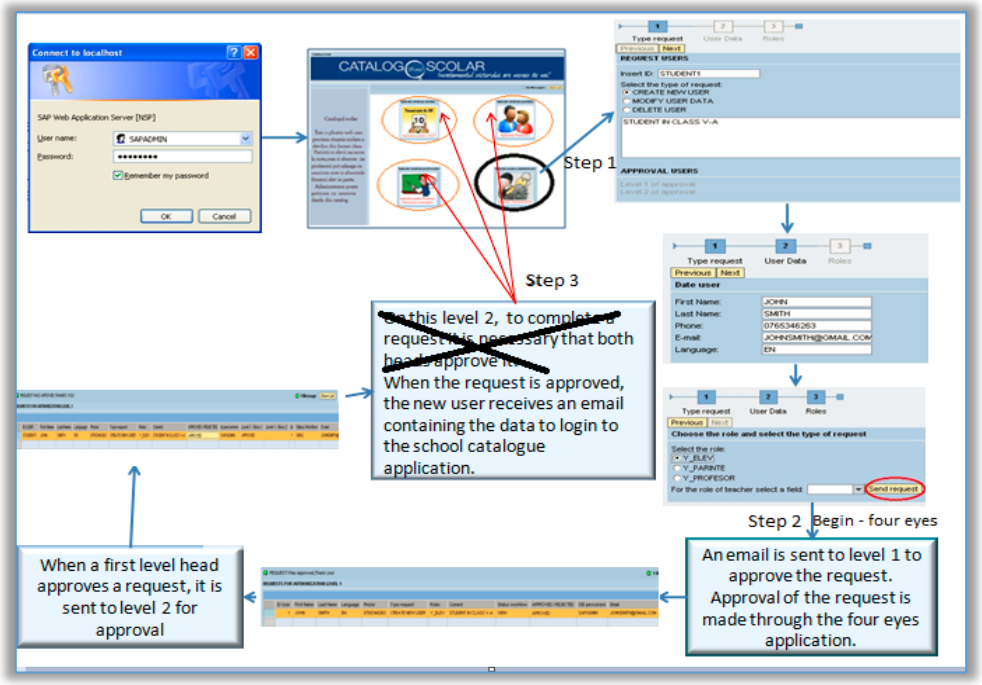

Figure 5. The case study application in conjunction with the four eyes application
Only the Administrator of the school catalogue may access the application through which the users can be given certain rights – Step 1. After the administrator makes a request (insert new user / delete user / change authorization for a user), the four eyes process starts – Step 2 (Figure 4). According to the four eyes principle, from this moment at least 2 other persons must approve/reject the administrator's request before the requested change to come into effect.

When the request is approved by at less two persons, the user is automatically informed by the application workflow, through an email, that the request made by the administrator has been approved – Step 3 (Figure 4). The new users that were inserted in the School catalogue will additionally receive all the information required to login for the first time in the School Catalogue.

3. CONCLUSIONS

This paper presents a way to implement the four eyes principle in SAP User Management. Our four eyes solution is built on two hierarchical levels. In this way, an administrator can make changes to the users of a School Catalogue only if at least two other persons approve those changes. The four eyes principle is a safe principle used more and more in an increasingly extensive range of areas and applications, from computer processes to banking systems and medicine.

References

[1] Samarati, P.,&De Capitani di Vimercati, S., (2001). Acces Control: Policies, Models and Mecanisms, Springer Berlin/Heidelberg
[2] Cristea, A.D., Prostean, O., Muschalik, T., & Tirian O., (2014). Contribution to the creation and development of a new authorization concept based on a learning process, Computer Application in Engineering Education, 22(1), 1-10
[3] Keller, H., & Krüger, S. (2007). ABAP Objects, SAP Press, Bonn, Germany
[4] Ferraiolo, D. F., & Kuhn, D.R. (October 13-16, 1992). Role-Based Access Controls, 15th National Computer Security Conference, Baltimore, 554-563
[5] Gellert, U., & Cristea, A.D. (2013). Web Dynpro ABAP for Practitioners, Second Edition, Springer Berlin / Heidelberg
[6] Cristea, A.D., Berdie, A.D., Osaci, M., Chirtoc, D., (2011), The advantages of using mind map for learning web dynpro, Computer Applications in Engineering Education, 19(1), 201-207
[7] Berdie, A.D., Osaci, M., Prostean, G., Cristea, A.D., (2011), Web Programming features on integrated system SAP, Applied Computational Intelligence and Informatics (SACI), 6th IEEE International Symposium on, 227-230
[8] Osaci, M., Berdie, A.D., Hammes, A.D.,(2013), Studies on Efficiency of the Data Access by ABAP Programming, Soft Computing Applications, 707-713
[9] Berdie, A.D., Osaci, M., Muscalagiu, I., Prostean, G., (2012), A case-study about a web business application implemented in different SAP UI technologies, Applied Computational Intelligence and Informatics (SACI), 2012 7th IEEE International Symposium on, 111-114
[10] Berdie, A.D., Osaci, M., Raich, R., Cristea, A.D., (2011), The Componentisation Efficiency in Realizing a WD ABAP Project, Annals of the Faculty of Engineering Hunedoara, 9(4), 151-154.
[11] Berdie, A.D., Osaci, M., Lemle, L.D., (2011), Comparative Statistical Study of Some SAP UI Technologies, AIP Conference Proceedings, 1389(1), 555-558
[12] Osaci, M., Berdie, A.D., Muscalagiu, I., (2012), Procedia-Social and Behavioral Sciences, 62, 585-589

ISSN 1584 - 2665 (printed version); ISSN 2601 - 2332 (online); ISSN-L 1584 - 2665