



# ORKA

## **Organisatorische Kontrollarchitektur –**

### **AP 1.1: Erstellung und Analyse der Fallstudien**

### **Use Case Scenarios for Organizational Control with respect to Business Processes**

Version 1.0 - Januar 2007

## Contents

<b>1</b>	<b>Introduction .....</b>	<b>3</b>
<b>2</b>	<b>Case Study A: Updating a Law in Austria.....</b>	<b>5</b>
2.1	Background.....	5
2.2	Process Description: Updating a Law .....	5
2.3	Case study characteristics.....	7
<b>3</b>	<b>Case Study B: Loan Origination Process in Banking Domain.....</b>	<b>9</b>
3.1	Case Study Characteristics .....	10
<b>4</b>	<b>Case Study C: An Inpatient Health Care Scenario .....</b>	<b>12</b>
4.1	Case Study Characteristics .....	13
<b>5</b>	<b>Case Study D: Cross Organizational Engineering Process .....</b>	<b>15</b>
5.1	Case Study Characteristics .....	16
<b>6</b>	<b>Conclusions .....</b>	<b>17</b>
<b>7</b>	<b>References .....</b>	<b>18</b>

## 1 Introduction

This is one of the very first work packages in the project ORKA. It describes several case studies to underline on the one hand the importance of dynamic organizational access control which is necessary in the professional field of IT-Systems. On the other hand this work package builds the foundation for further work in this project by describing which dynamic requirements an organizational access control system must support.

Access control takes place in various system environments. And every environment specifies with constraints under which circumstances a subject's authorization request is finally approved. However, in contrary to access control in, for instance, legacy systems (file servers, database management systems, etc.) or standard web services where access authorization decisions are usually determined in a stateless<sup>1</sup> manner, in business processes a subject's previous actions on certain tasks or objects during a workflow execution may influence access control decisions for permissions on later authorization requests. This requires on the one hand that the information about a subject's previous actions have to be available for the authorization evaluation process. On the other hand the policy specification language which finally is the tool to define the access control constraints has to support the required expressiveness to enable the specification of the above mentioned types of restrictions.

The following sections describe case studies which illustrate business processes in different scenarios. More precise, these case studies describe situations which illustrate the need for dynamic access control solutions as an organizational control instance for today's enterprise IT infrastructures. They especially show dynamic requirements for access control in business processes that are more complex than standard models as, for instance, RBAC96 [11] support.

The identified requirements will directly influence the requirements analysis for the specification language which is part of work package 2.2. Furthermore, the presented case studies will support the design phase for the development of the system architecture within the topic ENFORCE.

In the following paragraphs the four case studies concerning business processes are briefly introduced. We also state to which main types of requirements according to access control in workflows the single case studies contribute. This is followed by comprehensive descriptions of the single case studies and a listing of their generalized access control requirements.

The first of the four case studies describes the update process of an existing law as observed at the Austrian Federal Chancellery in the context of the Austrian Information System. The second case study provides an example of a typical loan origination process in the banking domain when a customer applies for a credit.

Both case studies have been chosen because they show typical characteristics in terms of separation of duty requirements. They illustrate that especially in business processes dynamic access control requirements are needed; requirements which have to be evaluated at run-time rather than during design-time as already Crampton [12] describes in his work.

---

<sup>1</sup> Stateless in this case means that the service deciding about a subject's authorization on a certain object does not take into consideration any previous actions a subject may have performed.

The third case study plays in the health care domain where a patient is transferred between various wards during his stay at a hospital. This scenario shows characteristics to be considered when access control should be based on object specific attributes as, for instance, the patient's health record. It should only be accessible by the doctors and nurses stationed at that particular ward the patient is located at the moment where an access to the record is requested.

The fourth case study illustrates a cross organizational workflow. In this scenario business partners work together on one project; but despite this collaboration, the internal workflow still have to remain hidden from external viewers. This case study follows the argument that also within a collaboration with different partners, companies do not want to publish their internal workflows and accompanying access control policies.

The following sections describe the four case studies in detail and show which restriction requirements the single scenarios depict.

## **2 Case Study A: Updating a Law in Austria**

This section describes a scenario as observed at the Austrian Federal Chancellery (BKA) in the context of the Austrian Legal Information System (RIS) (<http://www.ris.bka.gv.at/>). The overall aim of this system is to replace printed law texts by digitally signed electronic documents [1]. We first introduce the system as a whole, and then we detail the steps of the process.

### **2.1 Background**

The Federal Chancellery is one of 12 ministries in Austria. To fulfill their administrative duties these ministries use a variety of supporting IT systems.

One of the systems is called eLaw. This is an electronic legal records processing system which certain ministries make shared use of. This system can, for example, be used to facilitate and manage changes to existing laws. As such, eLaw may be classed as a records management system for public administration. The workflows implemented in eLaw are enforced through Fabasoft's eGov Suite 5.0.

Legislative information (e.g. gazettes, instruction edicts or tribunals) and the law that has been agreed upon by the involved political parties, is published in the Austrian Legal Information System RIS. The aim of this system is to replace printed law texts with digitally signed electronic documents, which are legally binding. The RIS currently provides services to more than 17,000 public administration officers over a nation-wide Intranet dedicated to the task. In addition, the general public may access the electronically published law via the Internet. RIS users access more than 6.5 million documents each month. The daily update rate of the RIS information repository can be up to several hundred documents changed on-line, with the system required to be constantly available: 24 hours a day, 7 days a week, all-year round.

The eLaw system is one of more than 30 public administration systems that feed data for publication into the RIS. Other such systems include the Supreme Court, the Administrative Court and the State governments.

### **2.2 Process Description: Updating a Law**

A typical scenario detailing the use of eLaw and its interaction with the RIS is that of a change to existing law, e.g. a change to the law concerning the Austrian Highway Code. This process is illustrated by Figure 1, and in the rest of this subsection each paragraph describes a step of the process (denoted by a rectangle in the diagram). Note that each step is based on a specific law which prescribes the exact legislative procedure; however, a more detailed analysis is not possible in this context.

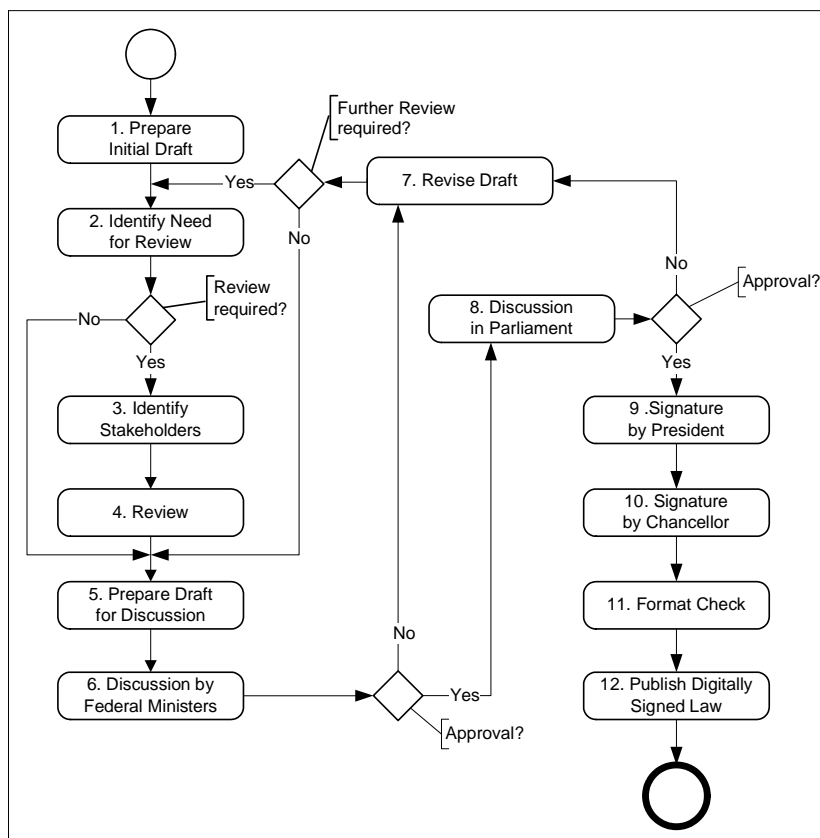


Figure 1: Workflow Representation

A law clerk working for the ministry of transport prepares a draft of the proposed change (step 1). This draft is initiated within the eLaw system (i.e. it is given an initial classification and some MS Word Documents are created). It is then decided whether the draft should be reviewed by external stakeholders (step 2). In our case of a change to the Highway Code, the draft would normally be sent to the Austrian Automobile Club for comments. The stakeholders are identified and invited either electronically (via email) or by post to review and comment on the draft bill (step 3). The draft is made available to them by physically sending them a copy of the draft or through the RIS (but not using an electronically signed format at this stage).

The stakeholders then review the draft (step 4), and send back their review either electronically or by hardcopy. A deadline may have been set for the review. Once the deadline for the stakeholders' review and comments has passed, the draft is prepared for further discussion (step 5) by a department responsible for coordinating the meetings of ministers, and the draft is eventually put on the agenda of the weekly meeting of the Austrian federal ministers.

If at the discussion (step 6) the draft is rejected, it has to be proposed again by the initiating ministry. In this case the draft is revised by a law clerk (step 7) and it is decided whether further review of the revised text is required. If the federal ministers agree to accept the draft without change, it becomes a government bill and is put into the RIS. At this stage there is no binding digital signature.

The bill is transferred to the systems of the parliament, which run independently of the eLaw and RIS environments. At this stage, an .rtf file containing the government bill is prepared and is placed on a dedicated server where it can be collected by the parliament's systems.

The government bill is now discussed by national council and then by the federal council (step 8). Both chambers may either agree or disagree, and possibly change the government bill. In case of an agreement, the text is passed back to the eLaw system and BKA to be published in the federal law gazette. In case of a rejection or possible veto, the draft is again revised by the originating ministry (step 7), the same way as if it was rejected by the federal ministers. The publication of the bill must obey very strict structural and layout requirements which are currently enforced through a set of MS word macros (over 70 different templates).

Prior to final publication, the president must sign and approve that the change to the law has been performed according to the constitution (step 9). Note that he approves that the legal process has been correctly followed; he does not approve the content of the bill. The president's approval must also be countersigned by the chancellor (step 10). These two steps currently require a paper-based signature.

A final check of the new or changed law is performed by the constitutional service (which is a department of the federal chancellery), who also give the document the appropriate label with respect to the federal law gazette (step 11). The changed law is then published in the RIS after it has been digitally signed to provide authenticity (step 12).

### **2.3 Case study characteristics**

Based on available data from private sector organizations [2][3][4], we believe that the threats to systems dealing with law texts originate from the inside of an administration rather than from the outside. Unlike a forged cheque which is only paid out once, a manipulated electronic law text may become legally binding to an entire country and may be applied in thousands of instances. Accordingly, after having described the legislative process, we now analyze some of its specific requirements in the area of security, and more specifically regarding access control. To illustrate our requirements we present possible but partially "hypothetical" threat scenarios from different stages in the process described above.

**Requirement 1:** One of the most often ignored requirements, despite being one of the most obvious, is that a legal clerk should not work in two incompatible offices. For example, a clerk working in the ministry of transport should not have access to information in the department responsible for releasing public tenders for highway maintenance.

In the specific context of the Austrian Chancellery, there is a strict policy that clerks working in different sections should not interact. This supports the validity of our presented requirement.

**Requirement 2:** The clerk initiating a legal draft should not be the principal who decides whether reviews by stakeholders are required.

Several possible threats arise if the initiating clerk is responsible for deciding about the need for review. For example, he may have a personal interest in the change he made, and will want to skip reviews, so that changes will go unnoticed.

**Requirement 3 a:** A clerk should not be allowed to modify a document and upload it onto the RIS at the same time.

The threat here is that a clerk responsible for drafting the document, and the review of the stakeholders' comments, could publish changes to the RIS immediately. In order to address this threat another clerk should be made responsible for first forwarding the changed document to the appropriate chambers and finally uploading it.

**Requirement 3 b:** A clerk should not be allowed to remove an already agreed upon document from the RIS without having been involved in its prior drafting.

**Requirement 3 c:** A clerk should only be allowed to remove an already agreed upon document from the RIS if he has not been involved in its prior drafting.

Requirements 3a – 3c represent possible alternatives for a requirement regarding addition and removal of documents to RIS, with 3b and 3c being almost the opposite of 3a. However, we observed that from time to time documents which have been agreed upon have to be removed from the RIS when small mistakes (e.g. a wrong date or spelling) were noticed.

**Requirement 4:** In case of a rejection (step 8) the draft has to be proposed again by the initiating ministry. However, the draft must not be revised by the same law clerk who initiated the draft.

In this case, it might be that the initiating clerk was too biased in his views and as such a fresh perspective is required.

**Requirement 5:** A clerk should not perform all the workflow steps involving a legal bill.

As a general security requirement, a clerk should not be permitted to work on a legal bill from drafting through to publication. At least one other clerk must be involved at a critical step (e.g. step 12 – final publication). This is often also referred to as a four-eyes principle or dual-control since two principals must agree on a change or supervise each other.

We immediately see from all of the above scenarios that it is essential to provide clerks with only the access rights they need to perform their tasks, limited to the times at which they need them, and only when such rights are compatible with actions they have previously performed. The workflow is the context-providing concept that is required to achieve these three properties and requirements like those above must be addressed with and within the workflow. That is to say that information used to make access decisions is provided by the workflow (e.g. who performed which step on which object), and that access control must be applied at selected steps in the workflow.

### 3 Case Study B: Loan Origination Process in Banking Domain

A standard service provided by a bank is that of offering credits to its customers. This may take various forms such as extending the overdraft limit on a current account; providing mortgages for buying a house; or simply offering a fixed sum of money the customer may use at his discretion. Depending on the specific kind of credit, the application process will differ in the principals involved and data that need to be considered. In fact, the specific type of credit requested will have a direct effect on the involved controls.

In the following we provide an example of a typical loan origination process in the banking domain as shown in Figure 2. The supporting Table 1 summarizes some of the required roles, the general service, the required access rights and associated workflow steps and business objects.

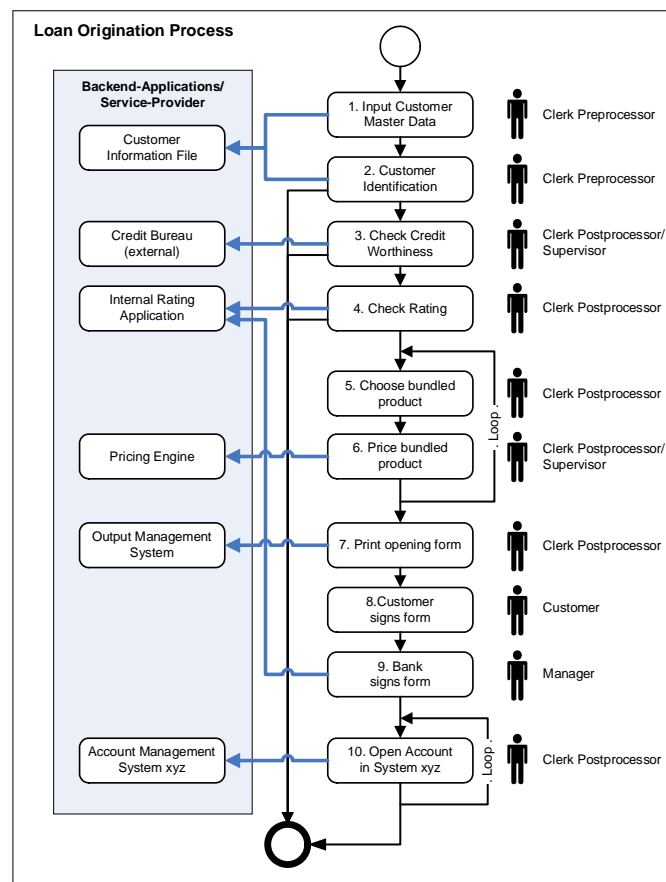


Figure 2: Loan Origination Process

The loan origination process describes a customer wanting to buy a bundled product. If he is not an existing customer, his master data and other identification-relevant data need to be entered into the system (step 1 and 2). Several external and internal ratings then need to be obtained by the processing clerk (step 3 and 4) in order to check the credit worthiness of the client (e.g. based on sums of liabilities, sums of assets, reasons for rating etc.). The system will then propose a preconfigured bundled product (step 5) to the clerk and customer (e.g. original price, customer segment special conditions, customer company special conditions, asset limit for price etc.). The customer and Bank finally come to an agreement expressed in the signature of the client (step 8) and Bank representative (step 9). Finally an account for the customer is created (step 10).

Workflow Step	Role	Service	Access Right	Business Object
1. Input Customer Data	Clerk Preprocessor	Customer Information File	query () update ()	Customer Data
2. Customer Identification	Clerk Preprocessor	Customer Information File	query ()	Customer Data
3. Check Credit Worthiness	Clerk Postprocessor	Credit Bureau	prepare () release <100k post ()	Rating Report
3. Check Credit Worthiness	Supervisor	Credit Bureau	release >100k	Rating Report
4. Check rating	Clerk Postprocessor	Internal Rating	query ()	Rating Report
5. Bank signs form	Supervisor	Internal Rating	update ()	Rating Report
6. Choose Bundled Product	Clerk Postprocessor	Product Database	query available products ()	Product Bundle
7. Price Bundled Product	Clerk Postprocessor	Pricing Engine	modify () commit <100k	Product Bundle
7. Price Bundled Product	Supervisor	Pricing Engine	commit >100k	Product Bundle
8. Print Opening Form	Clerk Postprocessor	Output Management System	post print request ()	Contract
9. Customer signs form	Customer	-	sign ()	Contract
10. Bank signs form	Manager	-	sign () update ()	Contract
11. Open Account	Clerk Postprocessor	Account Management System	open ()	Account

Table 1: Assignments of rights, roles and tasks

### 3.1 Case Study Characteristics

This section now defines a set of possible separation of duty properties. These are subset of the properties we discussed with SAP Banking Solution Architects.

**Requirement 1:** No person may be assigned to the two exclusive roles pre/post processor.

**Requirement 2:** A person may be assigned to the two exclusive roles pre/post processor but must not activate them both within one process. This means that either: a) they are not activated at any state, or b) they have not been activated one after the other.

**Requirement 3:** If the customer is an industrial customer, the master data must be verified by an independent clerk.

**Requirement 4:** If the credit bureau rating is negative then the internal rating must be performed by another clerk.

**Requirement 5:** If the internal rating is negative, then the case must be confirmed by a supervisor.

Requirements 4 and 5 are examples for application specific requirements where the type of access control that has to be enforced is dependent on task specific results.

**Requirement 6:** A clerk may only price a bundled product if he did not perform the operation “modify ()” wrt to the specific offer.

**Requirement 7:** If the customer is an industrial customer, then a clerk may perform tasks 1 to 9 or 10 but not both for the same customer.

**Requirement 8:** A principal may be a member of the two exclusive roles pre/post processor and the complete set of authorizations acquired over these roles may cover a critical authorization set, but a principal must not use all authorizations on the same object(s).

**Requirement 9:** A principal p1 may be assigned to the two exclusive roles post processor and supervisor. He may also activate them but not use them on the same object (Product Bundle).

If we check the process workflow, requirement 9 plays a role at step 6 where we can get two traces:

- a) The pricing at step 6 was done for less than 100k – since there is no supervisor involved, the stated requirement does not need to be enforced in this case.
- b) The pricing at step 6 was done for more than 100k – in this case requirement 9 has to be enforced and p1 can only commit operation as supervisor if he did not handle as post processing clerk before.

Requirement 9 is an application specific requirement where the type of access control that has to be enforced is dependent on object specific attributes; the price of the bundled product in the example above.

### 4 Case Study C: An Inpatient Health Care Scenario

This section describes a case study which focuses on a scenario in a health care environment. The workflow idea was taken from [5]<sup>2</sup> where the author used it to identify security paradigms for collaborations in clinical workflows where access controls mainly depend on object specific details (may a nurse have access to a patient records although the patient is not assigned to the station where the nurse is doing her shift?) rather than on workflow or task specifics (like separation of duties).

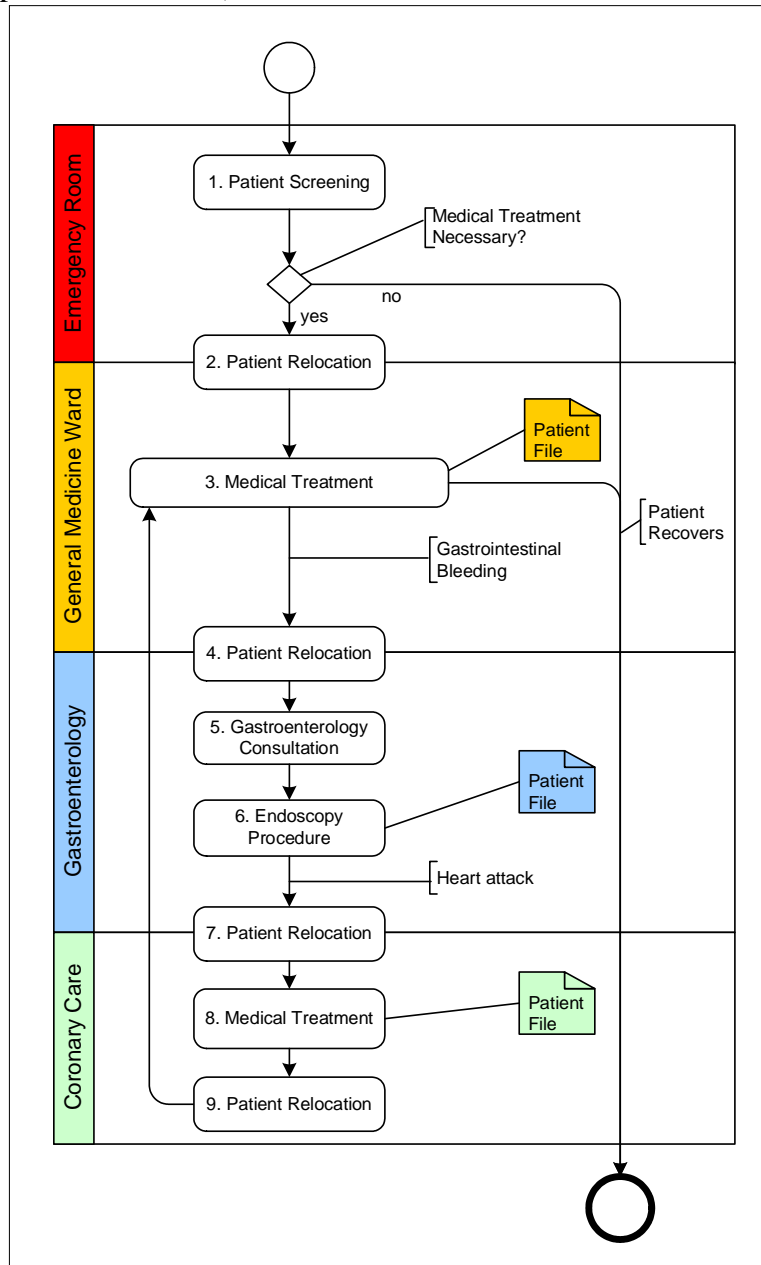


Figure 3: An inpatient health-care scenario

The workflow scenario begins with a visit to the emergency room by a patient who is suffering from pneumonia (see Figure 3). Upon arrival, the patient is quickly screened by a triage nurse (step 1) who determines that the patient needs to be admitted to the general

<sup>2</sup> The use case description and the requirement listing are direct citations from the referenced paper.

medicine ward (step 2). The current primary team that admitted the patient subsequently (step 3) requests a gastroenterology consultation because the patient is beginning to develop gastrointestinal bleeding (step 4). The gastroenterologist who is consulted decides to investigate further (step 5) and proceeds to do an upper GI endoscope procedure (step 6). While undergoing this procedure the patient has a heart attack and is immediately transferred to the coronary care unit (step 7) where a cardiology team takes over the care of the patient (step 8), becoming the primary team. Eventually the patient's heart condition is stabilized and the patient is transferred back to the general medicine ward. After spending a few more days in the hospital, the patient recovers, is discharged, and is told to see his/her primary care doctor for follow-up care.

The following points have been noticed by Thomas [5] about this scenario:

- At any given time, there exists a primary team that is a single point of contact for the patient and takes overall responsibility for the patient's care. The primary team may, of course, change during the course of care (such as when the patient was transferred from the general ward to the coronary care unit).
- A number of clinical staff (users) was involved in various roles in providing care at various points in the workflow. These included general physicians, specialists such as cardiologists, residents and interns, nurses, etc.
- The staff was organized into care teams and each team was associated with a single department or unit in the organization.
- Care teams were often dynamically formed. For example, when the gastroenterologist joined the care team as the result of a request for a gastroenterology consultation. This dynamic formation can be distinguished from the case in which a staff member is pre-assigned by the scheduling department to be on a particular team.

#### **4.1 Case Study Characteristics**

From an access control standpoint, the following requirements have been recognized [5]:

**Requirement 1:** The permissions a clinical staff member has to clinical records (documents) should reflect his/her role in providing care. For example, only the cardiologist may prescribe a certain drug for cardiac-related illness and only physicians, not nurses, may order lab tests.

**Requirement 2:** Only members of a patient's team should be able to get access to the patient's records. Thus, although a physician, P, may have the right to order a lab test by virtue of the qualifications and responsibilities that determine his role, P should have the right to do so for Patient A's record only when P is part of A's care team.

**Requirement 3:** Depending on the workflow, various clinical staff needs access to patient records at different points in the overall workflow. Therefore the primary care team in general wards should be given access to a patient's records only after the ER unit has requested transfer of the patient to one of those wards.

- Requirement 4:** Requirements 1 and 2 above should hold for any staff member who dynamically joins a team.
- Requirement 5:** When a patient is transferred from one unit to another, the members of the primary care team of the second unit should be given access to the records of the patient (according to their roles) and no one else.
- Requirement 6:** Certain team members may delegate duties and associated permissions to other team members. Thus a physician may authorize a resident or nurse to order a specific lab test or referral for a specific patient. The resident would, in this situation, would need limited (probably one-time) permissions to complete this order, even though under normal circumstances, he/she would not be able to give the order directly since their role is not endowed with such privileges.
- Requirement 7:** Once the patient is discharged, all permissions to the patient's medical records should be deactivated.

The patient in the scenario is transferred from one ward to another - over 4 wards in total. Important is that his context changes from one relocation to another. The context is in this case the ward he is currently laying on. With respect to this context it should only be the current responsible care team to be provided access to the patient's records. Would the context of the patient records not be changed when, for instance, a relocation from the General Medicine Ward to the station Gastroenterology occurs, the care team of the General Medicine Ward would have still access to the file whereas the team of the Gastroenterology would not.

## 5 Case Study D: Cross Organizational Engineering Process

The following description shows an example process from the contract management domain. It involves two companies, a Mining Company (JJJ Mining) and a contractor (ABC Engineering). Scope of the process is the entire end-to-end process from the request for tender to the final payment of the contractor. The following figure depicts the process flow which is further explained below.

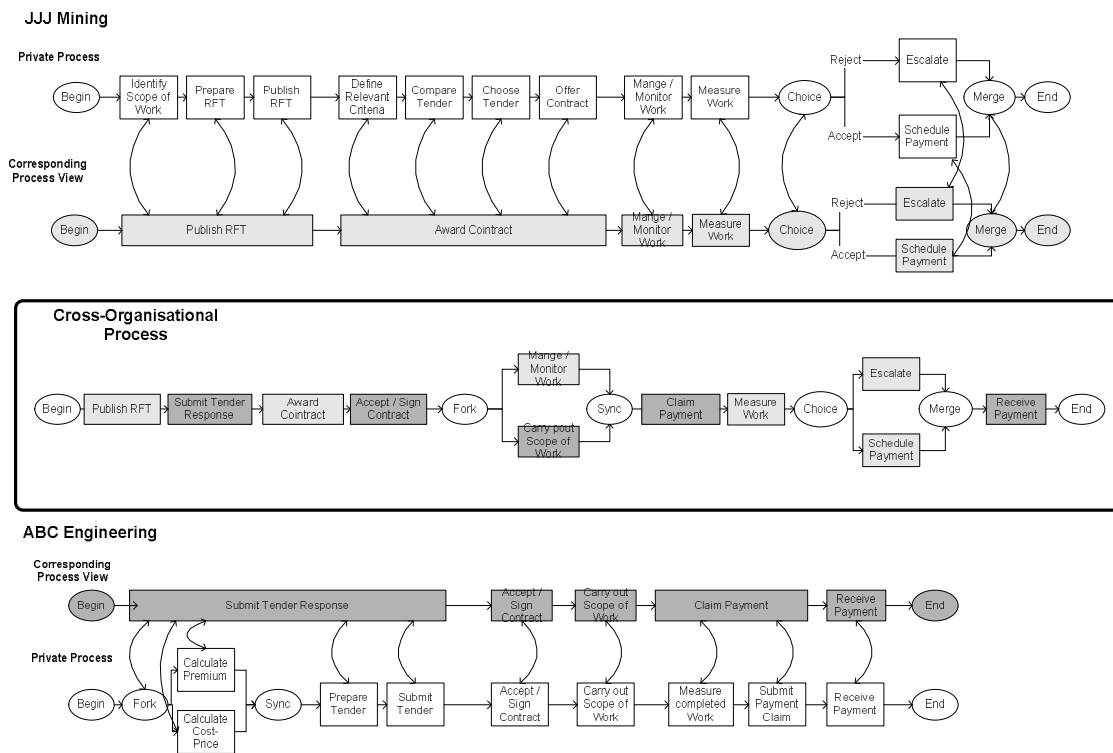


Figure 4: Example Business Scenario - Contract Management

The middle process shows the cross-organizational process as agreed by JJJ Mining and ABC Engineering. It interweaves the publicly available process views of each company. The process starts with the Mining Company making public a request for tender (RFT) that contractors can submit a response to.

To keep this process simple in the context of this paper, we only model the interaction between the Mining Company and the contractor that is finally chosen to deliver the work. Other contractors responding to the RFT are not considered. Internally the publishing of the RFT would involve the identification of the scope of work and a preparation of the tender document. The contractors are only interested in the published RFT; consequently these steps are not exposed in the process view.

Once the RFT is published, ABC Engineering starts working on a response. Among other things the contractor would estimate a cost-price and a premium. Noticeably these are confidential information that should not be revealed to the Mining Company and are therefore hidden in the private process.

Once the contractors have submitted the response, JJJ Mining has to choose which tender to accept and to award the contract. Awarding a contract involves several internal steps which again are hidden behind the view task. Activities include defining relevant criteria to choose the tender, compare the incoming tender according to these criteria, choose the most suitable tender and offer a contract to the contractor. The criteria that are used to choose the contract can be a lowest price, experience of the contractor in similar projects, etc. and observably this is sensitive information which should be concealed.

After signing the contract, ABC Engineering fulfils the work that has been agreed on. While ABC Engineering performs the work, it is managed and monitored by the Mining Company, hence these two process steps run in parallel.

Once the work is completed, the payment has to be arranged. ABC Engineering measures the work that they performed and submits a payment claim. On the Mining company side, the reaction on the payment claim is as follows: A surveyor measures the quality and quantity of the performed work and decides to accept or reject the payment claim depending on the results. If the payment claim is accepted, the payment is performed and the process ends. If the performance feedback of the surveyor doesn't correspond to the payment claim, an escalation process is started in which the contractor only receives payment according to the performed work and this process finishes. On the contractors side either the total amount of the payment claim or a part of it will be received. Assuming that any steps that result from a not full payment of the amount will trigger an exception process, this process ends after payment (total amount or less) has been received by the ABC Engineering.

### **5.1 Case Study Characteristics**

From a security point of view the following requirements can be recognized:

- Requirement 1:** Details of internal workflows shall remain hidden from external observers and global auditing processes. Only abstract process tasks are visible.
- Requirement 2:** Internal policy definitions are hidden from external observers.
- Requirement 3:** Only authorized partners may execute the tasks they are assigned to or agreed on.

## 6 Conclusions

Four case studies have been depicted in the previous sections. All four case studies play in different domains. The first one plays in the field of e-Government, the second one plays in the banking area, the third in the health care domain and the fourth shows characteristics for cross organizational collaborations. And every domain has its own requirements concerning the types of constraints. This selection therefore shows that access control cannot be just seen for one single domain, but different scenarios have to be considered to reflect the broad band of access control requirements to be considered for an organizational control system.

The analyzed results of these case studies now build the foundation for the further work packages in the ORKA project. The requirements listed in the above sections are more or less scenario specific. They will, for instance, lead to more generalized versions in work package 2.2 (SPEC: Anforderungsanalyse - Anforderungen an Beschreibungssprachen für Security Policies).

## 7 References

- [1] Republik Oesterreich BGBl I Nr. 100/2003.
- [2] Shein, E. CEO Warns Threats are Coming from the Inside. eSecurityPlanet.com, June 2004
- [3] KPMG, Fraud Survey Reports 1996-2002, KPMG International Canada, 2002.
- [4] Hulme, G. The Threat from Inside. Information Week, April 2003.
- [5] Thomas, R. K., Team-based Access Control (TMAC): A Primitive for Applying Role-based Access Controls in Collaborative Environments. Proceedings of the second ACM workshop on Role-based access control (RBAC '97), 1997.
- [6] Schaad, A., Moffet, J.: Separation, Review and Supervision Controls in the Context of a Credit Application Process - A Case Study of Organisational Control Principles. In proceedings of the 2004 ACM symposium on Applied computing, 2004.
- [7] Schaad, A., Lotz, V., Sohr, K.: A Model-checking Approach to Analysing Organisational Controls in a Loan Origination Process. In proceedings of the eleventh ACM symposium on Access control models and technologies SACMAT '06, 2006.
- [8] Schaad, A., Spadone, P., Weichsel, H.: A case study of separation of duty properties in the context of the Austrian "eLaw" process. In proceedings of the 2005 ACM symposium on Applied computing, 2005.
- [9] SAP AG: Handbook for Nehemiah and Maestro, 2004.
- [10] W3C: Web Services Architecture. In: <http://www.w3.org/TR/ws-arch/>, found in 2006.
- [11] Sanduh, Ravi S.; Coyne, Edward J.; Feinstein, Hal L.; Youman, Charles E. (1996): Role-Based Access Control Models. In: IEEE Computer, Jg. 29, Nr. 2, S. 38–47.
- [12] Crampton, J.: A Reference Monitor for Workflow Systems with Constrained Task Execution. Symposium on Access control Models and Technologies (SACMAT '05), 2005.
- [13] Koshutanski, H., Massacci, F.: An access control framework for business processes for web services. XMLSEC '03: Proceedings of the 2003 ACM workshop on XML security. New York, NY, USA, 2003.