

Impact of Mobile Dynamic Virtual Organizations on AAA-supported Adaptive Workflows

Semester Thesis in Business Administration
presented
by
Marcus Deluigi
Zurich, Switzerland
matriculation number 00-910-034

Made at the
Institute for Informatics
at University Zurich
Prof. Dr. B. Stiller

Supervisor: Martin Waldburger
Hand over: 15. July 2005

Contents

1	Introduction	8
1.1	Motivation	8
1.2	Task Description	8
1.2.1	Thesis Goals	9
1.2.2	Course of Actions	9
1.2.3	Thesis Overview	10
2	Summary of Key Requirements of Mobile Dynamic Virtual Organisations	11
2.1	Terminology	11
2.2	Requirements	12
2.2.1	Virtuality	12
2.2.2	Mobility	14
2.2.3	Virtual Organisation	15
2.2.4	Dynamicity	16
3	Summary of Authentication, Authorization, and Accounting Requirements	18
3.1	Terminology	18
3.2	Authentication Requirements	20
3.3	Authorization Requirements	21
3.4	Accounting Requirements	21
3.4.1	System Requirements	21
3.4.2	Data Requirements	22
3.4.3	Security Considerations	23
4	Determination of Electronic Workflows	25
4.1	Terminology	25
4.2	Categories of Workflows	28
4.2.1	Ad hoc vs Production	28
4.2.2	Horizontal vs Vertical	28
4.2.3	Stateful vs Stateless	29
4.2.4	Realtime vs Batch	29
4.2.5	Session Related vs Not Session Related	29
4.2.6	Buffered vs Callback	29
5	Definition of Value Metrics Applicable to Workflows	30
5.1	Technical Metrics	30
5.1.1	Timing Characteristics	31

5.1.2	Reliability	31
5.1.3	Usage Metrics	32
5.2	Business Metrics	32
5.3	Pricing Based On Value Metrics	33
6	Definition of an MDVO-AAA Model	35
6.1	Third Party View	35
6.2	Business Processes and Workflows	36
6.3	Tasks and Services with AAA/A4C	37
6.3.1	Authentication and Authorization	39
6.3.2	Accounting	39
6.3.3	Auditing	40
6.3.4	Charging and Billing	40
7	Application of an example scenario to this model	42
7.1	Introduction to the example scenario	42
7.2	Third Party View	43
7.3	Example Business Processes / Workflows	44
7.3.1	Registration	44
7.3.2	Ordering	44
7.3.3	Repair Service	45
7.4	AAA/A4C	45
8	Evaluation	48
8.1	Advantages of MDVO with AAA-supported Workflows	48
8.2	Disadvantages of MDVOs with AAA-supported Workflows	48
8.3	Evaluation of the Suggested MDVO-AAA Model	49
8.4	Analysis of the Example	49
9	Conclusion and Future Work	51
	Bibliography	52

List of Figures

3.1	Authentication, Authorization and Accounting (AAA) and Authentication, Authorization, Accounting and Charging (A4C) with Accounting, Metering and Billing	20
4.1	Task	25
4.2	Workflow	26
4.3	Business Process	27
6.1	Mobile Dynamic Virtual Organisation (MDVO)-AAA Model	35
6.2	Business Processes Model	37
6.3	A4C Model	38
6.4	Authentication & Authorization Model	39
6.5	Accounting Model	39
6.6	Auditing Model	40
6.7	Charging / Billing Model	40
7.1	Third Party Example	43
7.2	Workflow Example 1	44
7.3	Workflow Example 2	45
7.4	Workflow Example 3	46
7.5	AAA Example	47

List of Tables

2.1	Requirements and Recommended Features of Virtuality [1]	14
2.2	Requirements of Mobility	15
2.3	Requirements of virtual organizations	16
2.4	Requirements of Dynamicity	17

List of Acronyms

AAA	Authentication, Authorization and Accounting
A4C	Authentication, Authorization, Accounting and Charging
AS	Accounting System
ATP	Available to Promise
B2B	Business to business
DVO	Dynamic Virtual Organisation
ID	Identification
IT	Information Technology
MDVO	Mobile Dynamic Virtual Organisation
NGO	Non-Governmental Organization
ROI	Return on Investment
SP	Service Provider
VO	Virtual Organisation

1 Introduction

Mobile Dynamic Virtual Organizations MDVOs are regarded as well suited means to support adaptive electronic workflow execution where its participating organizational entities remain legally independent. However, working in a distributed, dynamic, and even mobile or at least nomadic environment imposes some challenging issues to be solved.

1.1 Motivation

Within this semester thesis, MDVOs with their particular characteristics have been analyzed - especially with respect to a classification of different business process types in an inter-domain environment, together with collaborative aspects in dynamically executing and adapting workflows, where MDVO members have to be authenticated, authorized, and the respective workflow steps have to be accounted and charged for.

A platform as the one to be developed within the project Akogrimo [2] will support pervasive access to knowledge by means of offering mobile grid services, that help its possibly dynamically changing organizational members to fulfill complex problems in specific application domains with a clear economic orientation such as e-Health or e-Learning.

1.2 Task Description

Executing adaptive electronic workflows based on mobile grid services imposes the need of an embracing understanding of the following components as well as an outline of the respective interrelationships between them:

- MDVOs: Starting from the quite well researched virtual organizations, new characteristics, possibilities but also requirements have to be identified when taking into account that organization members can join and leave a virtual organization dynamically and that they are nomadic or even mobile.
- Adaptive workflows: Especially in the area of complex problem solving, the solution of one problem easily can provoke following problems to be solved. Consider for example a patient with a heart attack: After that a sensor-equipped mobile device automatically has detected the patient's condition it transmits important status data to an emergency central. This event triggers several other activities to be executed such as to locate medical personnel on duty near the patient's location

in order to send them to the patient. These problems can be represented by electronic workflows. While designing a model to implement these workflows it has to be hold to their adaptiveness and to the possible interconnections of different workflows.

- Authentication, Authorization, Accounting AAA: In an economic-driven business scenario that relies on a services oriented platform able to have built on top of the platform itself domain specific solutions that incorporate possibilities to execute adaptive workflows and that admit service provision to be achieved through possibly many legally independent service, technology or content providers, it appears to be a key issue to have a well working AAA-model in place, for both, services users and service providers.

In particular, the key aim of this thesis work was to develop a model for the collaboration of organizational entities within adaptive workflows in the environment of a mobile virtual dynamic organization, keeping the focus on AAA supported mobile grid services which can guarantee that in every administrative domain all participating actors are correctly authenticated, authorized to access the resources needed to pursue the workflow and that the mobile grid services are reliably accounted by meaningful and appropriate metrics.

1.2.1 Thesis Goals

Considering the various tasks described to be worked on, 3 concrete thesis goals have been derived which can be listed as follows:

- The aim of this thesis is to analyze clear findings in the areas of MDVOs and adaptive workflow executions.
- The subsequent goal is to apply these respective findings on the underlying technical AAA supported grid services infrastructure by means of appropriate requirements definitions.
- The final objective is the development of an MDVO-AAA model which determines the final outcome of this thesis.

1.2.2 Course of Actions

Based on the 3 key thesis goals listed above, the following activities have been conducted and respective results are documented throughout this thesis.

- Summary of key requirements of Mobile Dynamic Virtual Organizations
- Summary of Authentication, Authorization, and Accounting requirements
- Determination of electronic workflows

- Definition of values for workflows and its components
- Definition of value metrics applicable to workflows
- Definition of an appropriate MDVO-AAA model
- Application of an example scenario (e.g., grid services) to this model
- Evaluation of advantages and disadvantages

1.2.3 Thesis Overview

The remainder of this work is structured as follows. Chapter 2 - 3 summarizes the key requirements for Mobile Dynamic Virtual Organizations and for Authentication, Authorization and Accounting. Chapter 4 determines electronic workflows and chapter 5 defines value metrics applicable to these workflows. Chapter 6 sketches an example business scenario. An evaluation in general as well as of the example scenario in detail is done in chapter 7. And, finally, respective findings are concluded and an outlook towards future work is given in chapter 8

2 Summary of Key Requirements of Mobile Dynamic Virtual Organisations

In this chapter, the concept of Mobile Dynamic Virtual Organisations (MDVOs) will be introduced. In a first step, the terminology of MDVOs is described. For this purpose, a structured approach has been chosen. The term itself consists of 4 parts. The description starts from the attribute virtual, leading to virtual organizations and finally to the attributes dynamic and mobile. Thus, mobility and dynamicity are regarded as forming extensions to virtual organizations.

Having achieved that, the second step consists in deriving major requirements on an MDVO with regard to these aforesaid structural areas. This happens with intent to develop an appropriate model for mapping the organizational view of MDVOs to the underlying technical infrastructure, based on AAA-supported grid services. will give a list of key requirements essential for all MDVOs

2.1 Terminology

Virtual Organisations (VOs) are regarded as a suitable reflection for grid computing on an organizational level. The introduction of Mobile Dynamic Virtual Organisations (MDVOs) consequently takes up this concept while carrying on towards the integration of dynamic and mobile grid resources. MDVOs thus are seen as an enhancement of virtual organizations only. In the following, the term MDVO is split into its components, whereupon these elements are described in more detail.

Virtual characterizes the access to services by use of Information Technology (IT) [3].

VOs are alliance organisations of legal autonomous business partners who replace horizontal or vertical integration with virtual integration. As result they appear as a single organisation against the customers [4, 3]. The members of VOs are usually geographically distributed and an VO is established only for a limited time.

VOs have been established for a long time, imagine the supply chain of automobiles or offshore software development. Dynamic VOs become more and more important in an rapidly changing marked. Main Characteristics of VOs are therefore modularity, distribution in space and time and heterogeneity which means that the single companies posses distinct core capabilities [5].

Dynamic Virtual Organisation (DVO) A DVO is one whose composition is frequently changing and the underlying IT system must therefore provide a generic and dynamic way of adding and removing members. This organisation enables the

overcoming of hitherto existing limitations in space, time and organisation. Combined with integration of knowledge it enables companies to react more dynamically and flexible to the market [3].

Mobile describes a system whose end entities (users and/or resources) are moving. This requires the creation of communication infrastructures and the modification of computer networks, operating systems, and application programs. The system has to support mobile users and resources should communicate in a seamless, transparent, secure and efficient way [6].

2.2 Requirements

For every structural element of an MDVO - virtuality, mobility, dynamicity, and virtual organizations - key requirements and recommended features are listed and described. The list is divided into two sections which consist of key requirements that are essential to be considered by every MDVO and recommended features which are not necessary, though seen as being desirable and useful.

2.2.1 Virtuality

Virtuality basically means that an MDVO relies on information and communications technology. This is caused by the assumption that automation and systems integration is a practicable means for lowering transaction costs. However, running a business that heavily depends on communication technology also comes with basic, nevertheless important requirements on the underlying infrastructure. This embraces needs in the areas of confidentiality, integrity and authenticity. Table 2.1 gives a more complete overview in this regard.

Name	Description	Reason	Key Req.	Rec. Req.
Accounting	Recording the use of resources.	The company needs to keep track of the usage for security, efficiency and charging reasons.		X
Addressability of resources	Each entity should be able to address it's packets directly to a resource.	Broadcast messages are not suitable for security and efficiency reasons. The same holds with a central distribution entity.		X

Anonymity	The receiver is not able to determine the sender.	Reasonable especially in areas such as Government, NGO, health care or free services in order to ensure privacy.		X
Audit	Messages with a certain importance are recorded.	Respective regulations have to be respected and the company could get in a position, where it is necessary to trace the events.		X
Authenticity	Guarantees the identity of the sender to the receiver.	For important messages, the company needs to know the real sender.	X	
Classification	The message get classified by some security criteria	Important for auditing and containment. Also applicable for prioritizing the usage of resources.		X
Containment	Certain (confidential) messages cannot leave the network	The company wants to keep its privacy in order not to publish business critical data.		X
Integrity	Guarantees that the message was not altered.	For important messages, the company needs to know the correct content.	X	
Message flow confidentiality	A third party is not able to determine, whether a message was exchanged between to partners.	The knowledge of a message exchange can be an important fact.	X	
Non-repudiation	Enables the receiver to proof to a third party, that the sender actually sent the message.	The company needs to proof a claim, e.g. for orders.	X	
Proof of delivery	The sender can examine, whether the message was received.	Deadlines are important particularly in legal matters.	X	
Proof of submission	Sender can examine, whether the message was sent to a specific mail system.	To exclude technical failures.	X	

Reliability	The IT infrastructure has to be permanently available	A VO ceases to exist in case of a breakdown. Loss of revenue and contract penalties could even lead to insolvency	X	
Resources	All resources needed to run and administrate the IT infrastructure	There have to be enough administrated resources for a company's business and communication. A cost allocation has to be constituted.	X	
Privacy	Prevents a third party of reading a message	Business competitors should not read a company's internal message.	X	
Quality of Service	Availability and minimum response time for services.	For most applications, a certain response time is indispensable.		X
Transparency of resources	It should not be evident to the user, where the resource is and how the it is accessed.	Dealing with technical parameters causes an additional effort on time and costs.		X

Table 2.1: Requirements and Recommended Features of Virtuality [1]

2.2.2 Mobility

Mobility defines, as mentioned above, moving entities. But not only users are mobile: Mobile nodes can also provide services. The term "entity" encompasses users *and* nodes.

Even though mobile devices might be limited for the time being, the human behind represents a *significant* resource. Therefore, the requirements of mobility are mainly about the integration of human into a (possibly adaptive) workflow besides than the technical requirement of, for example, higher and steady bandwidth for the mobile device.

Name	Description	Reason
Session Movement	Nomadic users move around between different terminals [6] and continue their session.	Useful for companies with nomadic users who do not have a fixed workplace (e.g. IBM)

Terminal Mobility	Roaming users, while moving around with their devices, want to continue their sessions when they cross different localities [6].	This happens today in cell phones telecommunications.
Service Mobility	The ability of the infrastructure to maintain the services for a user while he or she is mobile [6].	The services should be independent from the devices and from the location of the user with respect to the network he is accessing.
Location Awareness	The ability to locate the user (mostly by the infrastructure used by the user)	Necessary because of the field of activity of the company, for monitoring and navigation reasons of employees. This is especially important for adaptive workflows.

Table 2.2: Requirements of Mobility

2.2.3 Virtual Organisation

Name	Description	Reason
Transparency	Must prevail in the firms structures: the employees must be straight over responsibilities, contact persons and available entities.	To prevent loss of control
Legal aspects	Aspects concerning, among others, privacy, distribution of services, patenting and licensing need to be clarified.	Single coworkers may work for different companies in conducting their work. Possibly the employers will hold back important information for the project if it is correlated with the company's business. Maybe some of the VO Members work with a competitor at some later point in time.

Knowledge management	A system managing knowledge is essential for permitting access to the know how across company borders. The emerging documentation should also be accessible to all stakeholders.	To prevent loss of expertise.
Quality of Management	It has to be guaranteed that the involved companies are able to master the transferred tasks.	This applies particularly for co-operations with different cultures, languages and times.
Compatible Workflows	The software of existing workflows should be able to interact (see chapter 4).	Human intermediation is often unnecessary, slow and error-prone. World wide standards for "Plug 'n Play" are desirable.
Defined Communication Flows	Because of the heterogeneity of the usage, one should be limited to few means of communication.	For the different requesters it is not evident whether the information was not read, the inquired had no time or he did not know the answer. [7]

Table 2.3: Requirements of virtual organizations

2.2.4 Dynamicity

Name	Description	Reason
VO Manager	A central manager, who structures the VO and reassigns competencies.	A hierarchical structure is assumed to be essential. A top and fully authorized instance is therefore necessary.
Trust Hierarchy	A hierarchical structure for trust relations.	The fact, that all organisations are bound into one VO does not necessarily mean that all involved organisations want the others to read all of their messages.
Standards	To make things of the same type all have the same basic features.	To enable all potential members to regroup to a VO without larger adaptation.

Ad Hoc	Generic recognizing and configuring of the participants.	Desirable in all cases, however it requires an enormous technical expenditure, which will only be worthwhile with very fast changing systems.
--------	--	---

Table 2.4: Requirements of Dynamicity

3 Summary of Authentication, Authorization, and Accounting Requirements

Authentication, authorization and accounting is used to a large extent with network services. Incoming connection calls, inquiries and other service requests are processed, answered, rejected and/or passed on - often many hundreds per second or more. For each request, the service provider has

- to recognize the customer (authentication),
- to decide, which services the customer may use (authorization) and
- to determine, to which extend the service was used (accounting, charging) .

or, otherwise expressed, the Service Provider (SP) has to answer the questions “who”, “what” and “how much”.

This chapter deals with AAA Requirements, necessary for the definition of the MDVO-AAA Model in chapter 6 on page 35.

Similarly as in the summarization of key requirements of Mobile Dynamic Virtual Organisations (see chapter 2 on page 11), a precise definition of the used terms is first given in order to prevent misunderstandings and ambiguities. Each subsequent usage of these terms relates to these definitions. The terms are ordered in a way to make an easy understanding possible, since some are dependent and have to be defined against each other.

Afterwards, requirements, considerations, and recommendations are given for authentication, authorization and accounting with respect to their initial definitions.

3.1 Terminology

In the following, relevant terms for the concept of AAA as well as for its extension, referred to as A4C, will be listed and explained. To this end, constituent parts for AAA and A4C are defined first, leading consecutively to a characterization of AAA and A4C itself. Besides textual description of these various terms, their inter-relationship is presented on one hand in 3.1 by means of a timeline-based visualization and on the other hand by a short example.

Authentication Demonstration of an identity.

A client provides some information (i.e. username and password or a certificate) in order to satisfactorily show it's identity.

Authentication Proof of an identity.

The server proofs the received data in order to verify the suggested identity. It is *not* an identification, since the server has no understanding of other identities or roles of the client or who the client is in detail (human or machine). *Nor* is it an access control, because the server has no knowledge about the permissions associated with that identity. However, some authentication systems may deal with access permissions.

Authorization After the authentication an authorization takes place, in which certain rights are granted to the client due to its verified identity. These rights consists of three parts: *who* may access *what* with what *operation*.

Accounting Describes the collection of data about resource consumption and behavior. This includes the control of data gathering (via metering), transport and storage of accounting data [8]. Accounting is needed for auditing.

Auditing Defines the process of retrieval of information and the events taking place in the system [9]. Auditing is needed for charging.

Metering Meters are needed for capturing data about resource consumption (accounting) in a network [8]. Metering is also needed for charging.

Charging derives non-monetary costs for accounting data sets based on service and customer specific tariff parameters [8].

Billing translates costs calculated by the charging into monetary units and generates a final bill for the customer [8]. Most literature use the term charging for billing and charging together.

AAA Enfolds Authentication, Authorization (building together the first 'A' in AAA), Authorizing and Accounting

A4C Enfolds AAA, Auditing and Charging.

Since the collection of data without making it available makes little sense, AAA is usually implemented together with auditing instance.

The separation between accounting and auditing is not always clearly possible. With two separated instances in a network, some of the functions and requirements listed here could also be assigned to the auditing system.

Figure 3.1 illustrates the interactions of the defined terms: The first 'A' of AAA determines, who gets authenticated and the second, who wants to access a specific resource. The access is granted, based on the user's service profile. During the resource usage, the resource's metering component registers the service consumption with respect to available parameters, such as usage time. Withing the accounting component, the metered data gets transfered into the accounting database. The auditing component reviews the accounted resource consumption for charging and security purposes. In charging,

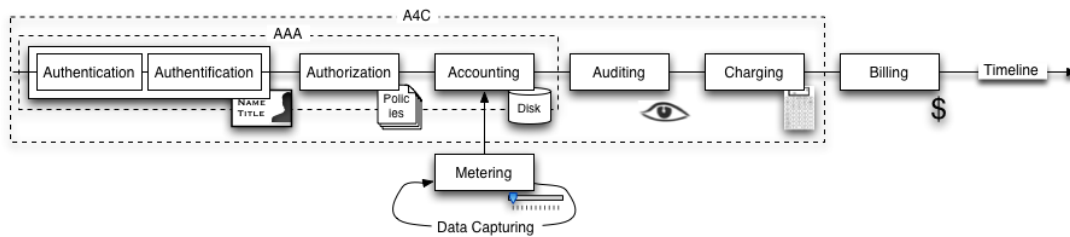


Figure 3.1: AAA and A4C with Accounting, Metering and Billing

the received accounting records are transformed into (non-monetary) charging records, by means of a charging function incorporating specific parameters. Within the billing component, the charging records are equipped with monetary values and a bill is send to the customer.

3.2 Authentication Requirements

Authentication has to take place in one of these four ways: Somebody *has* something (i.e. a key or a card). These items are called Secure tokens. Or somebody *knows* something (i.e. a pin or a password). The system is then knowledge based. Another way is if someone *is* somebody (i.e. biometric criteria) or at a certain location (i.e. a certain computer). The fourth way is if somebody *can* do something, i.e. signatures, called cryptography based. A combination of one of these techniques is usually implemented.

Four kinds of authentications at the identity itself are possible: local authentication (at each entity), direct authentication (someone shares something with an entity), off-line authentication (i.e. with public keys) or indirect authentication (a third entity makes the authentication and confirms it to the requested entity).

No matter which of these ways is chosen, it should be protected against all known attacks, such as:

- Replay attacks
- man-in-the-middle attack
- masquerading (someone prevents to be someone else)
- keystrokes sniffing
- network sniffing
- password sniffing

Further more, the authentication server has to be protected against brute-force or denial of service attacks. Since each technique may be broken in future, the way of authentication should be extendable to various algorithms. It is recommendable, not to reduce the system to a single authentication server, since that represents a vulnerable bottleneck.

3.3 Authorization Requirements

Authors S. Farrells et. al. have provided [10] an embracing list of authorization requirements.

Main aspects of the paper are:

- *Reject capability*: The authorization server must be able to reject authorization requests if the clients are not authorized.
- *Reauthorization on demand*: The authorization server must be able to reauthorize an entity (e.g. if a connection suddenly terminated and the users security token lost its validity).
- *User de-authorisation* [11]: It must be possible to revoke the rights of users and entities, for example if they are abusing the system or if they changed their service providers and are not customers anymore.
- *Support for access rules, restrictions & filters*: The authorization server needs to apply access rules and restrictions in order to have different policies for different users.

3.4 Accounting Requirements

The accounting requirements are divided into three parts: the requirements on the accounting system itself, the requirements due to the possible accounted data and some security considerations.

3.4.1 System Requirements

Accounting serves only one purpose: making information about the resource consumption of the involved entities available. For this reason this data must be collected and stored. Since this data represents a resource by its own, and due to in Section 2.2.1 on page 12 given recommendable features “Transparency of resources” and “Addressability of resources” it seems to be reasonable to place the accounting system as independent entity into the network which makes the inquiry service available against all authorized entities.

Inquiries to the auditing system should be possible at any time. Due to the last requirement, the Accounting system has store its data always consistently and the information should only be stored at one place. However, a distributed data base with several accounting entities is nevertheless possible.

There are two possibilities, how the Accounting System (AS) gets the necessary information about the resources consumption of the involved entities:

- It could monitor the network traffic and analyze the transferred data.

- Each monitored entity contains a metering and AS component, which announces the necessary data autonomous to the AS.

Since it is to be assumed that the involved entities use different data structures for package transmission and since the goal of accounting is to map the resource consumption to suitable metrics which may vary among the entities, the first mentioned possibility is not suitable with the dynamic aspect. Therefore, each monitored entity has to have an AS compatible component.

In each entity occurs very different kinds of data (and metrics). Some meta information for the description of the conveyed data is essential. Conceivable would be an entry into a global table of the AS on the registration of that entity.

Possibly, parts of the stored data will be mapped to a suitable metric (e.g. for the scheduling - users with small resources consumption are preferred to those with a high one, or for the Charging). The Accounting system should therefore store the units of the appropriate metric per entry, additionally. If the metric changes, the resources consumption can be queried in the auditing system with a metric that was valid at that time. This is of importance particularly for charging.

Since many metrics are session dependent, i.e. they only get applied on a successfully completed session, and the entities, however, constantly send new entries and the sessions are possibly extended over several entities, the accounting system should have stored the metric function.

A metric function could be implemented as mathematical linkage of the stored entries or as a black box function in a script language. In both cases meta information about the input values of the function must be present.

Many metrics are applied to (successfully) terminated sessions and these may contain several entities, the system therefore has to assign and store global Identifications (IDs)

3.4.2 Data Requirements

The different kinds of possible accounted data constitute some requirements to the accounting system, since it has to support the correct storage and retrieval of these data and to create links between correlated information.

A substantial, but possibly not complete list is given as followed:

- Accounting information related to session progression

There must be support for accounting transfers where the information contained in the accounting data has direct bearing on the establishment, progression and termination of a session [11].

For crucial services (e.g. in banking), the accounting system must keep track of each single step during the session. This may also be important for security reasons.

- Accounting information not related to session progression

There also must be support for accounting transfers where the information contained in the accounting data has direct bearing on the establishment, progression and termination of a session [11].

This compasses all other data which is not related to the session progression, but may be related to the session itself (e.g. the session duration).

- Stateful and stateless accounting [11].

The behavior (and therefore the charging) of some services may depend on the user state or some internal parameters (e.g. the system load). A distinction between these two kinds of accounted service data is therefore required.

- Support of arbitrary correlated IDs

Some networks need to be able to relate the accounting to some aspect of the session [11].

- Real-time Accounting.

Real-time accounting involves the processing of information on resource usage within a defined time slot.

Time constraints are typically imposed in order to limit financial risk [12]. There are also requirements to provide real-time monitoring of port and user status, so that the state information can be used to implement policy decisions, monitor user trends, and the ability to possibly terminate access for administrative reasons [13].

- Batch accounting / non-realtime Accounting

Session activity information is stored and processed by a long term batch process to produce accounting usage records [13].

- Accounting Record Extensibility

The accounting record has to be extensible for data, occurring and needed in the future.

- Dynamic Accounting

Some services may require dynamic allocation of resources. Information about the resources required may not be known during the authentication phase, it may come up later. (e.g. IP Addresses for multi-link bundles) It is also possible that the authorization will change over the time of the session [13].

3.4.3 Security Considerations

The AS is a weak point for company's privacy. All important data within the system is carefully collected and accurately stored within the system. The success of the company depends on the analysis of these data. Therefore it has also an inestimably value for unauthorized persons (or companies).

Security is one of the most important aspects of the AS and creates of the most challenging requirements. The system must provide sufficient and robust authentication techniques as required by network policies. It has to hide the authentication information from network snooping to protect from attacks and provide user privacy, As mentioned above, protecting message integrity exchanges from attacks such as replay or man-in-the middle is also an issue. Furthermore, hosts have to be unable to interfere with services authorized to an AS, or gain unauthorized services and they have to be unable to probe or guess at authentication information. The AS system has also to be protected from being configured or administrated from unauthorized users. And, finally, the network must be protected from illegal packets sourced by accessing connections [13].

4 Determination of Electronic Workflows

A workflow is a set of detailed described worksteps. These steps determine, who performs which task, how they are structured, what their relative order is, how they are synchronized and how their dependencies are.

Workflows are to be found in each company and form the basic unit for each value-adding process. A detailed understanding of all the possible workflows that may occur within a company is therefore a precondition for a meaningful MDVO-AAA model (see chapter 6 on page 35).

However, terminology in that area is not only incoherent within the literature, in some cases, terms are even defined with an opposite meaning to the definition of another paper. A detailed description of each used term in connection with workflows is therefore necessary in order to constitute the respective notion as it is used throughout this thesis.

The chapter is structured as hitherto: after introducing the new terminology, the actual determination of possible workflows follows.

4.1 Terminology

Subsequently, a collection of relevant terms for workflows, partly listed according to referenced sources concerning this matter, partly self-defined where necessary, as in these cases either no suitable definition was found or inconsistent information prevailed.

Task A task is a unit of work, which is implemented by an entity, but which has no value to the customer as individual performance [14]. It has clearly defined input and output values as visualized in figure 4.1.

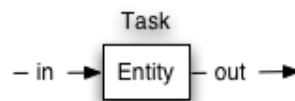


Figure 4.1: Task

Service A service is a completely automated task which is exclusively executed by electronic entities.

Service Level Agreement The conditions, to which a service can be used. The service is characterized by these. The service level agreement covers among other things: legal conditions, duration, costs, quality (i.e. accuracy), availability, accessibility (e.g. bandwidth).

Critical Conditions Conditions, to which no entities with correspondent service level agreements exist.

Critical conditions represent the restrictions of the user, how he or she wants to use the service. It is the task of the system to adapt the workflow in such a way that it approaches to the critical conditions as well as possible.

Workflow Special arrangement of tasks, which creates an output to customers. Usually contained out of several tasks as shown in figure 4.2.

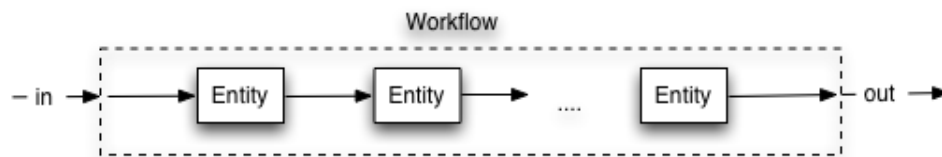


Figure 4.2: Workflow

Example: Consider a monthly expense report. This document, whether on paper or electronic, is completed once by an employee, forwarded to someone with signing authority, passed to someone who can enter its details in a ledger, then passed to someone who can issue payment before being passed to the bank or tax authorities.

Adaptive Workflow The Workflow possesses several choices of resources and adapts the involved entities and activities on basis of the service level agreements to the critical conditions as best as possible. An adaptive workflow consists of a “workflow template” and of a “execution engine”.

Workflow Template Consists of an exact definition of a workflow (including inputs and output) and a list of resources with their intermediary results and service level agreements:

$$\langle E_n, I_x, O_y, T_n, P_n, Q_n \rangle$$

E_n represents the entity with input I_x , output O_y and the characteristics time T_n , price P_n and quality Q_n .

Example: a workflow template with the content:

$$\langle E_1, I, O_a, 3, 5, 2 \rangle$$

$$\langle E_2, I_a, O, 2, 3, 4 \rangle$$

$$\langle E_3, I, O, 8, 1, 1 \rangle$$

Could generate a workflow from the entities E_1 , E_2 , which delivers the result within 5 time steps, but costs 8 monetary units. Or it could generate a workflow from the entity E_3 , which produces the result in 8 time steps but costs only 1 monetary unit.

Execution Engine If a Workflow is to be implemented, the execution engine then applies the workflow template to current parameters and creates the most optimal Workflow. This can either happen in choosing the most suitable resources or in distributing the work on several available resources.

Business Process Concatenation of value-adding activities, which produce a single output for the customer. Contains several interlinked and dependent workflows, which is implemented for a parallel or alternative execution.

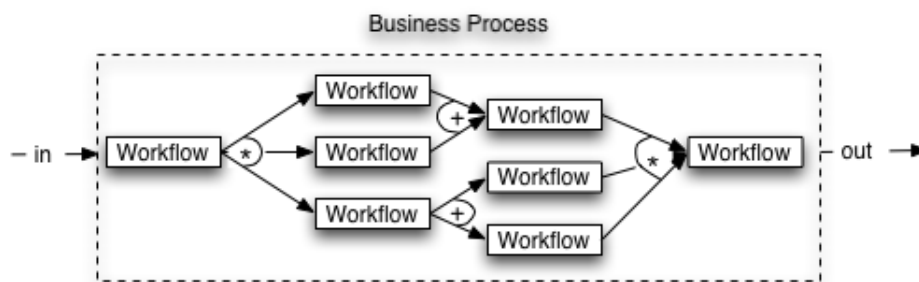


Figure 4.3: Business Process

The linkage of the Workflows can be categorized as depicted in figure 4.3: An *and-split* linkage enables all outgoing transitions after the execution is terminated. It is represented by a *. An *xor-split* linkage enables one single outgoing transition after the execution is terminated. Its representage is a +.

Tasks with more than one incoming transitions can be classified as follows: *and-join* transitions start the execution of the task if all incoming transitions are executed (*). *xor-join* transitions start the execution of the task on an arbitrary incoming transition (+).

For example that an insurance company and a driver whose car has broken down or suffered an accident, and the relationship between that driver and that company. As soon as the driver manages to get to a phone, multiple alternatives must be explored and multiple procedures launched. The following choices can be cited: the call center for the insurance company must determine if this driver is a customer, check the current status and privileges of this driver's policy, locate appropriate "partner" firms in the vicinity. These tasks would be necessary as the might be causal by the following reasons: taxis may need to be called, hotel rooms may need to be booked, substitute cars may need to be rented, garages may need

to dispatch tow trucks and finally, the company must locate, contact, and send in the appropriate claims adjuster for the region.

The aforesaid has to be conducted even before being able to determine the current state of the vehicle, or obtain a repairs estimate, or alert the appropriate police jurisdiction, ...

Thus, large number of workflows must be selected, initiated, and tracked, options must be presented at the appropriate time and resources must be called in when required.

4.2 Categories of Workflows

There are several possibilities for categorizing the different kinds of workflows by means of suitable attributes. Each of these attributes may or may not be passed by a workflow. Possessing *and* not possessing an attribute represents a characteristic. A particular workflow can own any combination of the above listed characteristics.

Since a business process only consists out of workflows, the characteristics can be applied to business processes as well. Since each characteristic consists of two mutually excluding attributes, a business process may consist out of workflows with both different attributes. One attribute is therefore stronger than another one and determines the characteristic of the entire business process.

4.2.1 Ad hoc vs Production

An *ad hoc* (or collaborative) workflow is defined for each use. There are four steps for doing any piece of work: Negotiation, Acceptance, Assignment (delegation the work to reviewers) and Review

A *production* workflow is pre-defined and prioritized, and this supports high volumes - there are no negotiations about who will do the work and how it will be handled. However, there may be additional tasks or workflows defined and added to the overall process.

A cross between ad-hoc and production is the *administrative* workflow. The flow is pre-defined and sometimes the flow can be reviewed or even altered (by adding event callbacks). [15]

4.2.2 Horizontal vs Vertical

A *horizontal* workflow moves the work through the organization. It is the most common workflow. A *vertical* workflow goes over the company boundaries. This may occur, when the workflow itself uses services from different companies.

4.2.3 Stateful vs Stateless

A *stateful* workflow changes as in dependence on different system internal state variables or service outputs. A *stateless* workflow is always the same.

4.2.4 Realtime vs Batch

Within a *realtime* workflow, the duration and response time of the workflow is fixed. The output is worthless if it cannot be kept. With a *batch* workflow, the result is not needed for a certain time. Usually, however, a time out value is defined to prevent endless waiting.

4.2.5 Session Related vs Not Session Related

A *session related* workflow is connected with a session, to which the result can be sent directly (but it does not depend on it - this would be otherwise a stateful workflow). If the session terminates, the workflow terminates as well (e.g. real-time stock exchange courses. If the session does not exist anymore, the courses should better be read from the data base).

If the workflow is *not session related*, it is not dependent on a session.

4.2.6 Buffered vs Callback

With *buffered* workflows, the result is stored on the callee entity until the caller fetches it.

This is useful, if e.g. the availability of the callers or the workflows is not always guaranteed, for example with mobile nodes, which are occasionally in tunnels or other places out of reach.

With *callback* workflows, the result is sent to the Callee.

5 Definition of Value Metrics Applicable to Workflows

Metrics or “measures” are a tool for controlling, charging and assessing the impact of a particular workflow. The management of metrics directly impacts the success of organizations participating in e-commerce. Using metrics allows:

- Analyzing and estimating of workflows
- Monitoring and triggering of workflows
- Controlling of Workflows and Services
- Success to be assessed
- Pricing and charging of services
- Return on Investment (ROI) to be estimated
- Targets to be set in terms of goals and scope of services

This chapter contains first a list of technical metrics for workflows. These metrics are useful and necessary for analyzing the system from a technical point of view: whether it is working to full capacity, whether new equipment is or will be necessary or if contracts and promises are satisfiable.

Afterwards, a section with business metrics follows. Business metrics, such as product (in sense of service) sales and costs are essential for analyzing the current market position and future trends.

Usually, the technical cost parameters are mapped to internal cost categories, which are reduced to some simple categories for the customer. This chapter finally describes the list of currently used pricing categories without giving a cost analysis of possible and feasible mappings.

5.1 Technical Metrics

There are three categories of technical metrics: timing metrics, reliability metrics and usage metrics. Timing metrics give some impression about the system response time and flexibility. Reliability is important for the service quality and usage metrics for the system configuration.

5.1.1 Timing Characteristics

The Workflow Response Time (T) is set as the total amount of time that a workflow instance spends within a workflow process before it finishes. The response time in a workflow is equal to the sum of the response times at the individual tasks, less any time that two or more tasks are superimposed on one another. Two or more tasks superimpose their response time when they are executed in parallel.

The *Minimum Workflow Response Time* (min T), sometimes referred to as the “service time” of a workflow, is the time required for a workflow instance to be processed, not accounting for any task delay time. Thus, it includes only the task response time, ignoring completely the impact of the task delay time. The minimum workflow response time is equal to the sum of the process time at the individual tasks, less any time that two or more tasks superimpose.

The *Workflow Response Time Efficiency* (E) is the ratio of the minimum workflow (w) response time and the workflow response time. It is instructive to compare these two measures, since instance efficiency measurement provides an indication of the time an instance is delayed during its execution and also indicates the degree a workflow process can be improved by reducing its response time.

$$E(w) = \frac{\min T(w)}{T(w)}$$

The *Setup Time* is the time, used to establish and publish a particular workflow

The *Task (t) Response Time*, expressed as $T(t)$, corresponds to the time an instance takes to be processed by a task. It can be broken down into two major components:

The *Delay time* (DT) refers to the non-value-added time needed in order for an instance to be processed by the task. This includes, for example, the instance queuing delay and the setup time for the task.

The *Process time* (PT) is the time a workflow instances takes a task while being processed.

$$T(t) = DT(t) + PT(t)$$

Besides taking these timings for their own, they can also be set in relation to each other. For example $\frac{\text{Elapsed time}}{\text{Effort time}}$ gives some conclusion about the system response time [16].

5.1.2 Reliability

System failures are IT and software failures which lead to a workflow terminating abnormally. IT and software include operating systems, communication protocols, hardware, etc.

The *System failure rate* is $\frac{\text{\#unsuccessful execution}}{\text{\#called executions}}$

Process failures are process exceptions which lead to an anomalous termination of the task (i.e. no authorization).

The *Process failure rate* is $\frac{\text{\#the service succeeded}}{\text{\#the service failed}}$

5.1.3 Usage Metrics

An important usage metric are the *number of requests sent*, the *number of users*, and a respective ratio $\frac{\text{Requests sent}}{\text{Number of users}}$. This gives some impression about the kind of customers, the company has: a small number of users with a high value of requests leads to a high ratio and will probably make the company to adjust their services to the customers. A high number of users with a small number of requests, however, will make the company to rethink their product offerings. Unsatisfied customers, who do not use the service for a second time may be a reason.

There are several kinds of system loads with multiple ratios: the transaction volume, the memory usage and the cpu usage. Each of them has to be set in relation to a time window to analyze peak times and should also be analyzed in total and per process, service and workflow (and maybe business process). Peak times may lead to costs charged on basis of the time of usage in order to induce some customers to request the services during times of less utilization. A reconsideration of possible low prioritized batch processes to be moved to these times with low load may also be a possible way. If a single service causes enormous load, the cost of the service has to be increased in order to map the system usage to the service costs. If the resource consumption of the service interferes with other services in a way that the company is not able to fulfill their service level agreements, the service might will not be available for all the time. If there is no anomaly in the resource consumption and each service uses the same amount (within some range), but the company has the load at the system's capacity, it needs to upgrade the system.

A last metric is the number of used processes (and therefore resources) per service, which could also be a possible cost parameter, which absolutely makes sense to the company, but is hardly traceable to the customer [17].

5.2 Business Metrics

Workflow cost (C) is the cost incurred when a workflow t is executed; it can be broken down into two major components: *Enactment cost* (EC) is the cost as associated with the management of the workflow system and with monitoring of workflow instances. *Realization cost* (RC) is the cost associated with the runtime execution of the workflow. This again can be broken into following cost elements: *Direct labor cost*, the cost associated with the person carrying out the execution of a workflow human task. *Machine cost*, the cost associated with the execution of an workflow *Direct material cost*, the cost of the materials, resources, and inventory used during the execution of a workflow task. And finally, *setup cost* is the cost to set up any resource used prior to the execution of a workflow task.

$$C(t) = EC(t) + RC(t)$$

In addition, *product sales* are also a metric of interest, having a direct impact on the revenue.

There are several kinds of *event metrics*. These include cases, when a the customer browses through service descriptions (e.g. on a web site, or sends queries to a service description service), a customer places an order, a authority responds to a credit check request, a customer makes a payment, a customer reviews an order, a customer cancels an order, a customer changes an order, a VO manager updates Available to Promise (ATP): if it is possible to see how much resources are not committed to customer orders and are therefore available for service promising, the VO Manager updates the delivery date, the delivery provides advice of receipt, the delivery provides a proof of delivery and it is time to invoice customer. Each of these value metrics need to be collected and counted and give a hint about the current system state, behavior and usage.

The product quality can be determined by the number of *support requests*, *user rankings* or general feedback and *usability testing* (such as precision of computations or locations or usability of query results). Another indicator are the *number of edits* or reviews required for each piece of result. the *information currency* is also an important quality metric: for information retrieval, it is important to know how up to date the information stored and retrieved by the service is. Finally, the *customer satisfaction* should be continuously be seized with surveys, follow-up telephone calls and focus groups [17].

5.3 Pricing Based On Value Metrics

The costs of a single IP stream for the usage of a service can hardly be determined. If the services are completely automated, only fixed costs result to a large extent. A service provider's goal is rather to appropriately distribute the resulting costs on the maximally possible users.

Typically used parameters are:

- Flat Rate
- Time based
- Volume based
- Type based
- Location of destination
- Advertising
- Service and content usage

A goal of pricing is the simple comprehensibility for the user and thus using as few parameters as possible.

The following models are among other things conceivable:

Flat Pricing A fix amount per time and unit (e.g. a month) [18, 19]

Paris Metro Pricing The user chooses a Network/Category of available services [20].

Priority Pricing The user chooses the priority for the packet processing [21, 22, 23].

Expected Capacity The user chooses the response time minimal available [24].

Edge Pricing The price is determined on congestion and route (e.g. for video streams) [25].

Responsive Pricing The price for a service changes continuously depending upon supply and demand [26].

Cumulus Pricing Scheme After the usage a certain amount of a value metric for a specific price is negotiated, the system gets periodically scanned and the actual usage is recorded. Over- and under-usage get accounted against each other and a trigger is set for the case of long-term over-usage [27].

6 Definition of an MDVO-AAA Model

A MDVO consists out of three layers, shown in figure 6.1.

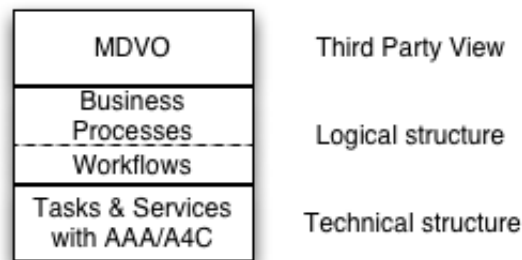


Figure 6.1: MDVO-AAA Model

The first layer represents the VO in the customer's view. The customer (either a person or another company) usually only gets in contact with a single company and it is not comprehensible for him, how many other companies are involved and commissioned by the company.

The second layer consists out of the company-internal logical and functional sequences for offering a product in form of services, i.e. workflows and business processes. The whole business of the company (and maybe even the employee hierarchy) is based on these structures.

The third layer contains the technical implementation and automation of the second layer and should encapsulate all technical details. The second layer should be completely independent of the third layer, since software, hardware and technical standards are changing and should not effect the company's business.

This chapter is structured in a way, that all layers are described consecutively in a section.

6.1 Third Party View

A user of a business process always uses the third party view, no matter whether it is an internal user or a customer, since a customer should deal not with the internal structures. These should be totally enclosed behind third the party view. An internal user should access the same structures as an external customer, since they are already present and the access becomes standardized and simplified.

Within the third party view, the company has to be addressed through one or more unambiguous resource locators (such as telephone numbers for mobile phones, ip/-domain name/url and port for web services) - otherwise confusion prevails. A single resource locator would simplify the connections.

A unified business process, present in all companies, is possible, providing (in dependence of the used resource locators) all available the business processes with their conditions (service level agreements).

6.2 Business Processes and Workflows

A virtual organization manager is bound to the resource location. It takes the requests and passes them to the available business processes or rejects them. The VO manager prevents having the address of each business process hard coded in customer calls and enables an easy way of adding and removing new services. A single VO manager simplifies the organizational structure to a central instance for a uniform handling of incoming calls.

Figure 6.2 on the following page shows a schematic view of a business process model. In dependence of the different possible business processes, initializations (such as real time/batch or session related of chapter 4) may be made. A distribution on several different internal VO managers is conceivable.

Since a central place is of benefit for administration of resource locations and business processes, the companies involved do not exist equally in parallel in most cases. A core organization is needed, which administers the critical sections. In this scenario, customer gets in contact exclusively with this company, for which it is usually called "service provider" (SP). A better suitable term would be "Business Process Provider", however, literature rarely distinguishes services, workflows and business processes.

A Workflow is a constant sequence of services. A business process contains a set of possible Workflows, which can be implemented in parallel and dependently from each other (see the respective definition in chapter 4.1 on page 27 or figure 4.3 on page 27).

The business process entity selects the combination of workflows most suitable for the customer (dependent on costs and time) and the system (dependent on utilization and efficiency) and administers its execution. Therefore, a request is sent to the workflow execution engine, which instantiates new processes due to in the stored workflows in the workflow database and links their executions.

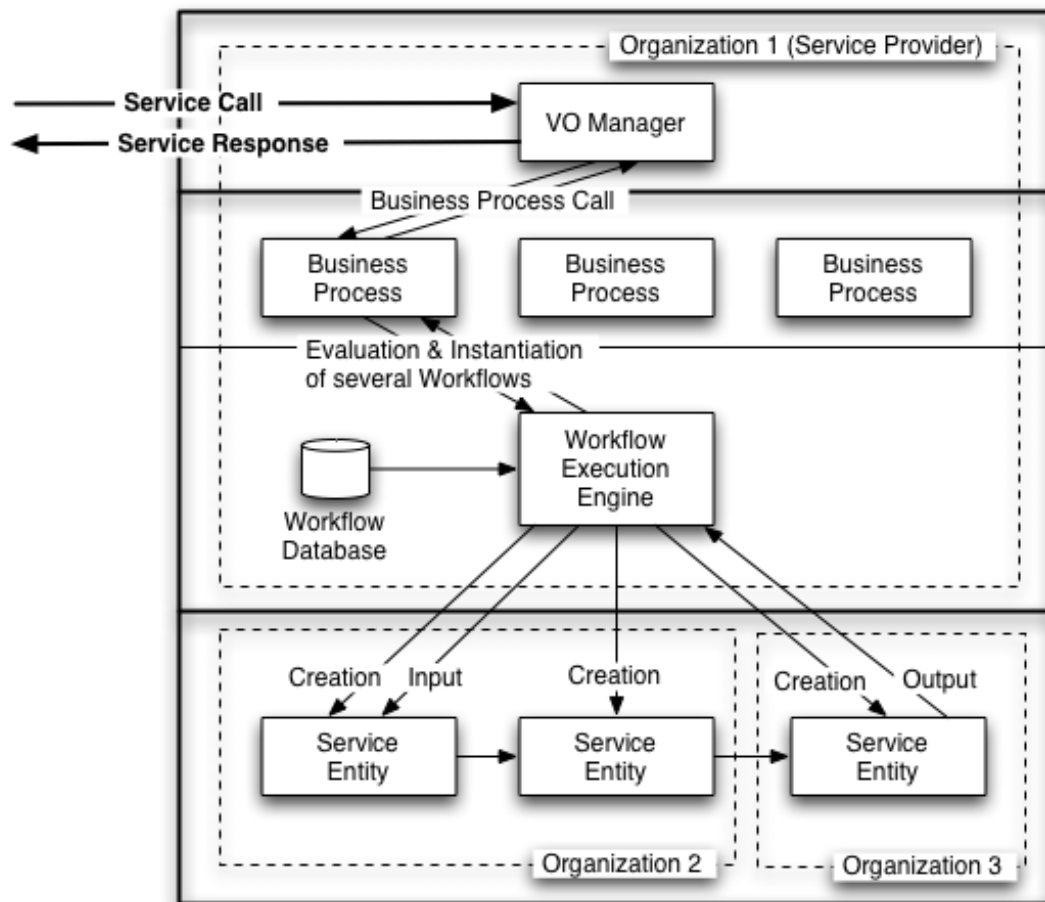


Figure 6.2: Business Processes Model

6.3 Tasks and Services with AAA/A4C

The lowest level in the MDVO-AAA model presented in figure 6.1 represents interaction of involved entities on the technical side with respect to AAA and A4C.

It can be divided into four subcategories.

1. Authentication and Authorization
2. Accounting
3. Auditing
4. Charging and Billing

All four subcategories are assumed to be within the core organization.

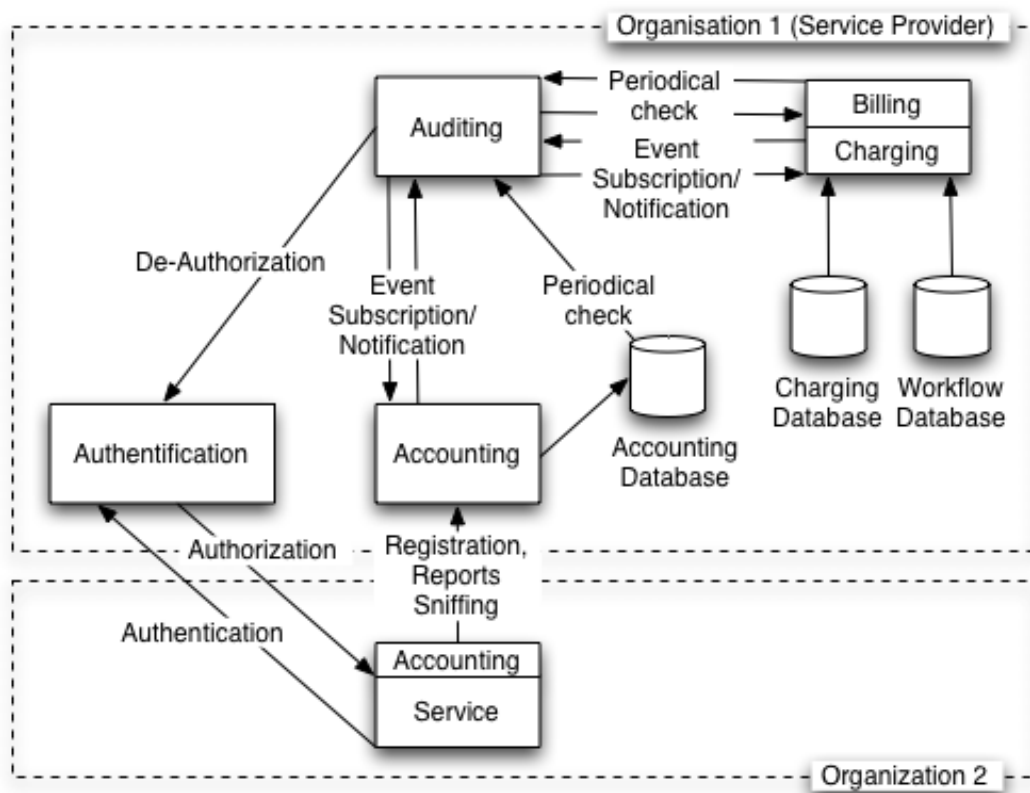


Figure 6.3: A4C Model

Figure 6.3 demonstrates how interaction of entities at the lower level works. A service has to authenticate itself to the authentication entity. It has also an accounting component, which delivers data to the accounting entity. Another configuration however might only consider charging records to be transmitted across administrative borders of involved entities. The accounting entity is monitored by the auditing entity, which has the ability to de-authorize the service entity if it behaves in an impermissible way. The billing entity gets the necessary data from the accounting entity and converts it to a monetary unit on basis of the charging and the workflow database. A detailed description of each part is given below.

It is possible, that each involved organization makes some or all available the A4C instances available to the other involved organizations and thus acts as an equal domain. Such an approach would not only reduce dependencies from one service provider, but would also provide for more security (e.g. against bottleneck attacks). However, the technical complexity per company and thus the costs per service would also rise.

In addition, a central “billing entity” would have to be established, in order to let the customer receive one single bill from the VO.

6.3.1 Authentication and Authorization

This is a classical challenge-response protocol, for which a nonce should be used and a session key should be generated. It is to be used for all involved entities, including the auditing, accounting and billing server.

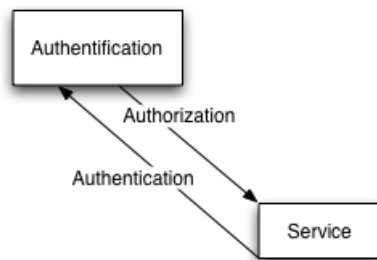


Figure 6.4: Authentication & Authorization Model

Figure 6.4 illustrates the part of the AAA/ A4C layer, that implements authentication and authorization. An entity sends the authentication, whereupon a server does the authentication and returns - in case of an affirmative result - the authorization.

6.3.2 Accounting

A separation into a part, that stores the needed information for the billing and one, that stores it for auditing is conceivable. However, since each entity requires a component which sends the information to the server, this model handles accounting without this distinction in order to simplify the implementation.

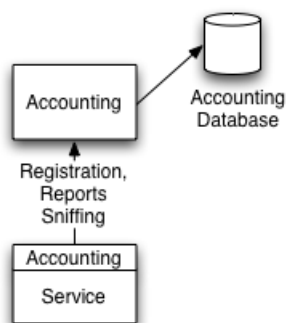


Figure 6.5: Accounting Model

Figure 6.5 on the previous page shows the part of the AAA layer, that deals with accounting.

6.3.3 Auditing

The auditing component is responsible for the correct behavior of all components within the system. It can register itself with the accounting server for alarm trigger and gets informed, when they fire. In addition it can make regular checks over the registered components within the system to examine their correct behavior.

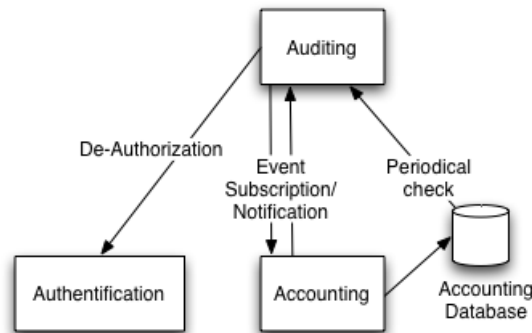


Figure 6.6: Auditing Model

Figure 6.6 illustrates the auditing component of this layer. The auditing entity accesses the accounting database for auditing and may initiate a de-authorization if the monitored service acts suspicious.

6.3.4 Charging and Billing

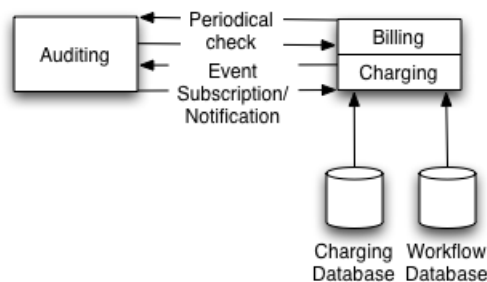


Figure 6.7: Charging / Billing Model

Billing gets periodically executed. Depending upon organizational politics for the computation of the price, different parameters are used (see chapter ?? on page ??).

Accounted information is transferred into charging data. In the charging database, conversions of the metrics to now monetary units and the required adjacent organization from entities are stored. The latter is necessary for splitting the charged price upon the involved organizations.

For the calculation of the selling price, it can be necessary that the context (business process and workflow) of the used entities has to be registered within the accounting system. Billing itself can also be regarded as a periodically running workflow.

Figure 6.7 on the preceding page describes the charging component: the billing entity uses the auditing entity for information retrieval and the charging and workflow database for generating the bills. This consists of two steps: First, charging records are calculated by means of charging functions whereupon to be billed amounts (expressed in a specific currency) are derived during the billing process. The auditing entity makes the data from the accounting component available.

7 Application of an example scenario to this model

Having determined characteristics of past work and having derived from gained insight into respective areas, an MDVO-AAA model in chapter 6 on page 35 is now applied to an example scenario in the field of logistics and fleet management. As a first step, the scenario is sketched in section 7.1. It is then analyzed from different viewpoints. This embraces considerations according to the developed MDVO-AAA model in the areas of a third party angle, an assessment of example business processes and workflows, and finally with respect to AAA and A4C.

7.1 Introduction to the example scenario

Let us assume, there is a company which runs a logistic center. The center consists of a storehouse, where the respective goods are mounted, and of a fleet of trucks which makes daily deliveries of these goods to the customers.

Whenever there is a customer who likes to order goods, he can - if he is already registered by that company - authenticate himself through the web (by means of a username and a password or a public key) and enter his order. An automatic connection to his business processes is also an option. The logistic center's system will check the assets of the goods of that order and if stock decreases under a certain minimum (i.e. less than the amount of average orders of a month). If so, the system will make a new order to the producer automatically. The customer order will then be stored in a database if it is possible.

During night, a batch process distributes the goods to the trucks and determines a route for each truck with respect to customer location and desired delivering times. The width of the favored delivering window could be an additional cost parameter, since the truck has to differ from the optimal route and other customers will get their goods delayed. Furthermore, gasoline stations together with their prices could be taken in account for planning optimal routes. The system also contains additional data about required services on the trucks and plans some intermission days for each truck. Beside that, the company has concluded a contract with a service provider for digital maps, so the route planning system can make some queries for distances between customers, optimal routes and blocked or jammed streets. Automatic consideration of toll fees (depending on the country) and a weather service to include possible delays could be also thinkable.

In case a new customer wishes to register, the service center has contracts with three additional service providers, so that it can check the validity of the address, the creditworthiness and the public key of the customer.

Since the company wants to focus on its core capabilities, it does not have service cars

itself. The company has contracts with a commercial repair service provider (similar to ¹TCS). They offer a product, which allows to locate the customer vehicles and the repair cars. Technically, that could be realized by using Global Positioning System or Galileo or by creating a Java application which uses a locating service run by the mobile net provider. A truck driver could send a signal in case of an accident or a break down and the company would coordinate their service cars and send them to the scene of accident. Contingently, all required additional steps are started for keeping the service center up-to-date and estimating the period of the breakdown, in calling the ambulance, the police or a taxi and a wrecking service.

7.2 Third Party View

Figure 7.1 outlines the overall organisation from a third party viewpoint.

Since the logistic center has a lot of connections to service providers, only the logistic center, the repair service and the customers are sketched, for the sake of clarity. The schema could be extended for any number of other service providers.

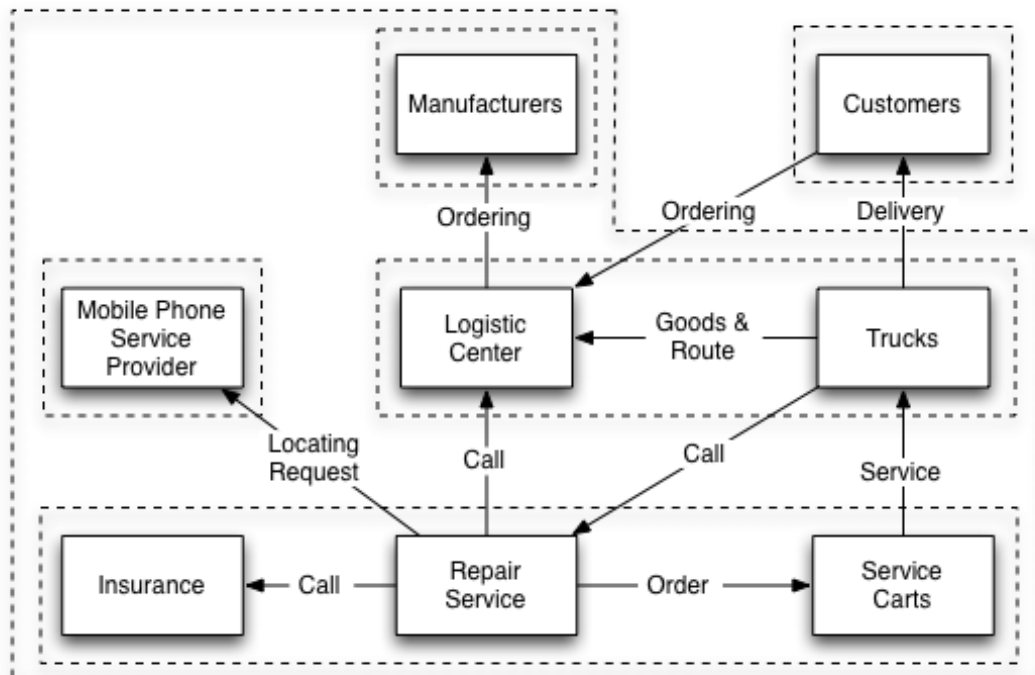


Figure 7.1: Third Party Example

¹Touring Club Switzerland, among others a mobile repair service for cars who suffered a break down en route

Customers place their orders to the logistic center, which itself generates orders to the producers. The trucks load the route plan and the goods at the logistic center and deliver them to the customers. In case of an emergency, they make a call to the repair service.

The repair service informs the logistic center and the assurance and coordinates its service cars which provide help to the trucks.

7.3 Example Business Processes / Workflows

There are only three typical business processes in this example. However, as mentioned above, there are a lot more within this scenario. A complete list would go beyond the scope of this thesis, but they can be created easily in the same way as the three sketched processes.

7.3.1 Registration

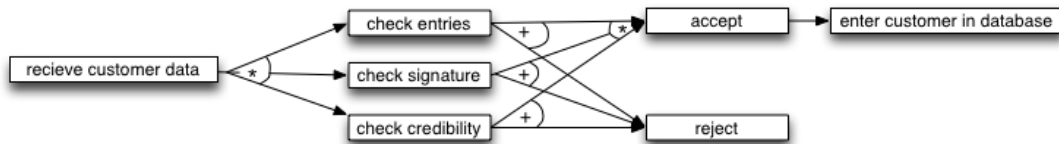


Figure 7.2: Workflow Example 1

If a customer wants to register, he first transmits the required data to a workflow as visualized in figure 7.2. Afterward the customer data, the electronic signature and the credibility are checked in three parallel workflows. If all workflows get an affirmative result, the business process accepts and enters the data in the database. If one workflow is negative, the customer is rejected.

7.3.2 Ordering

Figure 7.3 on the next page shows the outline of an ordering process. On receiving an order, the system checks if it is valid based on simple criteria. If this is the case, the stock and the feasibility of the order is evaluated. The order gets stored for further processing (e.g. route planning, billing) in an affirmative case.

Simultaneously, it is possible that the stock drops under a minimum and a new order has to be made for filling up the pile. If that is not possible, the range of goods has to be adjusted.

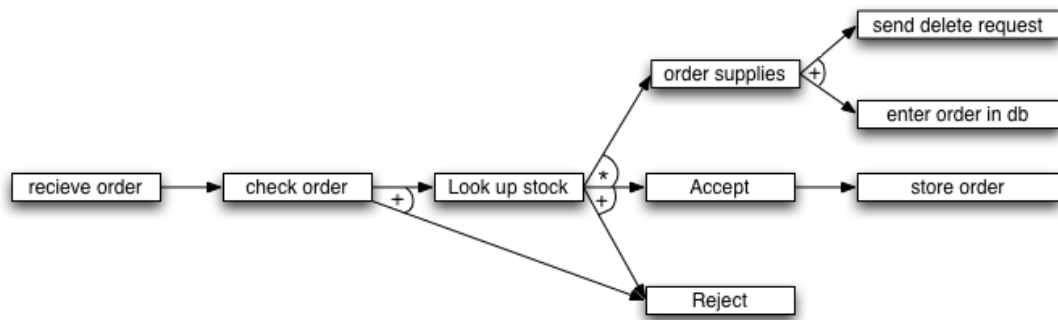


Figure 7.3: Workflow Example 2

7.3.3 Repair Service

On receiving a notification signal, as it is depicted in figure 7.4 on the following page, the repair service tries to locate and identify the truck, and to locate the repair cars nearby the truck (this could be done simultaneously). When the truck and the repair cars are located, one repair car gets chosen and a route to the truck transmitted. As soon as the repair service receives the status report of the repair car, it can choose further steps and either just inform the logistic center, or send an additional car with special repair supply, or order a taxi and a wrecking service. In the worst case, it has to inform the police and the ambulance, if not already happened.

7.4 AAA/A4C

For the sake of simplicity, only the interaction of two companies, the logistic center and one service provider for checking the credibility, are demonstrated and visualized in figure 7.5 on page 47. However, analyzing schemes hold for further companies, too.

The logistic center and the service provider have authentication, auditing, accounting and billing entities as described above. Each entity (including the billing entity or the ones participating in a workflow) have to authenticate at the authentication entity and to get authorized.

The authentication entity itself contains information about the possible services of the collaborating companies and has to authenticate at the authentication entity in order to issue authorization to the entities of their own company to allow a vertical direct communication.

If an entity wants to use a service of an entity not belonging to the company (meaning the same domain), it fetches an authorization from its own authentication entity.

This way, only qualified entities are able to use the services of the other company.

It would also be possible to link the billing entities for direct invoicing, so that the running costs can be processed immediately.

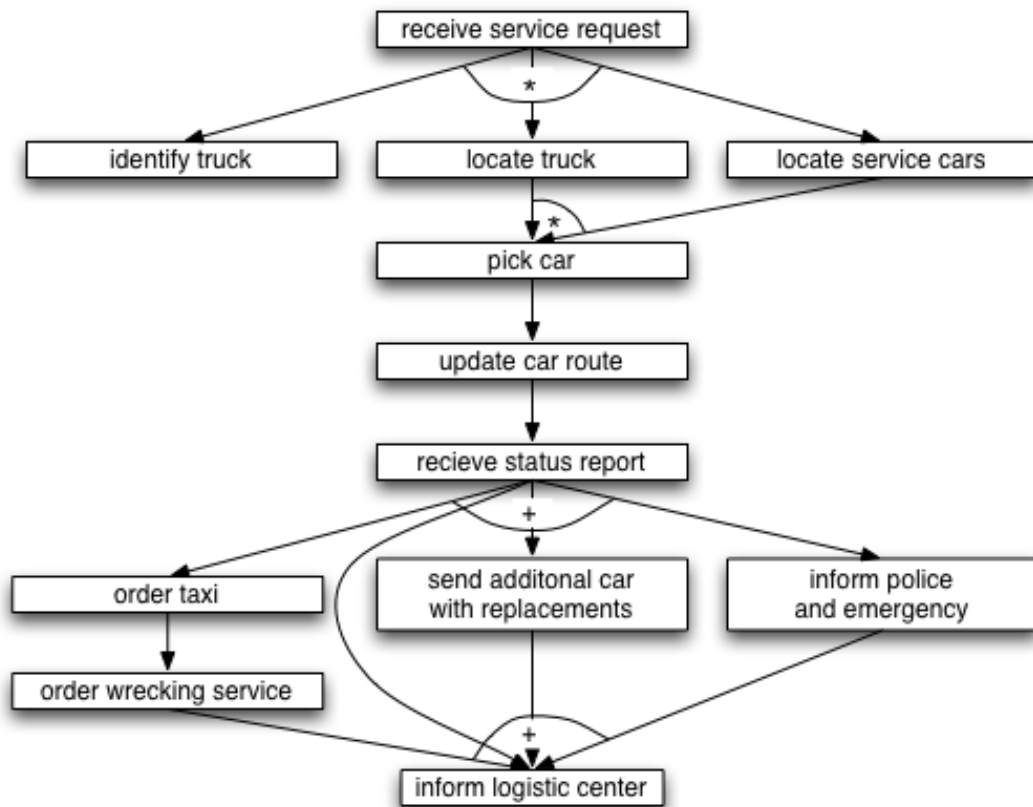


Figure 7.4: Workflow Example 3

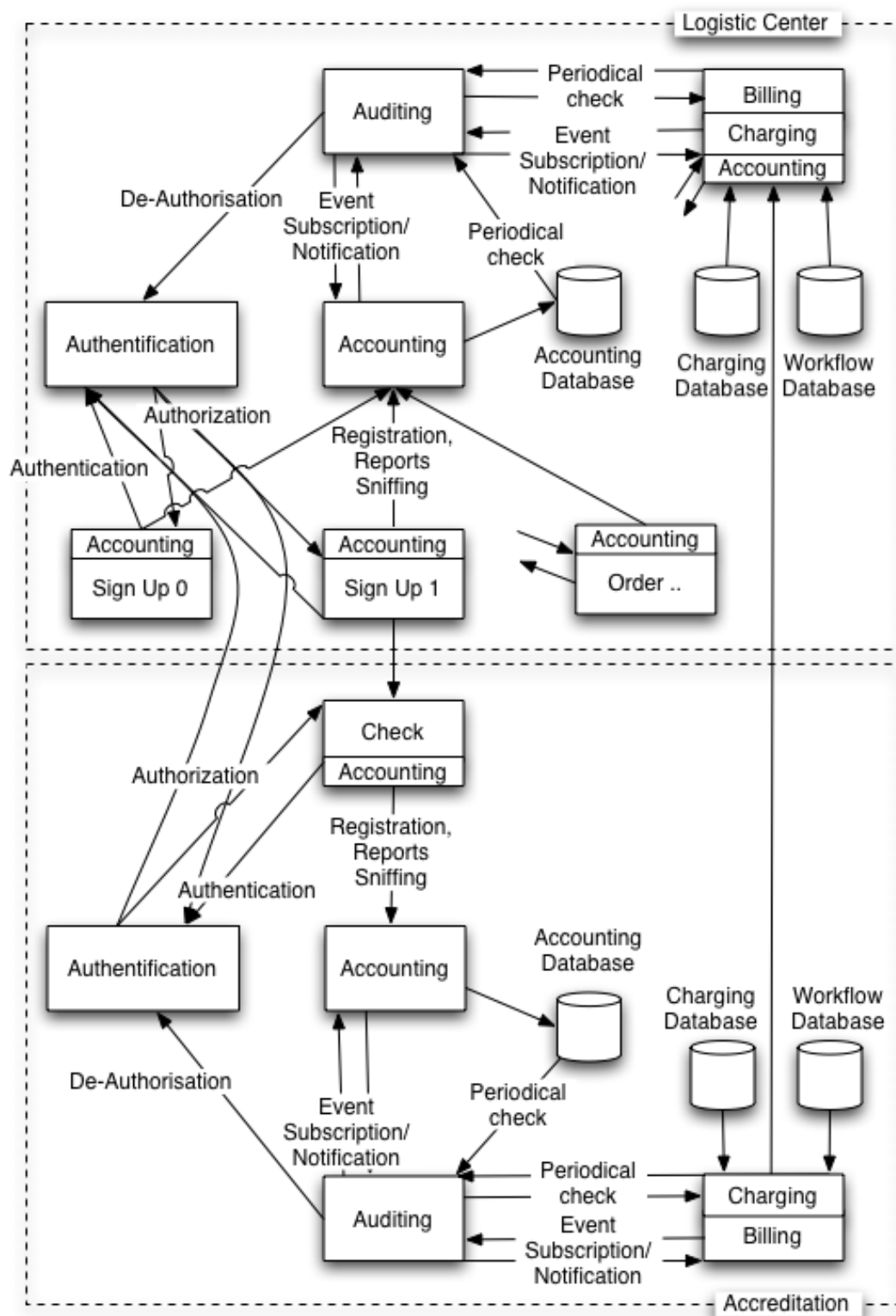


Figure 7.5: AAA Example

8 Evaluation

Within this chapter, an evaluation of the advantages and disadvantages of MDVOs with AAA-supported workflows is given in general and for the described model in specific. Finally, the provided example is examined with reference to the determined workflows and value metrics.

8.1 Advantages of MDVO with AAA-supported Workflows

AAA-supported MDVOs show key advantages in increasing workflow efficiency, reducing costs, and focusing on organization's core competencies. In the following, these aspects are further explained.

- Efficient and light structures by automated workflows: The automated workflow permits an optimal calculation of the needed parameters and thus one better utilization, lower production costs and better prognoses.
- Increase of the use for customers by fast processing and cost reduction: The automated processing permits a direct binding of the customer's company's production process to the service provider. Thus it does not play a difference whether the service is outside or within the company. For the physical exchange of goods an optimal supply is calculated, so that the participants of the MDVO have a competition advantage in relation to classical Business to business (B2B) company structures.
- Transfer of sections, that do not belong to the core capabilities and anyhow a quick and reliable access to these services: With the transfer of these sections to third parties it is possible to offer services more precisely, more reliably and faster to a larger number of customers with a lower price by a still fast access to these services.

8.2 Disadvantages of MDVOs with AAA-supported Workflows

In contrast to previously listed advantages of AAA-supported MDVOs, certain drawbacks have to be considered as well.

The companies of the MDVO develop a strong dependence on their IT infrastructure. If it breaks down - which still occurs (the blackout in New York in 2003 or the attack of the virus "MS-SQL Slammer" in 2003 are just two examples) - the company cannot run its business any longer. Not only income and customers potentially get lost, but

also compensation demands can occur with strictly calculated service level agreements, which could drive a company into substantial economic losses.

The involved companies in the MDVO have a very close partnership, which is hard to be canceled. As previously mentioned, a world-wide standard, that permits an efficient and fast exchange of the involved companies is desirable, but also increases the competition between the companies.

From dividing product services into smaller services and moving it to small specialized companies, these small services get a great importance for the organization. Possibly, the market for this service is too small for competitors, so that the organization will be dependent on the company. Furthermore, potential cross-investments in MDVO members might even increase dependence on them.

8.3 Evaluation of the Suggested MDVO-AAA Model

The model is held in a general form and can easily be adapted to usual or future AAA/A4C protocols. Scalability is ensured: technical implementation of involved entities (service entities as well as the authentication server) is not fixed, however currently used approaches (e.g. DNS Round Robin, Reverse Proxy or AkaDNS) can be used without any problems, on choosing TCP/IP.

However, the following inadequacies exist in the MDVO-AAA model with the elaborated requirements as they have not yet been considered in detail:

- *Message flow confidentiality*

Cannot be realized over Ethernet. The underlying technology is not specified, however there is no comparable technology permitting it and for the nearer future none is foreseen.

- *Anonymity (Recommended Feature)*

Is improbable with the same reasons as for message flow confidentiality and in the described scenario not necessary.

8.4 Analysis of the Example

The described Workflows can be categorized precisely on the basis of the created categories: Looking at the registration business process, all contained workflows are to be arranged as "production workflows". Workflows for the examination of the input data are to be categorized as vertical workflows, since they go over the organization's border. In contrast to that stands the input of the customer data to the internal database, which remains as horizontal workflow within the company. These workflows are all stateless, since their execution remains always the same, even if they are possibly not executed at all. In addition they are "not session related", since the workflows are always executed up to the end, as soon as they have been started. In addition, they are callback workflows, since the result is always passed on and not stored within the workflow.

The same categorization can also be applied to business processes: the registration process is a production process and it is vertical, since it calls services of other companies. In addition it is stateless, because its execution with the same input parameters is always the same. It is a batch process as the result is not immediately needed and it is not session related. In addition it is a callback process. The result is stored, however not during the process, but at an internal database.

The defined value metrics are also suitable to work with workflows. On the basis of derived technical metrics the usefulness of a workflow can be determined (e.g. reliability and timing characteristics) and the necessity (also for extending the system) based on the usage characteristics. With the business metrics a price/costs model can be set up, whose generic derivation, however, is not elaborated in this work.

The workflow metrics are also ascertainable for the whole business processes.

9 Conclusion and Future Work

The construction of MDVOs with an appropriate AAA/A4C structure is a development, which has already begun and cannot be stopped (online trading platforms which showed a high rate of growth in 1999 are only one example).

Within this thesis, it was possible to point out possibilities, characteristics and requirements for MDVOs and AAA/A4C-supported workflows, to determining possible metrics for these and to develop an MDVO-AAA model. Some considerations, e.g. Ad Hoc Workflows, are thereby probably more of theoretical kind and will hardly be found in practice.

Interesting considerations, going beyond the scope of this thesis, and thus forming the basis for future research activities, include an exact price analysis and a generic model for the apportion of the internal technical cost parameters to internal price categories, which are then summarized for external customers to cost expense categories.

Furthermore, specific characteristics in mobility-related issues as well as advanced investigations or adaptiveness of workflows should be targeted. Finally, a technical conversion of the MDVO-AAA model to the underlying infrastructure is suggested.

Bibliography

- [1] G. Caronni, B. Plattner, N. Weiler. Network security lecture, Summer Term 2004.
- [2] Akogrimo Project Website: <http://www.akogrimo.org>.
- [3] M. Rittenbruch M. Rohde and V. Wulf, editors. *Auf dem Weg zur virtuellen Organisation*. 2001.
- [4] R. Bradt. Virtual organisations: A simple taxonomy. 1999.
- [5] K. Möslin. Die virtuelle Organisation: Von der Idee zur Wettbewerbsstrategie. In *Auf dem Weg zur virtuellen Organisation*. Physica-Verlag, 2001.
- [6] A. Litke, D. Skoutas, T. Varvarigou. Mobile grid computing: Changes and challenges of resource management in a mobile grid environment. Presented at PAKM 2004 Workshop.
- [7] M. Rittenbruch, M. Poschen, H. Kahler, B. Törpel. Kooperationsunterstützung in einer teambasierten Virtuellen Organisation. In *Auf dem Weg zur virtuellen Organisation*. Physica-Verlag, 2001.
- [8] T. Zseby, S. Zander, G. Carle. Policy-based accounting. RFC 3334, 2002.
- [9] Overall network middleware requirements report, 2005.
- [10] S. Farrell, J. Vollbrecht, P. Calhoun, L. Gommans, G. Gross, B. de Bruijn, C. de Laat, M. Holdrege, D. Spence. AAA requirements. Technical Report 2906, 2000.
- [11] J. Loughney, G. Camarillo. Authentication, authorization and accounting requirements for the session initiation protocol, 2004. Internet-Draft.
- [12] S. Glass, T. Hiller, S. Jacobs, C. Perkins. Mobile ip authentication, authorization and accounting requirements. Technical Report 2977, RFC, 2000.
- [13] D. Mitton, M. Beadles. Network access server requirements next generation (nas-reqng) nas model. Technical Report 2881, 2000.
- [14] Wikipedia.
- [15] C. Plesums. Introduction to workflow.
- [16] J. Cardoso, A. Sheth, J. Miller, J. Arnold and K. Kochut. Quality of service for workflows and web service processes.

- [17] J. Robertson. Metrics for knowledge management and content management. Technical report, Step Two Designs Pty ltd, 2003.
- [18] L. Anania and R. J. Solomon. Flat: The minimalist price. pages 91–118, 1997.
- [19] P. C. Fishburn and A. M. Odlyzko. Dynamic behavior of differential pricing and quality of service options for the internet. 1998.
- [20] A. M. Odlyzko. A modest proposal for preventing internet congestion. 1997.
- [21] R. Cocchi, S. Shenker, D. Estrin, L. Zhang. Pricing in computer networks: Motivation, formulation, and example. *IEEE/ACM Transactions on networking*, (1), 1993.
- [22] R. Cocci, D. Estrin, S. Shenker, L. Zhang. A study of priority pricing in multiple service class networks. 1991.
- [23] A. Gupta, D. O. Stahl, A. B. Whinston. Priority pricing of integrated services networks. 1997.
- [24] D. D. Clark. Internet cost allocation and pricing. 1997.
- [25] S. Shenker, D. Clark, D. Estrin, S. Herzog. Pricing in computer networks: Reshaping the research agenda. 1996.
- [26] J. K. MacKie-Mason, L. Murphy, J. Murphy. Responsive pricing in the internet.
- [27] B. Stiller, J. Gerke, P. Reichl, P. Flury. Management of differentiated services usage by the cumulus pricing scheme and a generic internet charging systema. 2001.