

# Content

|           |                                  |  |
|-----------|----------------------------------|--|
| <b>2</b>  |                                  | Addition   |
| <b>4</b>  | Kenneth R. Walsh                 | Analyzing the Application ASP Concept: Technologies, Economies, and Strategies |
| <b>12</b> | Teasley, Covi, Krishnan, Olson   | Rapid Software Development through Team Collocation                            |
| <b>30</b> | Van Dijk, Algra                  | Role-based Access Control (RBAC)<br>Case study                                 |
| <b>48</b> | Elizabeth M. Pierce              | Assessing Data Quality with Control Matrices                                   |
| <b>54</b> | Jackson, Dawson, Wilson          | Understanding e-mail interaction increases organizational productivity         |
| <b>60</b> | Kavassalis, Lelis, Rafea, Haridi | What makes a website popular?  |
| <b>68</b> |                                  | Keywords articles IT Management select 1998-2004                               |



**Authors**

Aart van Dijk

Ton Algra

|              | Business | Information systems | Technology |
|--------------|----------|---------------------|------------|
| Strategy     |          |                     |            |
| Organization |          |                     |            |
| Operation    |          |                     |            |

# Role-Based Access Control (RBAC) Policy and implementation: KLPD employee authorisation for using SAP R/3 applications

**ABSTRACT**

Our society is changing, and the Dutch police are changing with it. This creates new challenges for supporting the police using modern ICT resources. This is why the 'Police ICT Plan' was generated. ICT support is also being further professionalized with respect to police enterprise activities. One of the packages that have been used within the Dutch National Police Agency (KLPD) for several years is SAP R/3. SAP R/3 Enterprise was deployed in July 2003. On this occasion, the KLPD fully revamped their authorisation concept. This represented a response to the needs of the KLPD and the control bodies, such as the audit service of the Ministry of Internal Affairs, to arrive at a modern, insightful and manageable authorisation concept. The new authorisation concept is based on 'role-based access control'. There is considerable (international) interest in this method. This article presents a summary of the ICT authorisation policy of the Dutch police and provides insight into how the authorisation concept is implemented in the KLPD, and in particular in SAP R/3. The article concludes with a summary of experience acquired to date.

## 1 Introduction

### 1.1 Information provision in the police corps

Our society is changing, and the Dutch police are changing with it. One of the current challenges is working cooperatively on the security and quality of life of a specific neighbourhood, district or municipality. Computers are useful tools for supporting this cooperation. Thanks to computers, we can send e-mails and faxes, consult databases and search engines, and create electronic files. We can quickly and conveniently communicate and exchange information – within a police corps, among corps, and with chain partners.

In practice, a few things leave something to be desired. One reason is that the police corps use different programs, which complicates exchanging information and employees. As a result, it sometimes seems that ICT does not adequately support police work, or sometimes even hinders it. For this reason, the three police consulting groups launched the ICT Platform in 1998 and the ICT Steering Group in 1999. The ICT Steering Group generated a phased plan called the 'Police ICT Plan'. This plan is aimed at revamping the ICT organisation without hampering routine police activities. In early 2001, the steering group and the three police consulting bodies approved the Police ICT Plan. The ICT proj-

ect has since been initiated and will continue until sometime in 2005.

#### **Police ICT Plan**

The Police ICT Plan describes the organisation of the revamped ICT in broad terms. The primary principles of this plan are:

1. ICT is henceforth a common issue. The individual corps now often act as 'ICT islands' that set their own courses, but ICT is something that belongs to and serves the entire police organisation.
2. In the revamped ICT structure, demand and supply will be clearly separated. The two sides will be represented by a 'customer organisation' and a 'supplier organisation'. Both of these are group-level organisations, and thus represent *all* of the police corps.
3. ICT is steadily becoming more complex. It is thus highly important to raise the knowledge level within the organisations. All users must in fact be able to use computers (even) better.

#### **Customer organisation**

The Police ICT Plan provides for a 'customer organisation'. It consists of the sections in the various corps that are responsible for information management, along with the group-level Police Information Management Collaboration (*Coöperatie Informatie-management Politie*, or CIP for short) organisation. A collaborative organisation was chosen because the police corps explicitly cooperate in the CIP and jointly guide this cooperation.

#### **Supplier organisation**

The Police, Judiciary and Security ICT Services Collaboration (ISC) acts as the ICT service provider. It satisfies the wishes of the 'customer' by providing suitable ICT solutions or supplying the proper products. ISC will act as an intermediary, with products being purchased in the retail market. The ISC can also offer its own products and services. The ISC cooperates closely with the Information and Technology Organisation (ITO), an agency of the Ministry of the Interior and Kingdom Relations (MIKR) that provides ICT services to the police, judiciary and other chain partners. This close cooperation between the ISC and the ITO leads to a fusion of the ISC and ITO. The ISC is (indirectly) controlled by the corps and the two police ministers.

#### **SAP R/3**

The SAP (Systems, Applications and Products in Data Processing) R/3 package is an important ICT application used in the enterprise activities of the Dutch police. This package is used by the National Police Agency, among others. Access security for SAP R/3 (or SAP for short) is a significant concern of the KLPD.

#### **1.2 Organisation of the police and the KLPD**

The Dutch police are organised as 25 regional police corps and the National Police Agency (*Korps Landelijke Politiediensten*, or KLPD for short). The KLPD is a special corps with central staff offices and group departments, including the Group Department for Information Provision (CDI), as well as a fascinating collection of enterprise service departments, including the National Investigation Department, the Aviation Police Department and the Traffic Police Department.

## **2 SAP R/3 in the KLPD**

SAP R/3 is used as a 'best of breed' package by the KLPD in the financial, logistics, personnel, and general and technical services areas. In addition, several new applications have been generated, such as 'aircraft fleet maintenance', 'forensic weapons', 'salary processing', and 'electronic shopping for the Logistics Department'.

Other applications, such as Employee Self Service (ESS), Customer Relation Management (CRM), Document/Record Management Systems (DMS), and Web Application Server (WAS), also form part of the picture. In summary, it can be said that SAP R/3 is a very important package for the enterprise activities of the KLPD.

## **3 Authorisation within the Dutch Police**

### **3.1 Dutch Police Basic Security Level (BBNP)**

The BBNP (*Basisbeveiligingsniveau Nederlandse Politie*) addresses basic security requirements and measures. The basic security measures are the measures employed for information security in each of the corps and the supraregional information systems.

The Police Information Security Regulations

(*Regeling Informatiebeveiliging Politie*, or RIP for short) define information security as the *reliability of information provision*, which is regarded as a *component of quality assurance* for the enterprise processes and underlying information systems. The BBNP guideline is thus *aimed at the quality of the information provision process* and defines a minimum set of measures for ensuring the reliability (i.e., the availability, integrity and exclusivity) of the information systems.

### 3.2 Authorisation guide

Corps employees are granted specific authorisations to allow them to use information systems and the information in them. These authorisations are dependent on the *function* or *functional role* performed by the employee. An employee only receives access to information systems, and may only exercise authorisations with respect to the data stored in these systems, to the extent that this is necessary for his work (*'need to use'* and *'need to know'*). Before an employee can process data, certain things must be *arranged* on the user organisation side and certain things must be *configured* on the automation organisation side.

### Separation of duties

There must be a *separation of duties* in granting, modifying and revoking authorisations. It is undesirable for a person to be able to grant himself or someone else authorisations without external control. The various steps in the authorisation process must therefore be assigned to persons holding different positions. The following steps are distinguished in the guide:

- *Disposition task*  
This task lies with the person or persons who have been empowered to grant authorisations for using an information system and the information in it.
- *Registration task*  
This task lies with the person responsible for assessing the granted authorisations based on the defined conditions and handling the granted authorisations. He maintains a central registry for this purpose.
- *Execution task*  
This task lies with the person or persons who

actually use the granted authorisations in the information system.

- *Control task*  
Routine supervision of the use of granted authorisations is the responsibility of the manager of the organisational unit where the employee is located. In addition, the corps manager can periodically have audits performed by an independent (external) EDP auditor.

### Authorisation procedure

It is essential to have an agreed *authorisation procedure* for granting, modifying and revoking authorisations in writing, and an *authorisation authority* that supervises proper operation of the procedure. This authority performs the following activities at minimum:

- Ensuring that authorisations are granted in accordance with the legal framework and the conditions specified by the system owner.
- Periodically investigating whether the list of persons allowed to grant authorisations is still correct.
- Periodically checking whether the granted authorisations still correspond to the actual situation.
- Recording the granted authorisations and maintaining these records (registration task).
- Reporting regarding this set of activities to the corps chief, if he is tasked with executing the authorisation procedure, and otherwise to the corps manager.

### Conditions

Authorisations are granted under the following conditions:

- Authorisations are requested and granted *in writing*.
- The function and/or functional role of each employee has been defined and is in effect.
- There is a current job description for each employee.
- The granted authorisations correspond to the tasks stated in the job description.
- The person granting the authorisation is authorised to do so.
- The duration of the authorisation is individually

specified for each authorisation.

- The authorised person has completed the necessary training for using the information system.
- The employee is actually an employee of the corps.
- The necessary security investigation of the authorised person has taken place.
- The user ID of the authorised person is correct.
- Authorisations are granted in accordance with the measures in the BBNP guideline.

#### 4 Role-Based Access Control (RBAC)

The concept of role-based access control (RBAC) plays an important role in access security. This is a methodical approach originating from the US National Institute of Standards and Technology (NIST). The motive for developing RBAC was the desire to have an access security method that is suitable for enterprise applications and that simplifies the administration and maintenance of access security. After international agreement on the RBAC standard was achieved in 2002, many producers have based their access security software on it. RBAC is based on *roles*, which are standardised sets of functions that are suitable for multiple users. Using functions and standardised sets of function linked to them is not new (see van Dijk, 1994), but a large amount of literature on the subject of RBAC has appeared in recent years, such as the book *Role-Based Access Control* by several employees of the NIST. RBAC is briefly described in this section.

In RBAC, the entities *users*, *subjects*, *objects*, *operations* and *permissions* play a prominent role, as do the relationships between these entities. *Users* are the entities that use an information system. A *subject* is a computer process or program that performs actions on behalf of a user. These actions are performed on an *object*, which is a resource that is accessible to the computer system. An *operation* is

an action performed by a subject. *Permissions* (which are also called *privileges*) are authorisations to perform actions. Such an action involves a combination of an object and an operation.

Figure 1 shows the relationship between users, roles, permissions, operations and objects. The 'subject' entity is not discussed in this article.

In RBAC, it is thus not allowed to link permissions directly to users. Permissions are granted by means of two links: *a link between users and roles* and *a link between roles and permissions*. A significant advantage of this arrangement is that if a user is assigned a different position in the enterprise, only the user–role link has to be changed. This does not require a large amount of specialised knowledge. There are also major advantages with regard to disposition and control activities. As the number of roles is limited and mirrors the organisational structure, the number of changes will be small after an initial period. In addition to yielding considerably lower costs, using approved roles provides continual overview and insight into authorisation activities. RBAC applications can be found at many different levels in ICT, such as in operating systems, database management systems, networks, workflow systems and Web services.

RBAC can also be used in Single Sign-On situations.

#### 5 Authorisation in the KLPD

##### Conclusion

Based on the above (see also Figure 2), it can be concluded that:

1. *The 'need to know' and 'need to use' principles must form the basis for granting permissions or authorisations with respect to data, information and information systems.*
2. *Permissions or authorisations with respect to*

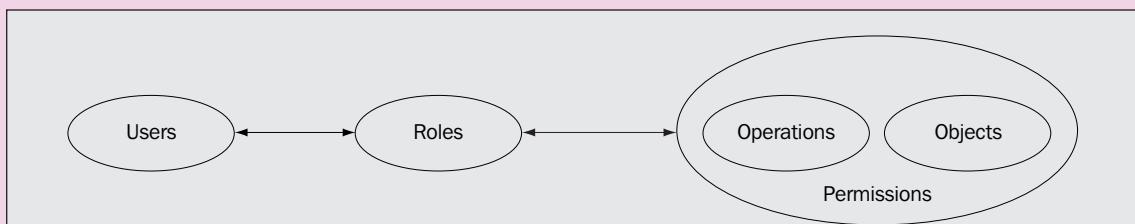


Figure 1. Relationship of RBAC components

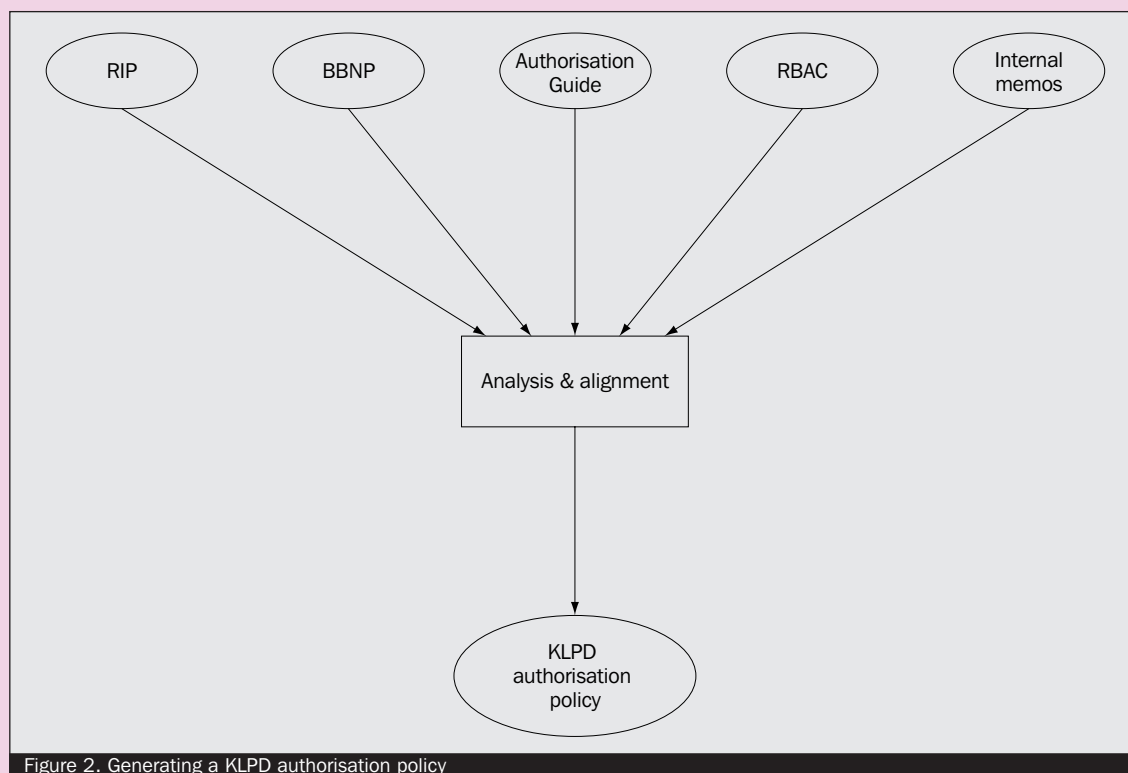


Figure 2. Generating a KLPD authorisation policy

*data, information and information systems must be granted using two links:*

- *a link between users and functions (or functional roles);*
  - *a link between functions (or functional roles) and permissions (or authorisations).*
3. *Directly linking users to permissions or authorisations is not allowed.*

## 6 Authorisation in SAP R/3

Many software suppliers have responded to the international interest in role-based access control. RBAC can also be used in SAP R/3 Enterprise. SAP R/3 uses roles and can combine roles to form composite roles. In RBAC, the term 'role' is primarily used in the functional sense. In SAP R/3, the term 'role' refers to a technical system role. In the KLPD SAP R/3 authorisation concept, the terms function and functional role (which have a process-related nature) were chosen for the KLPD business view, while the terms SAP R/3 role and SAP R/3 composite role (which relate to technical aspects of the system) were chosen for the SAP R/3 system view.

The relationship between the business view and the system view is defined by a 1-to-1 link between a function or functional role and a SAP R/3 composite role (see Figure 3).

Tasks are distinguished within a function or a functional role. SAP R/3 roles are clustered in a SAP R/3 composite role (see Figures 3b and 4). The actual link is made inside SAP R/3 between the user ID and the SAP R/3 composite role. In this way, a user is linked based on his function or functional role (role-based).

The authorisation structure within RBAC and SAP R/3 is designated as 'object oriented'. An authorisation object forms the basis for determining the access privileges. It has at most ten fields for this purpose, which are defined in the data dictionary. The authorisation objects and associated authorisation fields and activity codes (values) are linked to a role via a profile (a set of authorisation objects). Besides authorisation objects, transactions can also be coupled to a SAP R/3 role via a menu (see Figures 4 and 6).

**Generic and derived roles**

Certain positions occur relatively frequently in a company or organisation. An example is the position of sales manager. Each sales manager then has a specific area of responsibility. Within KLPD, there is a similar situation for the position of personnel officer. Each personnel officer is responsible for one or more departments.

In SAP R/3, it is possible to use 'generic roles' and 'derived roles'. A role can be described using a generic role. The *derived* roles are derived from the generic role. They differ from the generic role by having different entries in the 'organisational unit' field.

Derived roles can easily be derived from a generic role. If the generic role is modified, the derived roles automatically receive the same modifications. This simplifies role maintenance and ensures consistency.

**7 SAP R/3 Authorisation in the KLPD**

**7.1 Introduction**

In Section 5, it was concluded that permissions or authorisations with respect to data, information an information systems must be granted using two links:

- a link between users and functions or functional roles;
- a link between functions or functional roles and permissions or authorisations.

The implementation of RBAC in SAP R/3 Enterprise is briefly described in Section 6. In this section, we describe how all of this is used in the KLPD (see Figure 5).

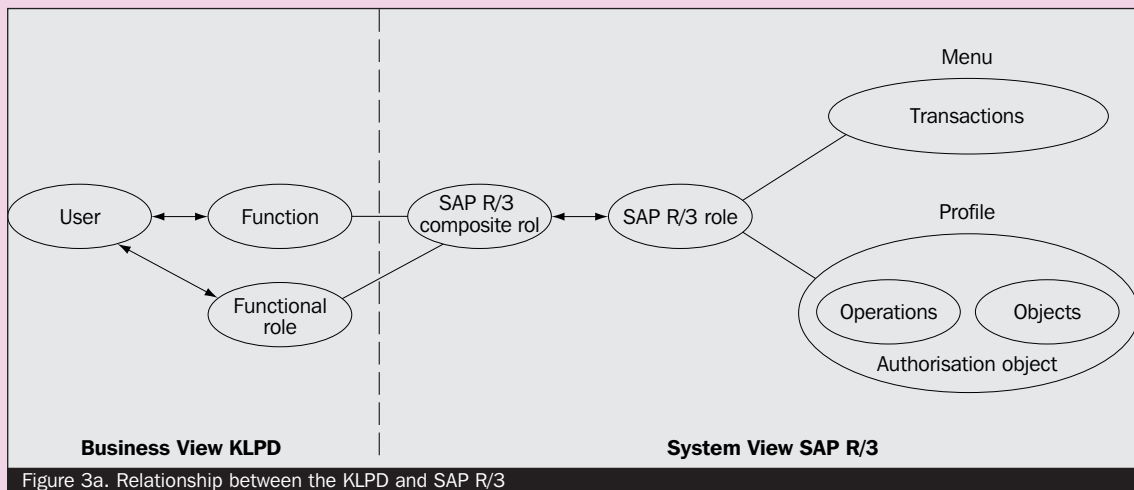


Figure 3a. Relationship between the KLPD and SAP R/3

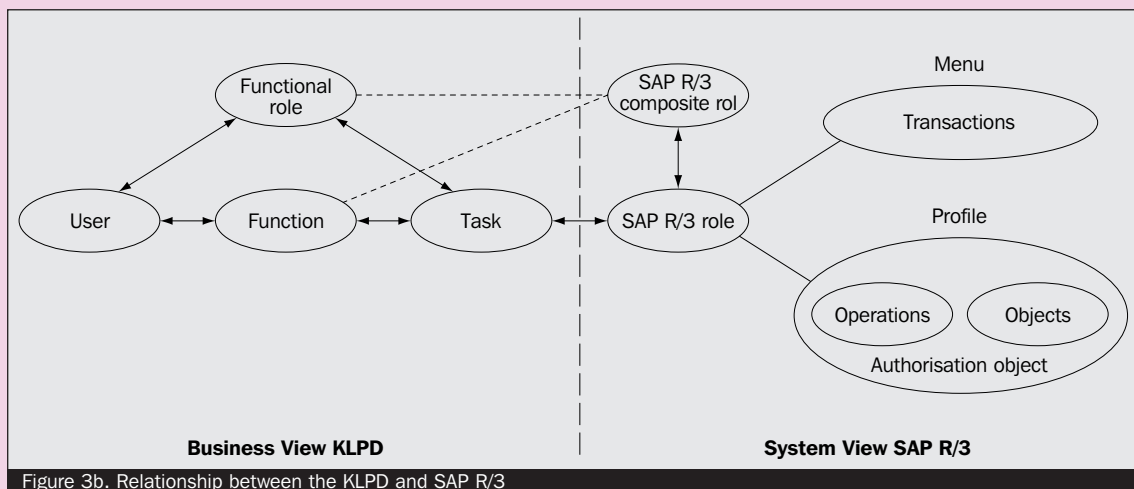


Figure 3b. Relationship between the KLPD and SAP R/3

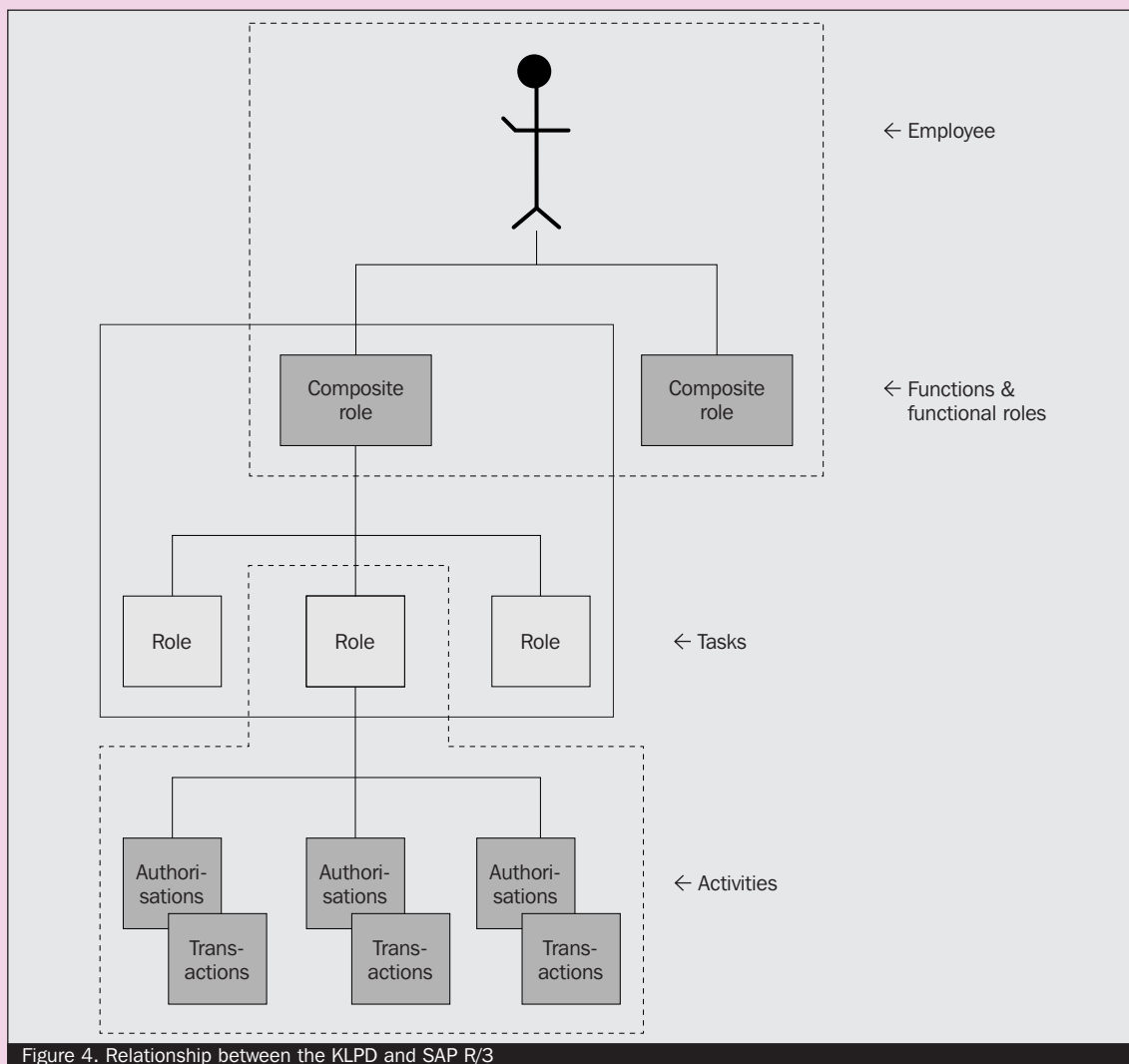


Figure 4. Relationship between the KLPD and SAP R/3

## 7.2 Roles and composite roles

Figures 3a, 3b and 4 show the relationship between functions and tasks in the organisation described in the Administrative Organisation (AO) and SAP R/3. Functions have a permanent nature. Functional roles have a process-related nature. SAP R/3 works with composite roles and roles. In practice, tables or matrices of composite roles versus roles are prepared. Based on the description of the function and associated tasks, the composite role and roles are generated by Application Management via Functional Management. Figure 6 shows an example of a function and its ultimately associated authorisations for a Personnel Management Assistant in the Water Police Department.

## 7.3 Implementation approach

When starting to implement RBAC, it is very important to define the functions and functional roles and the authorisations necessary for each function or functional role. Here a distinction can be made between different methods for developing functions:

- The *top-down* or *greenfield* method. This consists of using the organisational structure, security policy, job descriptions and process descriptions to arrive at an acceptable level of detail in defining the functions for using SAPR/3, and thereby the necessary authorisations.
- The *bottom-up* or *role-mining* method. This starts with existing authorisations and uses interviews with managers to determine which functions exist within a department or team.

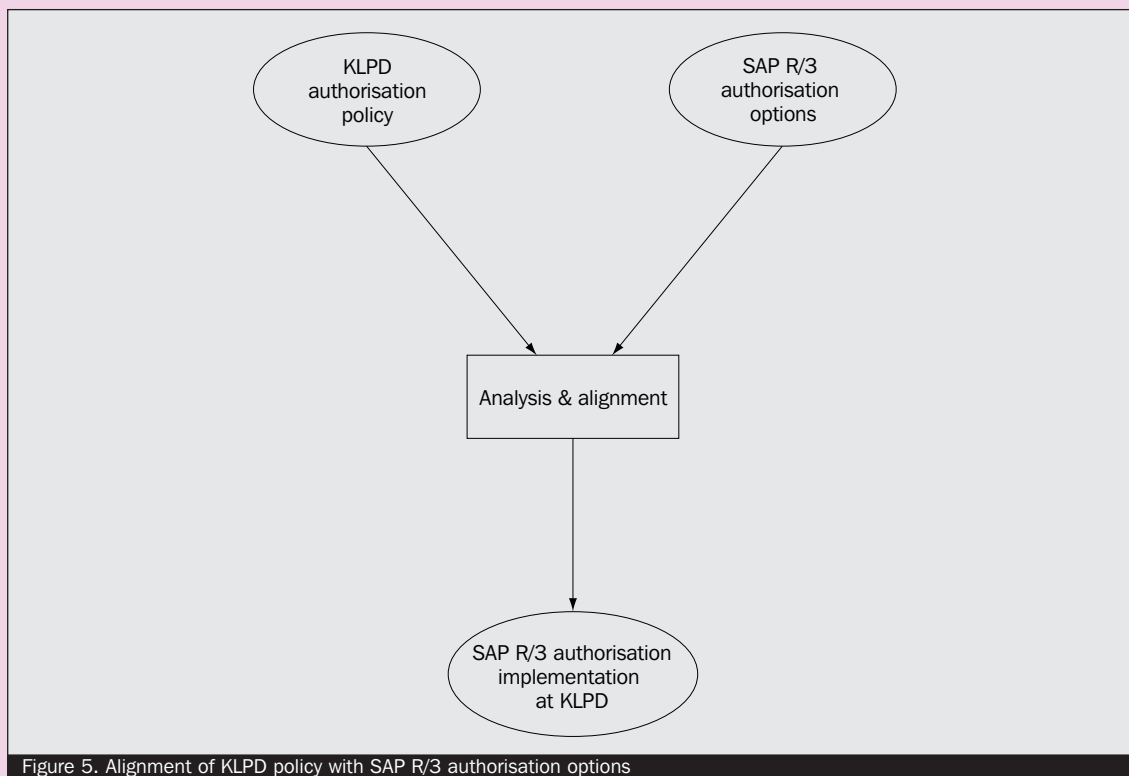


Figure 5. Alignment of KLPD policy with SAP R/3 authorisation options

A hybrid approach is also possible, consisting of a combination of the top-down and bottom-up methods. Two types of hybrid approach can be distinguished:

- *Type 1*: some functions or functional roles are developed using the one method, and others are developed using the other method.
- *Type 2*: functions and functional roles are initially determined using the bottom-up method, and then modified using insights obtained from the top-down method.

A hybrid approach employing both Type 1 and Type 2 was used by the KLPD to introduce the authorisation concept into SAP R/3. This was necessary due to the different initial positions of the various SAP applications. Type 1 was used for the personnel and logistics modules. Type 2 was used for the financial modules.

**Personnel**

The personnel modules of SAP 2003 were deployed in the second quarter of 2003. This was a greenfield situation, which formed an excellent starting point

for the top-down method (much preparatory work and little tidying up).

**Logistics**

The functions were charted by starting with the actual situation and combining it with the common-sense method. After that the peep effect was utilised (little preparatory work and much tidying up).

**Finance**

Excellent results were achieved thanks to good interactive cooperation between Application Management and Functional Management.

Once the authorisation concept had been introduced, the authorisations in the various modules were reasonably well standardised. After this, a phase was started in which the structures of the roles were fine-tuned to yield a truly unified authorisation concept.

**7.4 Separation of duties**

The various steps in the authorisation procedure are assigned to persons holding different positions:

- *Disposition task*  
This task lies with the persons who have been empowered to grant authorisations for using an information system and the information in it. This involves the heads of the FEA, P&O and Logistics departments.
- *Registration task*  
This task lies with SAP Functional Management, which is tasked with assessing the granted authorisations based on the defined conditions (signalling task) and handling the granted permissions (this does not apply to Functional Management's own authorisations). It maintains a central registry of this. FM also has an advisory function.
- *Execution task*  
This task lies with Application Management, which actually implements the authorisations in SAP R/3.
- *Control task*  
Day-to-day supervision of the use of granted permissions is the responsibility of the manager of the organisational unit where the employee is located. Some of the principles here are:
  - If more than one function or functional role is assigned to an employee, a check must be made to see whether this results in an undesired combination of functions.
  - For new or modified functions, a check must be made to see whether the function contains any undesired combination of tasks. A transaction matrix of undesired combinations can be helpful for this.
  - For new or modified SAP R/3 roles and

SAP R/3 composite roles, a check must be made to see whether this generates an undesired combination of authorisations.

Besides this, it is the task of the 'authorisation authority' to monitor proper operation of the authorisation process. The corps manager can periodically have audits performed by an independent EDP auditor. The Audit Department of MIKR performs audits at set times. Adequate reporting options are of great importance with regard to the control activities.

### 7.5 Quantitative data

Table 1 lists some quantitative data related to the authorisation concept as implemented in SAP R/3 at KLPD.

| SAP entity            | Qty    |
|-----------------------|--------|
| Composite roles       | 145    |
| Generic roles         | 17     |
| Derived roles         | 195    |
| (Individual) roles    | 68     |
| Authorisation objects | 1305   |
| Authorisation fields  | 80 671 |
| Users                 | 422    |

Table 1. Quantitative data, December 2003



Figure 6. (zie vervolg)

Composite role  
(function)

|              |                                |
|--------------|--------------------------------|
| Rol          | HRM01 : PMA_DWP                |
| Omschrijving | VR HRM PMA Dienst Waterpolitie |

Omschrijving Rollen Menu Gebr. Perso

| Rol                        | Omschr.                                   |
|----------------------------|---|
| 0000 : BASIS_KLPD          | ALG Basis rol voor iedere KLPD gebruiker  |
| 0000 : HRM_RAPPORT         | HRM Algemene rapportages                  |
| 00 : ALGEMENE_WEERGAVE_DWP | HRM Algemene weergave Dienst Waterpolitie |
| DWP_ : PMA                 | HRM PMA Dienst Waterpolitie               |

Role  
(task)

|              |                             |
|--------------|-----------------------------|
| Rol          | DWP_ : PMA                  |
| Omschrijving | HRM PMA Dienst Waterpolitie |

Omschrijving Menu Bevoegdheden Gebr. M

Menu van rol

- PA10 - Personeelsdossier
- PA20 - Personeelsstamgegevens weergeven
- PA30 - Personeelsstamgegevens verzorgen
- PA40 - Procedures

Doels

Transaction codes  
in the menu

Authorisations

**Rol weergeven: bevoegdheden**

Verz.: 0 niet-verz. org.niv., 0 open velden, Status: Ongewijzigd

|                    |  |                |
|--------------------|--|----------------|
| DWP_ : PMA         | HRM PMA Dienst Waterpolitie                            |                |
| Standaard          | Applicatieoverkoepelende bevoegdheidsobjecten          | AAAB           |
| Handmatig          | Basis - ontwikkelomgeving                              | BC_C           |
| Handmatig          | Personeelsbeheer                                       | HR             |
| Standaard          | Personeelsplanning                                     | PLOG           |
| Handmatig          | HR: Rapportage   | P_ABAP         |
| Gewijzigd          | HR: Stamgegevens                                       | P_ORGIN        |
| Gewijzigd          | HR: Stamgegevens                                       | DWP_ : PMA_F00 |
| Bevoegdheidsniveau | D  | AUTHC          |
| Infotype           | 0007-0009 0014, 0027, 0059-0060, 0127, 0303, 9915-9917 | INFTY          |
| Personeelsgebied   | DWP  | PERSA          |
| Medewerker sgroep  | *  | PERSG          |
| Subtype            | *  | SUBTY          |
| Organisatiecode    | *  | VDSK1          |
| Gewijzigd          | HR: Stamgegevens                                       | DWP_ : PMA_F01 |
| Standaard          | HR: Clusters   | P_PCLX         |
| Gewijzigd          | HR: Transactiecode                                     | P_TCODE        |

Figure 6. (zie vervolg)

| No. |                       | Description                        |
|-----|-----------------------|------------------------------------|
| 1   | Role                  | Technical name                     |
| 2   | Role                  | Description                        |
| 3   | Authorisation objects | Names                              |
| 4   | Authorisation objects | Technical names                    |
| 5   | Objects               | Descriptions                       |
| 6   | Objects               | Technical names                    |
| 7   | Object fields         | Descriptions                       |
| 8   | Object fields         | Technical names                    |
| 9   | Object content fields | Authorisation values or operations |

Figure 6. Example of a (single) function and its associated authorisations

## 8 Experience

### 8.1 Introduction

Configuring logical access security and authorisations in SAP R/3 is no easy task. From experience, it is evident that putting an authorisation concept into practice is often accompanied by complaints regarding authorisations. KLPD's experience in introducing the new authorisation concept based on functions and roles is described in Section 8.2. Experience from elsewhere is described in Section 8.3.

### 8.2 KLPD experience

#### General

- There is a (natural?) tendency to assign personal functions and roles. Although the literal sense of the model is followed, the underlying philosophy and principles are not followed.
- The chosen method provides a good opportunity for separation of the duties of FM and AM.
- No AM actions are necessary when people change positions, so the number of technical changes is much smaller.
- The authorisation concept gives auditors and administrators a considerably better view of granted authorisations than before.
- The implementation was performed using a combination of the actual situation and the common-sense method. This allowed a start to be made (see *Compact*, 2003/1). After that, a top-down stage was necessary for optimisation.

#### Logistics

- During the implementation of SAP R/3 Enterprise, the employees of the Logistics Department were confronted with many authorisation changes, which caused work processes to stagnate.
- As the Logistics Department did not provide sufficient input, the authorisation concept for the Logistics Department was implemented according to the Administrative Organisation.
- During the initial weeks after the implementation, (provisional) ac-hoc makeshifts were used to allow work to continue. The primary reason for this was that the authorisation concept was not adequately tested, due to employee absences in the Logistics Department.
- The Logistics Department desires to achieve a situation in which process responsibilities are assigned to a single position and the departments cooperate more on getting the entire job done.
- To prevent authorisation problems from occurring, end users must not be given (excessively) broad authorisations.
- SAP Application Management desires to transition to a (more) manageable authorisation concept and implementation that is easy to maintain and easy to understand for the KLPD as well as the MIKR Audit Department.
- The end users have been informed that the Administrative Organisation and authorisations will be restructured. This may mean that in the near future, certain tasks must be done by someone else in the organisation.
- It will be indicated which information must be

classified in connection with an extra security level for weapons and munitions.

### Finance

- FEA experienced the combination of introducing a new release of SAP R/3 (Enterprise) and a new authorisation concept as a severe strain ('it was made rather difficult for both sides'). As a result, a number of authorisation requests were put aside at the beginning.
- The new authorisation concept has produced increased separation of duties.
- The working method of Functional Management has changed. The new authorisation concept demands more 'think before you act'.
- Functional Management is obtaining better insight into SAP R/3.

### Personnel

- Employees of the Personnel Department are only authorised to access data for the employees in their department. In some cases, employees are authorised for several departments. This causes problems when an employee changes departments. One solution would be to use a dummy department. If all relevant personnel employees have access to this dummy department, a relocation can be made via the dummy department. For a relocation from department A to department B, the employee in department A can move the relevant data to the dummy department. The employee in department B can then move the data from the dummy department to department B. Presently, relocations are performed by a central personnel staff member. An argument for continuing to use this method is that using a dummy department is cumbersome and requires absolute precision. For a central staff member, relocations will be a routine task, but for local personnel employees they will be infrequent events.
- If an employee is moved from department A to department B, the historical data (the data prior to the time of relocation) are not accessible to the personnel employee in the new department. If necessary, the personnel employee in department B will request information from his colleague in department A.
- The policy states that all employees have only one function, but exceptions can be made for

good reasons. This will certainly be the case for several employees in the Personnel Department.

- An authorisation policy is needed.
- There will be a new function for the Training and Event Management (TEM) module. The employees in question are not permitted to have access to weapons data and the Special Investigation Applications Department.
- Employees 'can do what they have to do'.
- It is not absolutely necessary to technically enforce all authorisations; procedural agreements can be adequate in some cases. The challenge is to find a good balance. This can be determined using a risk analysis. With regard to screening off the Special Investigation Applications Department (DSRT) and the National Investigation Department (DNR), technically enforced authorisations are necessary.
- *The implemented authorisation concept is a very good system. One of its positive effects is that the organisation increasingly thinks in terms of functions instead of persons.*

### Functional Management

- *The authorisation concept is clear.*
- The decision to use a 'general display role' was a good choice.
- The chosen nomenclature is not always the best; a few adjustments would be desirable.
- One of the composite roles caused problems, but that has been solved.
- Where will the control body be positioned, and what will be its tasks?
- Will there be separate start menus for new projects, such as Contracts and FLIMS (Flight Maintenance of the Aviation Police Department)?
- Who maintains and manages the matrices of composite roles versus roles?
- The request procedure for roles must be refined.
- Replacements and holidays must be taken into account when granting administration authorisations.

### Application Management

- Using authorisations that are valid for only one or a few departments ('area of responsibility') creates *much work* and *restricts the operational flexibility* of employees:
- If a replacement is necessary for an employee due to illness or holidays, the replacement must

quickly have the new authorisations. If this does not work well, there is risk that people will use each other's user IDs and passwords.

- When restricted areas of responsibility are used, a *generic role* and the associated *derived roles* are used in the authorisation concept. Although derived roles are not supposed to be modified, this has occasionally happened. When a new generation of the associated generic role was created, the changes to the derived roles disappeared.
- Some employees find that screening off at the departmental level has gone too far and ask themselves 'Aren't we supposed to be a single organisation?'
- Although there is understanding for screening off (restricting access by colleagues) for a few departments, such as DSRT and DNR, people still wonder, 'How confidential can the DSRT data in SAP R/3 actually be?'
- Testing authorisations (particularly the negative tests) after changes takes a lot of time.
- Application Management must try to develop a method for formulating roles that causes roles to have a limited scope, allows them to be reused when formulating new functions, and avoids having to test them again when another role in the same function is modified.
- New functions should have to be approved by a control body. This acts to raise the threshold and prevents excessive function diversity.
- The KLPD has experienced various release changes. The profile generator tool has only been available in recent versions. Consequently, the SAP R/3 system in the KLPD had manually constructed profiles and authorisations as well as profiles and authorisations built using the profile generator. In a manner of speaking, the KLPD continued to further embroider at the level of release 3.0. With the change to the SAP R/3 Enterprise release and the new authorisation concept, the KLPD has again reached a 'state of the art' level with respect to authorisations in SAP R/3.

### 8.3 Experience elsewhere

#### KPMG

KPMG has conducted a large number of SAP R/3 security studies in the form of audits and 'quick scans' in the area of logical access security. The SAP

R/3 Security Competence Center has analysed the key aspects of the results of thirty-five studies. From these analyses, it is evident that shortcomings were found in a large percentage of the organisations, ranging from the basic measures to configuration and management. These are often due to insufficient knowledge or a lack of attention. Based on this study, KPMG has prepared several tips (see Table 2).

## 9 Conclusions and recommendations

### 9.1 Conclusions

- *The implemented authorisation concept is considered to be a very good system.* One of its positive side effects is that the organisation increasingly thinks in terms of functions instead of persons.
- It is important to maintain strict separation of duties between Functional Management (registration function) and Application Management (execution function) with regard to authorisations for SAP R/3. The chosen method makes this quite feasible.
- No action by Application Management is necessary for job changes, so there are many fewer changes.
- The authorisation concept gives auditors and managers a much better view of the current situation than before. In a manner of speaking, the authorisation concept has changed from a 'black box' to a 'white box'.
- The configuration of the Administrative Organisation needs improvement. Beside further improvement of the processes, it is desirable to have a matrix of undesired combinations of functions and tasks.
- New functions should have to be approved by a control body.
- Using authorisations that are valid for only one or a few departments ('area of responsibility') creates much work and restricts the operational flexibility of employees.
- The administration functions related to authorisation must be honed.
- With the change to the SAP R/3 Enterprise release and the new authorisation concept, the KLPD has again reached a 'state of the art' level with regard to authorisations in SAP R/3. The experience gained with the new authorisation concept can also be used in other KLPD informa-

| Tip | Description  |
|-----|--|
| 1   | Create authorisations for administrators as 'quick wins' using the principle 'all activities except...'  |
| 2   | Replace broad authorisations for developers and consultants with display authorisations.   |
| 3   | Utilise the knowledge of your external advisor for configuring the relevant security parameters and filling in the tables.   |
| 4   | Analyse the logging features in SAP so you can use them to best advantage.   |
| 5   | Test the authorisations negatively as well as positively.  |
| 6   | Select a structure for the authorisation concept that is sufficiently flexible, manageable, controllable and secure.   |
| 7   | Use authorisation options as restrictively as possible.  |
| 8   | Create a role-based configuration using flexible building blocks.  |
| 9   | Isolate critical transactions functionally and technically into their own roles.   |
| 10  | Give careful thought to clear nomenclature.  |
| 11  | Also secure made-to-measure work.  |
| 12  | Monitor the presence of inactive users and remove them in a timely manner.   |
| 13  | Familiarise yourself with the Computer-Aided Test Tool (CATT) and use it for administration and configuration, for instance when uploading and downloading authorisations. |
| 14  | Establish clear agreements for making security impact analyses for change requests.  |
| 15  | Analyse the utility and capabilities of the support tools.   |
| 16  | Involve your own administrators in configuring the authorisation concept during the project.   |
| 17  | Use Access or Excel with data from SAP tables to keep your documentation current.  |

Table 2. Tips from a KPMG study

tion systems and elsewhere within the police organisation.

**9.2 Recommendations**

- Provide good reporting capabilities with regard to granted authorisations.
- Further elaborate the AO procedures, including with regard to Functional Management and Application Management.
- Configure the control function, in addition to the disposition, registration and execution function.
- Investigate the need for restricting authorisations to the area of responsibility of personnel staff members.
- Try to achieve a good balance between technical and procedural measures, instead of attempting to enforce all authorisations by technical means.
- Give further attention to the administration functions.

## 10 Opinions on the New Authorisation Structure

### *The opinion of... Jacqueliën Wijnhoud*

*Jacqueliën Wijnhoud works in the Functional Management section of the Financial/Economic Affairs (FEA) group department. Her primary area of responsibility is Human Resources.*

*Jacqueliën: 'Using roles and composite roles in SAP makes things clear, and so do the naming conventions that are used. With them, it's immediately clear which role you're looking at. The composite roles are grouped roles, so they give you a good overview of the functions available in a particular module.*

*I find it irritating that the user organisation regularly requests a new role or composite role without knowing what effect this will have in SAP R/3. People don't give sufficient consideration to other options, and once the role has been built, they realise it's not exactly what they wanted. The preliminary study is not adequate. This is especially true for projects that have a rather independent character, and where Functional Management is not sufficiently involved.'*

### *The opinion of ... Albert Aarts*

*Albert Aarts works in the Functional Management section of the Financial/Economic Affairs (FEA) group department. His primary area of responsibility is Finance.*

*Albert: 'It used to be simpler. We just passed the requests on to Application Management, who ensured that the new wishes were honoured. It worked, and no one looked to see whether users sometimes had authorisations that were too broad. In short, some users accumulated quite a few authorisations, and we lacked an overview. But the new authorisation concept based on 'need to know' and 'role-based' takes a bit of getting used to. There is more separation of duties, and that costs me quite a lot of time. I have to think more about something before doing it, and I sometimes run into problems when I'm surprised by an authorisation deficiency somewhere during the testing process. This is partly because some transactions pass data 'under the counter' to another transaction, which may be outside the granted authorisations. A big advantage is that I'm learning a lot more about SAP R/3, and that's really great!'*

*The opinion of ... Hans Smits*

*Hans Smits is the 'first among equals' in SAP Application Management.*

*'In contrast to the previous concept, the new authorisation concept is strongly based on functions within the organisation. That makes it possible to separate user administration from authorisation development. This produces a meaningful and logical separation of duties. The new authorisation concept was introduced at the same time as a new release of SAP R/3 (Enterprise). Although various things made strong demands on the (user) organisation, this did not cause any delays. By resolutely adhering to the new authorisation concept and using common sense in configuring the authorisations, we were able to exact the cooperation of the user organisation. Of course, that means that if the user organisation puts little effort into the new concept during the implementation phase, extra effort must be put into it during the maintenance phase. This could be clearly seen at KLPD. SAP HR was implemented in 2002, which already gave us a head start on the new authorisation concept. There were hardly any problems with this module with the release change. The authorisations related to the SD and MM modules had been regularly modified over the years and had become strongly person-specific. In that case, changing to function-related authorisation is no easy task. It demands a lot of understanding and patience from the implementer, as well as from the user organisation. As a result of adhering to the concept, the user organisation also started to think in a more function-oriented manner. Besides contributing to a better understanding of the authorisation concept, this also helps the KLPD in considering how to configure its processes and promotes 'chain awareness'.'*

*The opinion of ... Gé Kramer*

*Gé Kramer is the head of the Applications section, which is responsible for SAP R/3.*

*'Implementing an authorisation concept was a difficult issue from the very beginning of the SAP R/3 implementation. These capabilities were simply unknown to the organisation with the (outdated) applications it was using. Such advanced capabilities for separating duties were very limited at that time. The culture was also not always conducive to letting itself be forced into such a rigid scheme. The KLPD was initially a merger of several highly different police activities that could not be placed in a regional organisation, and they were housed in several divisions. A reorganisation was started in 2000, with twelve primary departments and four group departments being established in order to better fit with the organisation of the regional corps. This change had direct consequences for the match between the processes and the tasks for which people were made responsible. During the most recent implementation of HRM, an activity was immediately identified for streamlining the processes and implementing the SAP configuration on that basis. The SAP authorisation concept, which is a science in itself with very many possibilities, was a direct aid in this process. Not everybody shared this opinion. Separating processes from person-specific tasks was a major change to the status quo. Because the implementation and actual maintenance fall within the ICT organisation, the attention to the authorisation concept quickly came to be seen as a new hobby of the ICT group. It is thus important for management to play an active role in implementing separation of duties based on the AO. The authorisation concept must therefore be a direct reflection of the AO agreed on by management. Now that the authorisation concept is operational, practical experience shows that the theory is sometimes at odds with everyday reality. Fine-tuning after the implementation is thus also necessary, and here it is necessary to be alert to attempts to again implement person-specific authorisations.'*

**About the authors**

**Ir. A.J. van Dijk RE** is an independent IT consultant and IT auditor employed by Avédé-Info B.V., Zoetermeer. He has conducted IT audits at the KLPD and is the project manager of the POTVIS project, which aims to improve the SAP R/3 infrastructure in the KLPD.

**A.L.P. Algra** is employed as a Senior SAP Consultant at Ordina Enterprise Applications. He has acted as a consultant for introducing and improving the authorisation structure in SAP R/3 for many companies, including multinationals. At the KLPD, he is involved in the POTVIS project, in particular the introduction of the new authorisation concept.

**References**

- [Algr2003] Algra, Ton, SAP Autorisatie Concept, KLPD KLPD/Ordina, 2003 (internal)
- [Baut2000] Bautz, J., e.a. Checklist informatiebeveiliging, Praktijkreeks Informatiebeveiliging, Ten Hagen en Stam, 2000
- [Dijk1994] Dijk, Aart J. van, Schermbeeldcommunicatie en autorisatie, Informatie, March 1994, vol. 36 no. 3, pp. 191–198
- [ECIB2001-1] ECIB, Informatiebeveiliging Nederlandse Politie, Basisbeveiligingsniveau Nederlandse Politie (BBNP), ECIB, Den Haag, 13 December 2001
- [ECIB2001-2] ECIB, Informatiebeveiliging Nederlandse Politie, Autoriseren, ECIB, Den Haag, 13 December 2001
- [Ferr2003] Ferraiolo, David F, D.R. Kuhn and R. Chandramouli, Role-Based Access Control, Artech House, Boston/London, 2003
- [Hael2002] Haelst, Werner van and Jack van der Voort, Trends in het beoordelen van SAP R/3-toegangsbeveiliging, De EDP-Auditor, no. 1, 2002, pp. 11–18
- [IBM2003] IBM Business Consulting Services, SAP Authorization System, Design and Implementation of Authorization Concepts for SAP R/3 and SAP Enterprise Portals, SAP PRESS, Waldorf, 2003
- [Mien2003] Mienes, P. and B. Bokhorst, De (on)beheersbaarheid van toegangsbeveiliging, Compact, 2003/1, pp. 42–50
- [Moss2002] Mossinkoff, O., AO/IC en autorisaties, Project Jurist 2002, Ministerie van Justitie, Den Haag, 2002
- [Regi2001] Regieraad ICT, Bestek 2001-2005 Voor de vernieuwing van de informatiehuishouding van de Nederlandse politie, Driebergen, 16 February 2001
- [Slui2000] Sluiter, J. and A.J. Vethman, Role based access control in e-business, Informatiebeveiliging, Jaarboek 2000/2001, pp. 44–49
- [Review] Review The concept of this article was reviewed by the following persons: Willem van Amerongen (ICT Operations, Applications), Gé Kramer (ICT Operations, Head of Applications), Peter Regien (FEA, Head of Functional Management), Hans Smits (ICT Operations, SAP Application Management), Gertwin de With (FEA, AO/IC)
- [Twee2003] Tweede Kamer der Staten-Generaal, Zicht op taakuitvoering politie, 28 791, Sdu Uitgevers, Den Haag, 2003
- [Vree2001] Vreeke, A. and D.M. Hallemeesch, Richt jij de autorisaties even in?, De complexiteit van het SAP R/3-autorisatieconcept, Compact, 2001/6, pp. 27–33
- [Wel2003] Wel, J.A. van der and N.L. Homma, Gegevensbeveiliging aan alle kanten lek, Automatisering Gids, 5 September 2003, p. 17