IDENTITY MANAGEMENT DEFINED

How to position enterprises into the Identity Management framework

Informatics & Economics
Faculty of Economics
Erasmus University Rotterdam

Monday, 19 December 2005

Drs. (Master) Thesis:
Identity Management Defined
Written by:
Frank Ramdoelare Tewari
Supervised by:
Dr. ir. Jan van den Berg
Co-reader:
Dr. Jimmy Tseng

Acknowledgments

I would like to take this opportunity to express my gratitude and appreciation to everybody who helped in the process of writing the thesis. The guidance and support of my supervisor Jan van den Berg has enabled me to successfully complete the thesis. I would also like to thank Jimmy Tseng for his feedback and support and for the great time when I was working for the PRIME Project. Furthermore I would like to thank my parents for their unconditional love, understanding and support. Last but not least, I would like to thank Linde van der Burg, who has supported me unconditionally in the past busy months while carrying our child, her smile was all the motivation I needed.

Frank Radju Ramdoelare Tewari
Monday, 19 December 2005

TABLE OF CONTENTS

CHAPTER 1: INTRODUCTION

In this chapter an introduction to the thesis will be given. The background of the thesis, as well as the subject, the research objective and the methodology will be explained. Finally an outline of the thesis will be made.

1.1 Background

"The rapid advance of information technology (IT) over the past decade has threatened two essential components of individual security: identity and privacy." [2]

Since the advent of the personal computing era in the 1980's, information technology has advanced greatly. From the development of distributed systems and the advent of Internet it has become a challenging task to maintain control of all the different systems available. Moreover, keeping track of personal information disclosed on the Internet, as well as maintaining high standards of internal control and information security within companies has become increasingly complicated. Identity Management applications lay at the core of resolving these type of problems.

Identity Management (IDM) can be defined as following (see section 2.2.2):

Identity Management is a comprehensive set of processes that enable end users to securely access a broad range of internal and external IT systems, control the digital representation of users and manage information about identities.

This definition adequately describes the scope of Identity Management. However, many different applications exist and new technology is emerging constantly, therefore the marketplace and the scope of Identity Management are also continuously changing. Some examples will be given, both from a consumer and a business point of view, to further describe the use of Identity Management in order to introduce the background of the thesis.

From a *consumer's point of view*, the growing E-commerce (see section 2.1.3 Contexts of Identity) market is not very transparent concerning privacy regulations. Consumers are often asked to give up personal information on the Internet in exchange for benefits or when making a transaction, although it remains uncertain if this information is well managed and not abused. During the past years a variety of Identity Management applications have emerged to manage consumer's privacy requirements on the Internet. Nowadays, a great variety of vendors exists that produce or incorporate these applications, and the market is growing rapidly. More usage scenarios are emerging for these types of applications. For example, it's not hard to imagine that in the near future we are able to obtain an electronic driver's license when making more use of E-government (see section 2.1.3 Contexts of Identity), protected by Identity Management applications.

From a *business perspective*, Identity Management plays an important role in information technology. On the one hand, companies often have such a broad variety of systems and platforms that a good IDM system has become indispensable, especially as a result of legal requirements. Businesses frequently own many different legacy systems (existing computers systems and applications with which new systems or applications must exchange information) as well as systems bought from different vendors. Identity Management applications enable users to securely access these systems in a more direct and efficient manner. An example of achieving this goal is deploying Single Sign On solutions (SSO, see section 2.3.2), which enable users to make use of only one password to access a variety of IT systems. Another example is using a central data repository for user information (see section 2.3.5) which stores dispersed data in one central location for easy access. On the other hand, companies wishing to increase efficiency, user productivity or accomplish cost savings also are in need of an effective Identity Management solution. This demonstrates the variety of objectives that can be met by making use of IDM solutions. To further illustrate the broad scope of Identity Management observe the so-called "ghost accounts", which are accounts within an IT system remain active when the user has already left the company. When employees leave a company their account often is not deleted for quite some time due to a possible backlog of the IT department or structural problems of the department. Many Identity Management applications are able to tackle this problem thus relieving the workload of system administrators and increasing efficiency yielding considerable cost savings and risk reduction. Today, Identity Management systems are fundamental for accountability in business relationships; controlling the customization of user experience; improving internal control; mitigation of risk; cost reductions; protecting privacy; and adhering to regulatory controls (see CHAPTER 3: THE NEED FOR IDM).

Identity Management forms an integral part of Information Security. Information Security is designed to protect information of value against unauthorized access and changes. The Information Security Management System Specification, BS 7799 [30], has set the standard for handling the Confidentiality, Integrity and Availability (CIA model, see section 3.2.6 Regulatory Compliance) of information. It is interesting to see how the IT market keeps innovating to tackle these challenges. To illustrate, we can use the example of the energy supplier Enron. Specifically the bankruptcy of one of U.S.A.'s biggest companies in December 2001. Each of Enron's operating companies had its own vice president of IT, and that person was free to dream up his own IT architecture. This decentralization resulted in an incredible complexity of different systems, leading to poor efficiency and high costs. Moreover, due to poor internal control and "creative" though illegal accounting systems Enron was declared bankrupt in the end of 2001. The lack of control and complexity of systems are issues that can be solved by using Identity Management solutions. Several IDM solutions make it possible to fully trace activities made by an employee in the IT system, which improves internal control. The company would have been able to proof compliance and trace fraudulent activities. In hindsight, a good Identity Management framework might have saved Enron, by centralizing and simplifying the IT framework and enabling better internal control.

"*While there is no clear and direct link between Enron's profligate IT spending and its accounting scandal (although both were fuelled by same decentralized, entrepreneurial culture) several experts believe the situation in IT would eventually have caught up with the company."*[1]

Moreover, the market of available Identity Management products is continuously changing; several fusions and take-overs have recently taken place among the main IDM competitors. This indicates the strong growth of Identity Management as a whole and demands for an overview of the current technology. As the market is growing, more and more companies are interested in investing in Identity Management solutions, although the investment decision is often a difficult task, especially if the needs and benefits to be obtained are not clear in advance.

To sum up, Identity Management is a broad and interesting subject. The fact that the IDM market is still continuously changing and innovating adds to the interest to learn more about this technology.

1.2 Motivation

This thesis and it’s subject, namely Identity Management, has been greatly influenced by my participation in the PRIME [3] (Privacy and Identity Management Europe) Project. PRIME addresses research issues of identity management and privacy in the information society. I have worked on the PRIME Project on behalf of the faculty of business administration of the Erasmus University in Rotterdam. During this period I have had the privilege of working with Identity Management software prototypes developed by the Prime consortium, meeting leading figures of the consortium as well as attending several Identity Management seminars.

What I encountered is that the subject Identity Management is still quite new and broad to many individuals and companies. Corporations want to improve efficiency, meet regulatory requirements, gain competitive advantage, lower costs using Identity Management, however many IT managers are overwhelmed by the broad variety of possible solutions. Moreover, literature on the subject is often dispersed and tends to focus on exclusive components of Identity Management. Due to these circumstances and my growing interest in the subject I decided to base my thesis on Identity Management.

1.3 Research Objective and Approach

The subject of the thesis is *Identity Management.* The goal is providing an extensive analysis and explanation of the concept Identity Management.

The research objective:

Development of a positioning model that defines several categories of enterprises and determines an appropriate Identity Management approach for each category.

Different companies have different information needs. Depending on their specific information need they need to define their appropriate Identity Management approach. The research objective of the thesis is to define *different categories of businesses that require different Identity Management approaches*. In order to achieve this, an *IDM positioning model* is developed (see CHAPTER 4: THE IDM POSITIONING MODEL).

The needs of companies vary depending on their core business, strategy, and size, among others. Therefore, different categories of companies require different IDM applications or a different IDM framework. The emphasis on specific components of Identity Management (see section 2.3 Identity Management Framework) varies according to the specific needs of each category. For some companies the emphasis might be on access control, because of legal requirements for example. For others, efficient access to all their different IT systems or even improving customer experience might be of the essence. In addition to distinguishing between different categories of companies, the positioning model determines *which IDM solutions are appropriate in the different categories* depending on the desired benefits.

To construct this model, there must be an analysis of the concept Identity Management and its marketplace, as well as valid data in the form of business cases which support the investment decision and which will be a way to test the validity of the model itself. When implementing the model it is necessary to know what products are available in the market and how these products relate to the specific IDM components described in the thesis. Moreover, business cases provide real IDM implementation scenarios. Case studies will be compared to the positioning model. Therefore, the thesis includes a full explanation of IDM, an overview of the available IDM products in the market, and an explanation of the IDM investment decision supported by a business cases.

1.4 Methodology

My experience working for the PRIME Project has given me access to a great variety of information on Identity Management, as well as hand on experience with Identity Management Systems and software. The thesis is based on an extensive literature review concerning IDM (see REFERENCES), as well as practical experience gained while working for the PRIME Project.

The approach is to develop the IDM positioning model (see section 1.3 Research Objective and Approach) based on a literature review on Information Security and Identity Management. In order to be able to practically implement the model, an overview of IDM products is made. The products are linked to IDM components described in the thesis. This market overview is based on different market studies (see REFERENCES). The model's validity is evaluated based on real cases on Identity Management implementation. The objective is to observe if the model predicted an adequate IDM approach compared to a successful IDM implementation case. An evaluation of the model is provided as well as proposals for further investigation.

1.5 Outline

This section provides an overview of the structure of the thesis. The content of the thesis as well as the relationship among the chapters is described. The thesis is structured as follows:

The following topics are addressed in the thesis:

- Introduction *(Chapter 1).*
- Defining IDM *(Chapter 2)*.
- The need for IDM. *(Chapter 3).*
- The IDM positioning model. *(Chapter 4).*
- The Identity Management marketplace. *(Chapter 5).*
- The IDM investment decision. *(Chapter 6).*
- Evaluation of the model. *(Chapter 6, 7).*
- Conclusion. *(Chapter 7).*

Several questions are raised when constructing the thesis. Following an overview of the questions is provided. Moreover, an indication is provided of which part of the thesis deal with the different questions.

-*What is Identity Management?*
Chapter one provided an introduction to the thesis and its subject. The topic Identity Management will be thoroughly explained in chapter two. An in depth analysis is made: starting with the concept identity, followed by the concept IDM and an IDM framework is constructed.

-*What is the need for Identity Management?*
The need for IDM is explained in chapter three. The chapter will provide the drivers for IDM adoption from a consumer and a business point of view.

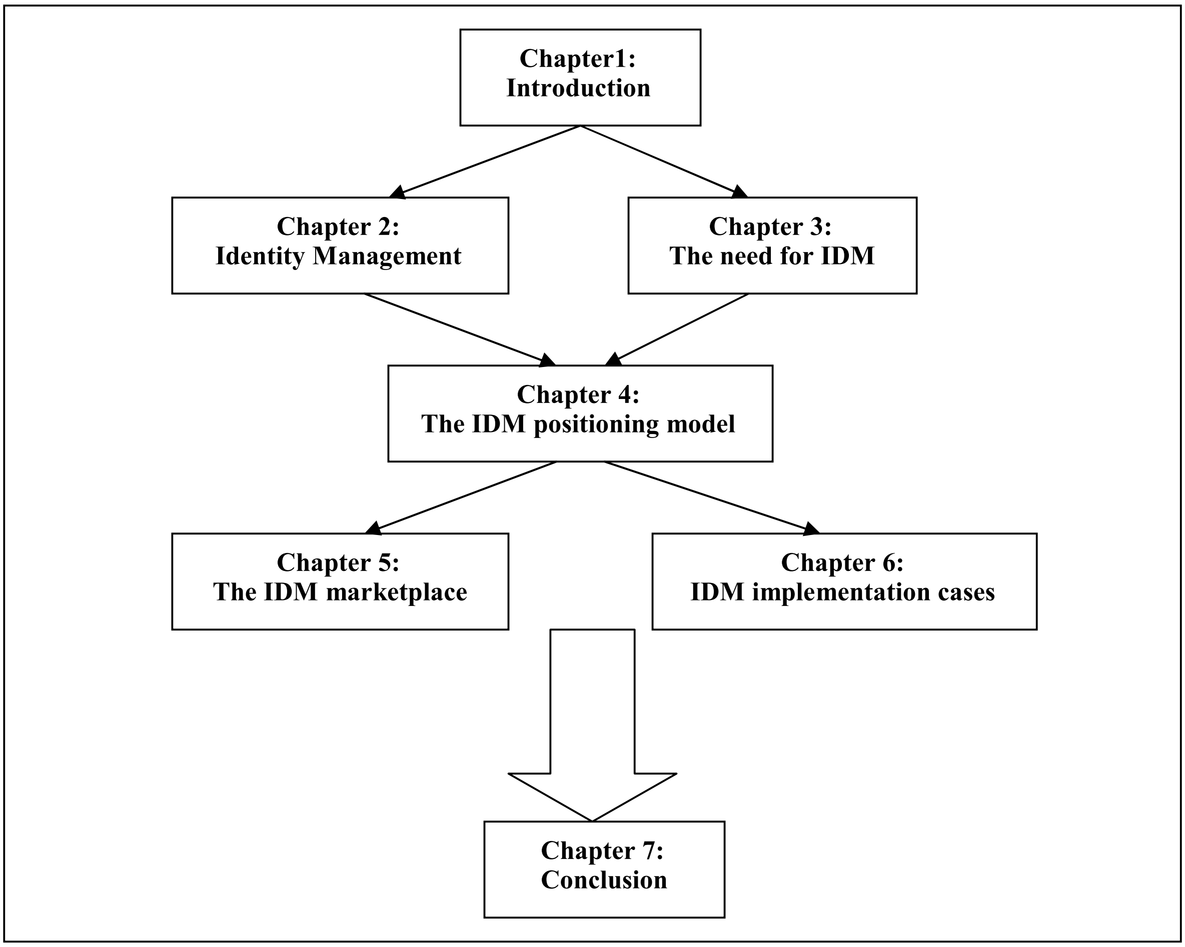
-*What is the appropriate Identity Management approach for enterprises?*
Different types of companies have different needs. A positioning model is developed to define different categories of businesses, each of them with the most appropriate Identity Management approach. The positioning model will be presented in chapter four.

-*What Identity Management solutions are available nowadays?*
The IDM marketplace is extensive and developing continuously at great speed. A non-exhaustive overview of the main competitors and their products will be made in chapter five. The products are

classified into several IDM components, which directly relate to the positioning model since different solutions are needed for different companies.

-*How to approach the Identity Management investment decision?*
Chapter six provides an overview of the IDM investment decision, using business cases. The business case will be compared to the positioning model to test the validity of the model.

Following a schematic overview is provided of the relationship among the different chapters of the thesis:


Chapter1: Introduction
Chapter 2: Identity Management
Chapter 3: The need for IDM
Chapter 4: The IDM positioning model
Chapter 5: The IDM marketplace
Chapter 6: IDM implementation cases
Chapter 7: Conclusion

CHAPTER 2: IDENTITY MANAGEMENT

Chapter two defines the concept Identity Management (IDM). First the concept identity is explained, with the objective to explain the relationship between the real world and the virtual world. Furthermore the evolution of IDM, the IDM framework and its technical components are described.

2.1 Identity

As the term Identity Management indicates, the concept identity plays an important role. To fully grasp the objective of Identity Management, one must first understand the concept of identity. Identity is a complicated concept with many nuances, ranging from philosophical to practical. In the following sections identity will be described. The explanation begins describing identity in its most generic sense. The concept is then broken down to finally describe the concept identity as used in Identity Management.

First of all identity is explained in its most generic sense. Following a definition of identity [7]:

Identity is defined as the distinct personality of an individual (or object) regarded as a persisting entity.

Following the given definition will be analyzed and explained.

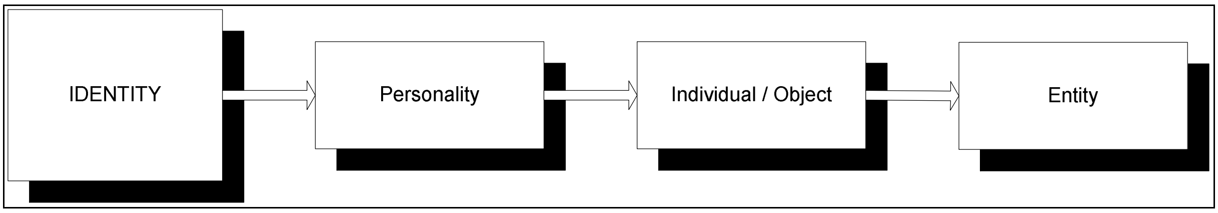


Figure 1: Identity schematically represented.

As Figure 1 shows the concepts introduced in the definition directly relate to each other. The concept "personality" is a collection of characteristics. These characteristics can be behavioral traits, physical traits, and adjectival attributes, among others. The combination of these attributes form an unique picture of the individual or object. An individual most often refers to a person or to any specific object in a group of things. An object is considered to be a physical entity. An object point directly to a entity. Following a definition of the concept entity [6]: *An entity is something that has a distinct, separate existence, though it need not be a material existence*. An entity can be, for example, a person, an animal, but also a pen, a computer program or even a conceptual thing within a business such as an employee. In the definition of identity, entity was conceived as "persisting", which determines the non-volatile aspect of the concept. It defines the continuity of the concept identity, it remains the same identity over a period of time. As is explained, the concepts identity, personality, individual, object an entity each point to each other. Therefore a simplification of the definition is possible. When the pointers to each other are eliminated from the definition, a direct link is obtained from identity to entity. The new definition of identity is:

Identity is the perception of an persisting entity formed by an unique combination of characteristics of the entity.

This definition views the concept identity as a perception of an entity. The definition is deducted from the previously given definition of identity. The new definition provides a simplified explanation of the concept identity. Figure 2 depicts the concept schematically.

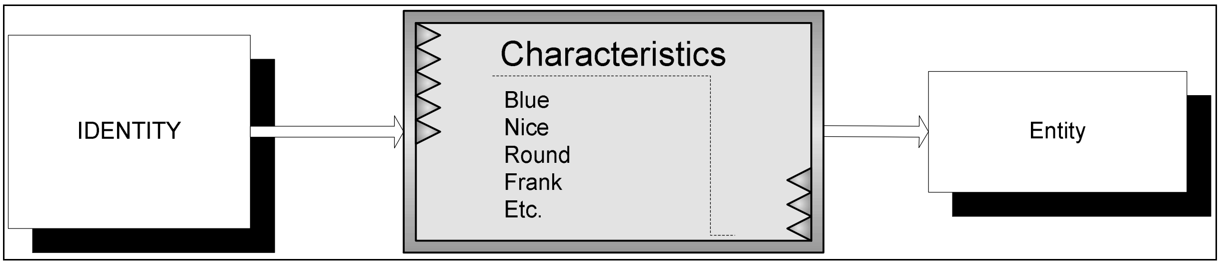


Figure 2: Defining identity as a perception of an entity.

This definition focuses on the combination of unique characteristics that an entity owns. One of the key issues is to know how to distinguish between different identities, to be precise, what uniquely identifies an identity. Each of the characteristics of the entity aid in defining the identity. These characteristics are referred to as *identifiers*. *ID's* or *identifiers* are pointers to the specific entity that is identified. As Figure 2 shows an identifier can be a name, like Frank, or even depict size, shape, color, etc. The identifiers play a key role in establishing the identity.

As can be observed that the concept identity now points directly to the concept entity. An identity is conceived as a perception of an entity. Therefore an identity doesn't need to be a perception of a material existence. The entity to which the identity is pointing can be non-material, or even a concept.

With this notion I would like to introduce the distinction between the human and the virtual world. The concept identity can be looked at from two perspectives; the *human* perspective and the *virtual* perspective. The Information Technology environment is often depicted as the virtual world and the human world is physical reality as we know it. In the following sections it will be explained how the concept identity relates to these both worlds, and ultimately how it relates to Identity Management.

2.1.1 Human Identity

In the human world, we refer to an identity as *human identity*. This is the traditional notion of identity. In the human world an identity points to a physical entity. The entity can be any physical object, but to be more precise, it focuses on the identity of a person. Therefore, in the remainder of the thesis human identity points to the identity of a person. Every time an identity is viewed from a human perspective, we are referring to it as human identity.

Identity in its most generic sense is considered to be a reflection of an individual (subject or object), formed by a collection of characteristics which together form an exclusive perception of the individual. Traditionally, we consider an identity to directly relate to a physical object or subject. For example, when we talk about the identity of a person named John, we are referring to the perception of the collection of identifiers that point to John. Identity is usually perceived from a human perspective: "*Definitions around the concept of "human identity" usually define the term "identity" from the difference between the public and the private aspects of a human*."[4]. Following, a definition of human identity [4]:

Identity is explained as an exclusive perception of life, integration into a social group and continuity, which is bound to a body and shaped by society.

The definition points to the perception of the identifiers of the entity which are bound to social constraints. For example, the identity of a man named John would be formed by the perception people have of John based on identifiers like: the way he behaves himself within a specific social group, his appearance, his name and other social attributes. The combination of identifiers forms the identity of John. This definition is clearly from a human point of view, it focuses on the perception that society has of an entity. The perception is where the difference between the private and public aspects of the person identified is established [4]: *such concepts of identity modify the difference between "I" and "Me"*. By this definition, "I" is the instance that is accessible only by the individual self, perceived as an instance of liberty and initiative. "Me" is supposed to stand for the social attributes (identifiers), defining a human identity that is accessible by communications and that is an inner instance of control and consistency [4]. This explanation is yet another reinforcement of the fact that identity must be conceived as a perception of a person by society, there exists a difference between the perception of the person and the perception of society (difference between private and public aspects of a person).

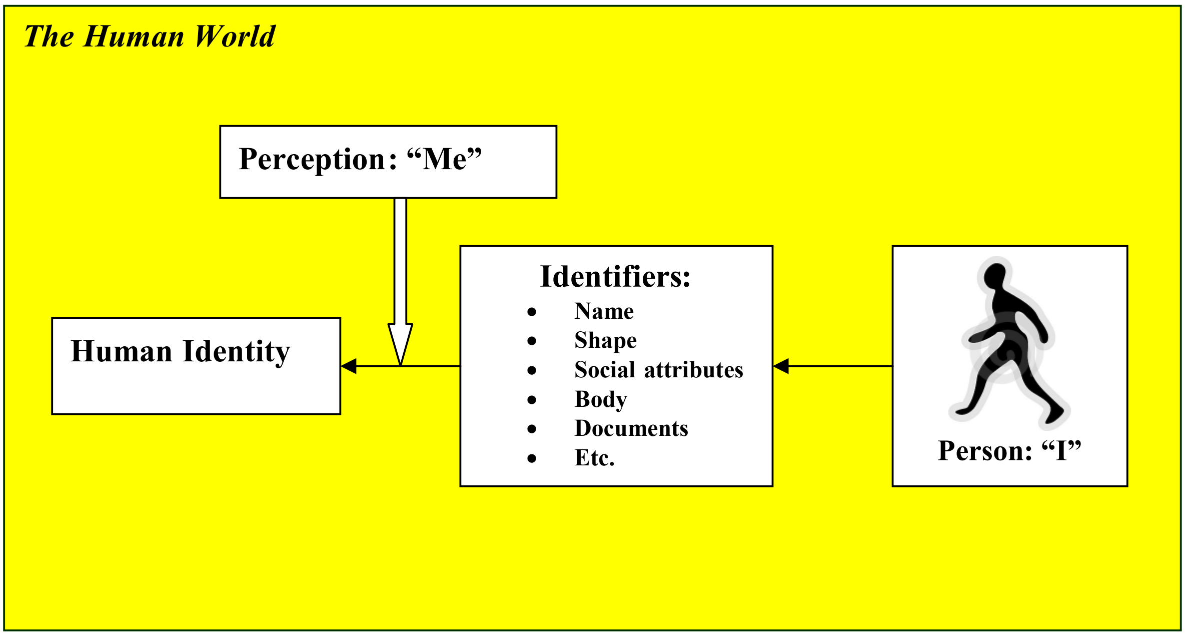


Figure 3: Representation of the concept human identity.

As can be observed in Figure 3, the perception of the person is formed by a combination of identifiers. These identifiers are characteristics that directly point to the person described. Identifiers for human identity can be the person's name, physical traits, character traits, documents, social attributes among others. There exist a great variety of identifiers, just as long as they point directly to the person identified. Some examples of identifiers are documents like a passport, ID card, driver's license, among others. Other examples are the shape of a person (big, small, etc.), the name, function within social group (employee, father, etc.). The key lies in the unique combination of identifiers which together form the human identity of a person.

2.1.2 Digital Identity

"*Identity can no longer be taken for granted as a fundamental physical characteristic. Rather, identity has become a database entity that can be disconnected from physical recognition –even bought and sold as a commodity-…*"[2].

The concept identity has been given a different meaning with the advent of the computer era, especially the internet era. Information Technology has had a transforming effect on commerce, communication, business, among other areas. When making use of IT systems it could be said that we are entering a new world, the so-called *virtual world*. People use a computer to access different IT systems, within those systems they perform actions and sometimes the computer performs actions automatically on behalf of the person using it. The actions performed within the IT system take place in the virtual world, however the person using the computer forms part of the human world (see section 2.1.1 Human Identity). As a result there is an interaction between both worlds. This has lead to a different concept of identity, the so called *digital identity*. Identity Management takes place in the virtual world and therefore mainly focuses on the management of digital identities. Following the concept digital identity will be explained. First a general concept will be described, then digital identity will be explained as used in Identity Management.

A generic definition of digital identity [6]:

> *Digital identity is the digital representation of a set of claims made by one digital entity about itself or another digital entity.*

The digital representation of claims introduced in the definition refers to machine-readable (computer) identifiers. This could also be described as the perception in machine-readable terms of a digital entity.

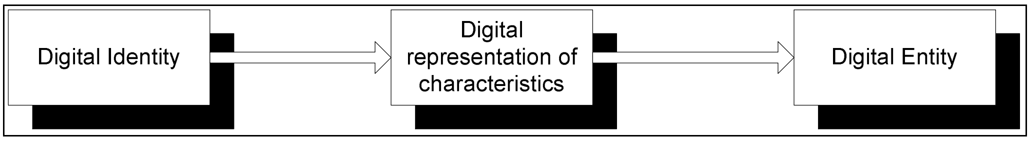


Figure 4: Digital identity schematically represented.

The definition points to a perception of a digital entity, which will be explained following [6]: *a digital entity is defined as a digital resource that functions as a unique and self-coherent subject or organism.* This definition of an entity points to a digital resource, in other words, an object within an IT system. Moreover the definition of digital identity contains a recursive aspect, namely, the reference to *itself*. This represents a digital entity making claims about itself. For example a program making statements on behalf of another program: *digital identities are not an exclusive quality of humans and will be increasingly associated with non-human entities* [9]. To illustrate, a digital identity could also represent a system, a device, or a function within a company such as “accountant” or “employee”. Basically, this definition points out that the digital identity is a collection of claims made by an entity, becoming a digital representation of that entity. It does not differ that much from the definition of human identity because identity is also interpreted as a representation of an entity.

Now the definition of digital identity can be simplified and represented as used in Identity Management. The concept identity has taken on a new form, in its most generic sense it still represents a perception of an object, however its physical character has disappeared. Digital identities are still associated with humans within Identity Management. For example when making a profile on a chat box; the profile is a digital representation of the person making the profile. The identity refers to a human, and therefore to a human identity. As a result the simplified definition of digital identity is:

A digital identity is the machine-readable representation of a human identity.

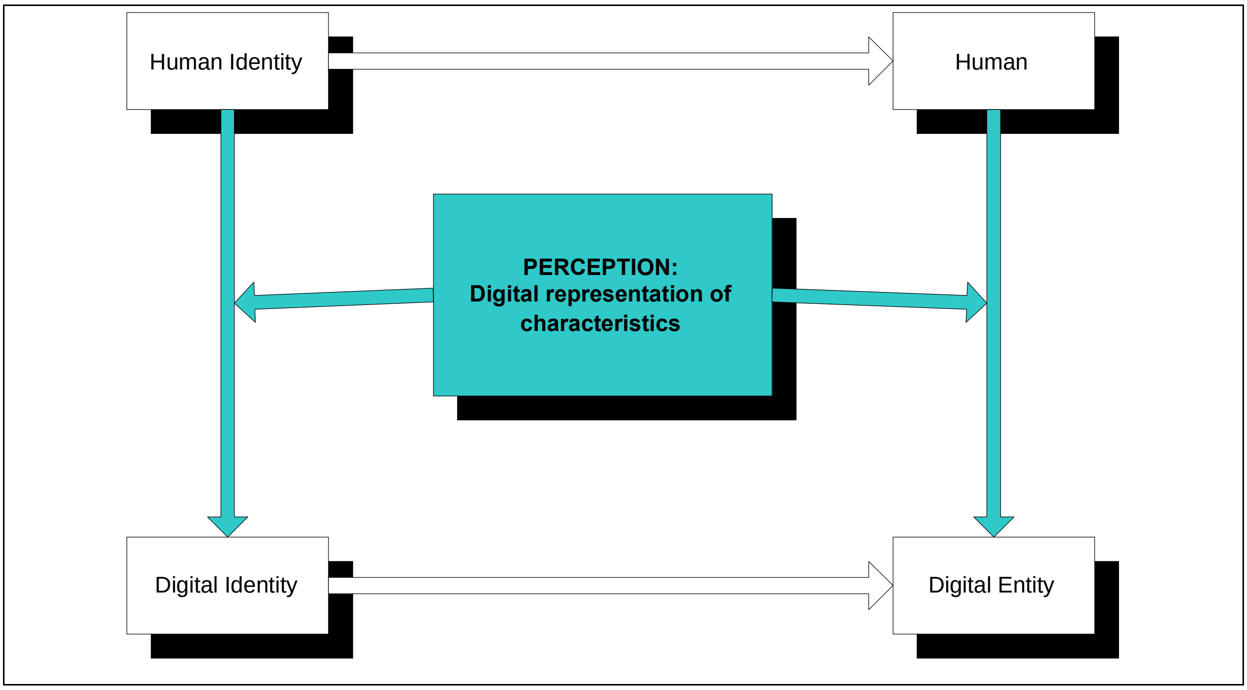


Figure 5: An overview of the relationship between human identity and digital identity.

ID's or identifiers are pointers to the specific entity that is identified. All entities in IT systems need machine-readable names; assigning ID's is a process of mapping real-world identities to machine-readable ones. This mechanism allows to identify the human using the system as a digital entity with his own digital identity. To illustrate: a person uses a computer, the computer identifies this person based on a set of identifiers and maps these to machine-readable identifiers thus creating a digital representation of that human. As a result a digital entity is created that is linked to the human, and this entity becomes a digital identity, a digital representation of the human identity. We now have a direct relationship between the human and the virtual world, namely the digital representation of the human using the IT system into the Identity Management system.

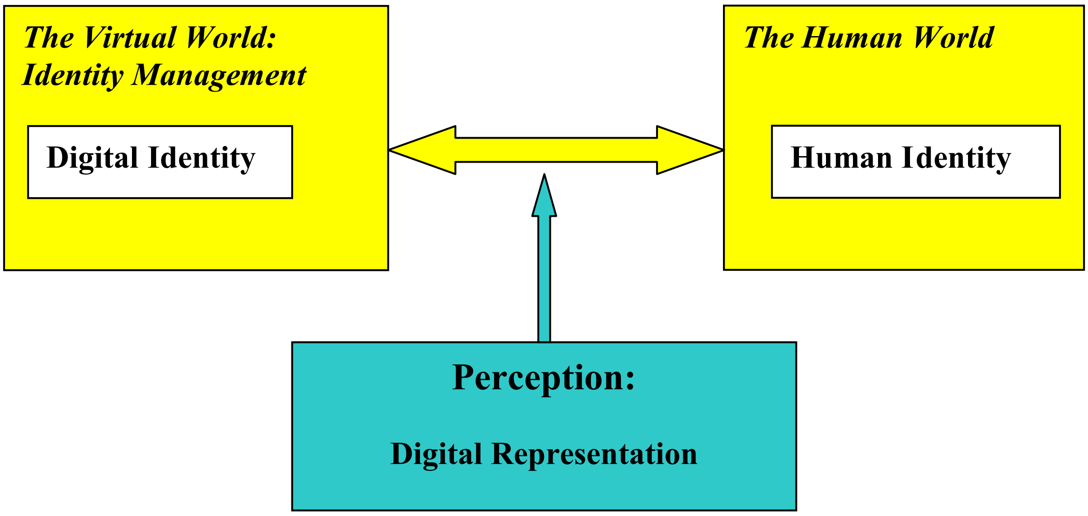


Figure 6: The existing relationship between the virtual and the human world.

To sum up, in Identity Management a digital identity always refers to a human being. The digital identity of a person becomes the digital representation of their human identity. The digital identity works within the IT system on behalf of the human that is being represented. In the following sections it will be explained in what different contexts digital identity is used and identity will be described as an actor.

2.1.3 Contexts of Identity

"Privacy is one of consumer's most important concerns about using the Internet for e-commerce and other purposes" [10].

First of all the concept of *roles* will be introduced. An identity can play different roles in different contexts. For example, take a man named John with a determined identity. John has two children and works in a supermarket. He still has the same identity however he is both father and employee, thus playing two different roles. In Identity Management digital identities can have several roles too. For example, the digital identity can be defined as having the role of "supervisor" within an IDM system. The system will recognize this identity as a supervisor and therefore allow the identity to perform actions that only a supervisor can perform. The IDM system knows the role of an identity thanks to the identifiers. Every identity is made up of a combination of identifiers. Some of these identifiers provide personal information about the person to who the identity is pointing (see section 2.1 Identity). That information forms the identity's *Personal Identifiable Information* (*PII*[1]). The PII of an identity is a

[1] Personal Identifiable Information will be referred to as PII throughout the rest of the thesis.

collection of pointers that provide personal information of the person identified. Different perceptions of the identity's PII are defined, depending on the context [9] (see *Figure 2*):

- *Me Me*: PII the subject is aware of and directly controls.
- *Known Me*: PII the subject is aware of and indirectly controls.
- *Unknown Me*: PII that the subject is not aware of and over which the subject has no control.

The PII of an identity define his role in the environment, therefore the Identity Management system has to administer this PII according to a specified policy. Figure 7 provides an overview of the contexts in which digital identities can be used. The contexts are described in the remainder of this section. As can be observed the different contexts make use of the three perceptions of the identity's PII. Ultimately, people aspire to keep the gap between the "me me" and the "unknown me" as small as possible because people like to know who knows about their personal information.

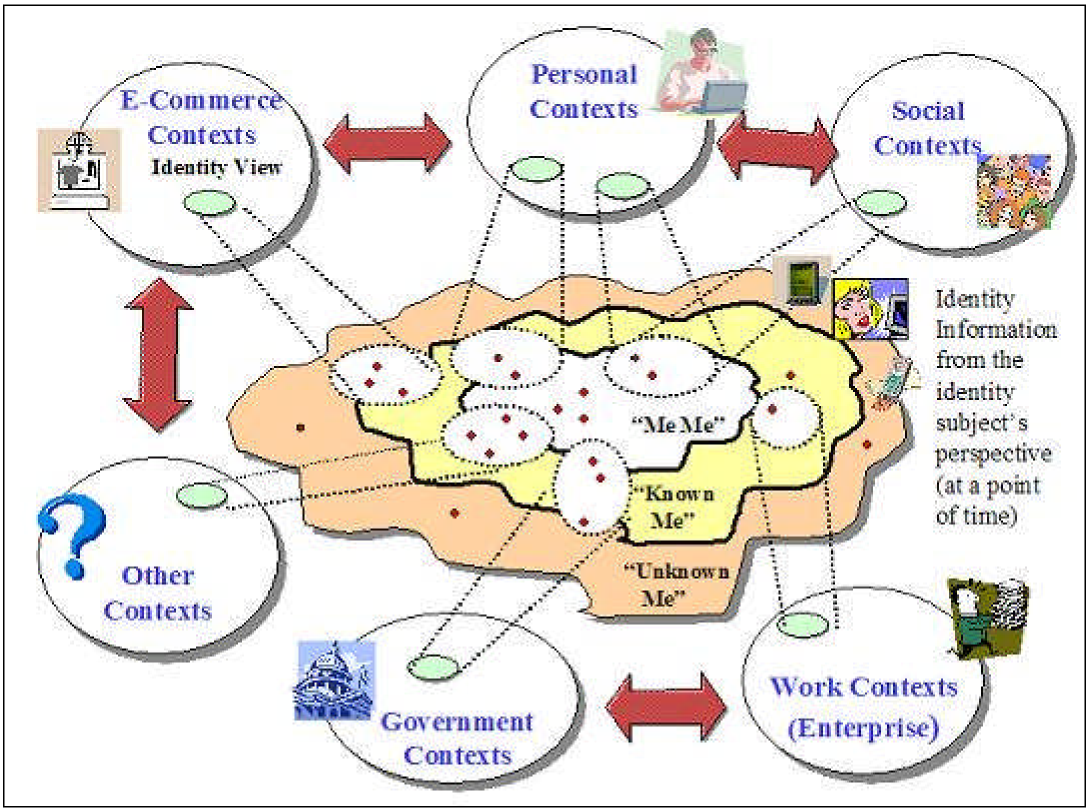


Figure 7: The different views and contexts of identity [9]

Following different contexts will be explained to define the different roles an identity can play. Identity Management systems are also used in a number of contexts. By understanding the different identity contexts it will be easier to understand those of IDM systems. The following contexts are defined on a high-level and therefore globally define the vast array of identity usage. The contexts are: the consumer context and the work context.

-Consumer context:

The consumer context consists of identity usage for consuming purposes. To be more precisely, it consists of a *personal, social, e-commerce*, *e-government* and *e-health* context. The consumer context is focused on the use of the Internet. Identity usage in this scenario can be surfing the web for information or for e-commerce, e-government, e-business, among others. E-commerce is the buying and selling of goods and services on the Internet, especially the World Wide Web. In practice, this term and a newer term, e-business, are often used interchangeably. For online retail selling, the term e-tailing is sometimes used. E-government consists of government activities that take place by digital processes over a computer network, usually the Internet, between the government and members of the public and entities in the private sector, especially regulated entities. These activities generally involve the electronic exchange of information to acquire or provide products or services, to place or receive orders, to provide or obtain information, or to complete financial transactions. Another area of interest is e-health, the online activities concerning exchange of health care information and, in the near future, possible online health care transactions. An example of the growing interest in e-health is the eHealth Initiative and Foundation [16], who have expanded upon a growing set of resources and tools designed to support states, regions and communities across the nation who are engaged in health information exchange.

When surfing the web, most individuals wish to conserve their *privacy*. Although awareness for privacy concerns on the Internet still needs to be increased, we see that this is one of the main reasons in Europe for not using e-commerce. Especially when making use of e-commerce most individuals will express their concern for possible misuse and be reluctant to give up personal information. In this role, minimization of the data that is collected on the individual is desirable. In the near future it is not unthinkable that, for example, a driver's license will de digitally issued. This role of an identity raises a whole new set of privacy and security concerns. Identity theft could become disastrous in this scenario. Therefore, protection of data and being able to take on a different role with less disclosure of personal information is essential in these scenarios.

To sum up, the consumer context consists of:

- Personal context: surfing the Internet for information or leisure.
- Social context: usage of IT for social purposes.
- E-commerce context: usage for online transaction.

- E-government context: usage for online governmental activities.
- E-health context: usage for online health care activities.

- Work context:

Work context refers to the business environment in which an identity can exist. Rather than being a customer like the consumer scenario described before, the different possible roles the identity can adopt are those in a business/ working environment. Employees will have different defined roles, depending on their responsibilities and privileges. Therefore, some employees can access different information than others. To obtain this, the definition of their role within the organization is essential. Other roles are, for example, suppliers, third parties, among others. The Identity Management system must take into account all these different roles, based on different types of identities. An Identity Management systems play an important part in a work context, since many IDM applications have the objective of increasing effectiveness and user experience within a company.

2.1.4 Identity as an actor

After the previous explanations of the concept identity, this section describes identity as an actor. In section 2.1.2 a digital identity was described as a digital representation of a human identity. Identity Management focuses on digital identities. These identities can perform actions on behalf of the person using the IT system. In result, the digital identity of that person is an actor. Following will be described how IDM systems are able to perform actions with digital identities.

The content of an identity is crucial in Identity Management. An IDM system is able to manage a digital identity depending on its content. The content of the identity usually varies depending on the context where it is used, and the role that identity plays within that context. An identity can be used in several contexts (see section 2.1.3). The content provides information about the identity for three key aspects of Identity Management: *identification, authentication* and *authorization*. These three components form the *access control* component. After performing these three steps the IDM system is able to let the digital identity perform actions like ,for example, getting access to information or other systems.

Identification is the first step; each digital identity is identified by the IDM system by a set of pointers. These pointers are referred to as identifiers. An example of an identifier is name, which the IDM system can recognize. To illustrate, a person uses the computer and provides his digital identity by entering a username. By entering that name, that person is claiming to be owner of that digital identity.

The next step is *authentication.* Authentication is the verification of a claimed identity[5]. An IDM system must know if the digital identity is really what it claims to be. For acting within an ICT system, the user has to be assigned an identifier. In general there are three different methods for authentication [5]:

- Something you know (e.g., a secret such as a password)
- Something you have (e.g., a token or a chipcard) and
- Something you are (biometrics).
- Where you are (location-based services).

The location of the identity can often also offer identity information. For example, the so called *location-based services* offered by mobile operators are based on the location of the device. They offer services based on the location of the identity; by identifying the position, access is granted to a vast variety of services. Once the digital identity is authenticated and established, this identity can now undertake certain actions such as get access to information or obtain a privilege to perform certain actions.

The third step is *authorization*. Through the authorization process the IDM system enables the identity to perform actions if its authorized to do so. The IDM system checks the content of the identity and then, based on the policy of the system, determines what the privileges of the identity are. An authorization example is the existence of a driver's license. When somebody owns a drivers license he is authorized to drive a vehicle. The same situation occurs within an IDM system, if the digital identity has the proper credentials, it will be authorized to perform actions.

As described earlier in this section; identification, authentication and authorization is based on the content of the digital identity. Figure 8 depicts the information that make up the content of a digital identity. In Figure 8 the content of the identity can be observed in three different environments, namely; company, web and application. These environments are chosen as examples. It can be seen that the identity is formed out of three distinct parts:

- *Profile*: characteristics that define the identity in its context.
- *Identifier*: pointer to the specific entity that is identified.
- *Access control*: authentication and authorization data depending on context policy.

These three part provide the IDM system with the necessary information to decide what actions to undertake with the given digital identity.

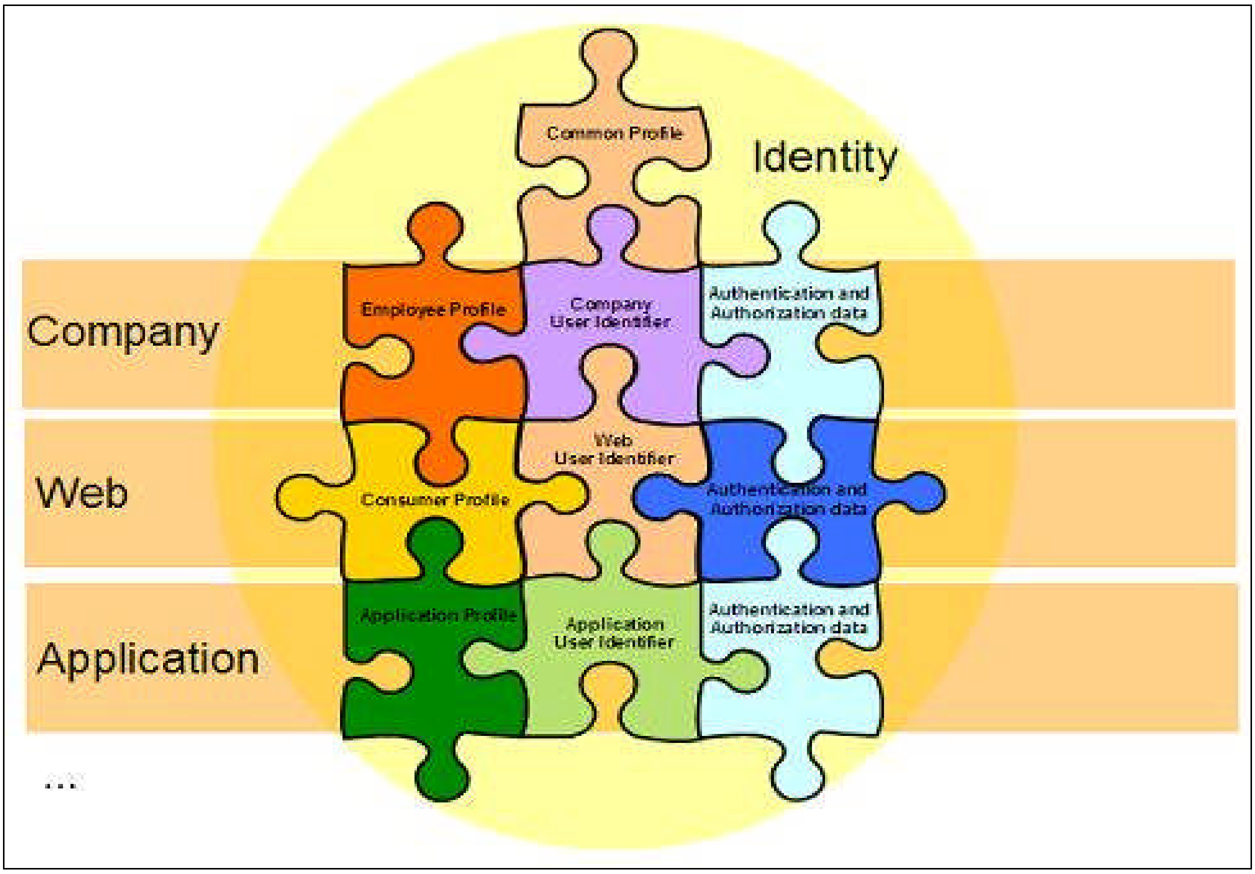


Figure 8: Identity content [9]: When used in a context, an identity provides profile data, identification, authorization and authentication data.

Now that is explained how a digital identity functions as an actor within an IDM system, we can look at an identity as an actor within society. The identity of an individual is protected by law. Legal protection of the identity is used for the protection against misuse of identities; Identity Management often is used for the same purpose. The legal requirements are incorporated into Identity Management solutions; therefore legal compliance is one of the drivers for businesses to invest in these solutions. The main legal sources of the protection of human identity are [5]:

- Constitutions.
- International Treaties
  - Treaties of the European Union.
  - European Convention for the Protection of Human Rights and Fundamental Freedoms.
  - European Directives.
- National Law.
- Other national Regulations.

The aspects of human personality that are protected by the above mentioned legal sources are:

- One's name.
- Freedom from physical constriction (habeas corpus).
- Inviolability of the domicile and right of privacy.
- Freedom of speech and self expression, in particular:
    - The right to choose one's image.
    - The right to protect one's honor.
- Freedom of movement and to settle (granted only to fully aged people).

For digital identities legislation and regulations also apply. Apart from the normal legislation applying to an identity, most laws and regulation for digital identities focus on privacy and integrity of data. All of these legal aspects must be taken into account when identities are managed. When managing identities within an IT system, legal compliance is of the utmost importance (see section 3.2.6 Regulatory Compliance).

The concept identity has been described in detail in the previous sections. With this information in mind, the concept Identity Management will be explained in the following sections.

2.2 Identity Management

The following brief introduction gives an overview of Identity Management; in the following sections a detailed explanation is provided.

Enterprises today want to extend their use of the Internet as a business-enabling platform, achieve unprecedented levels of efficiency, capture market share, increase customer loyalty and generate new revenue streams. Some of the challenges businesses are facing today are escalating costs of user administration, increased security risks, the growing number of regulations, low user productivity, inefficiencies and errors when trying to access information of partners, among others. Identity Management plays a key factor in enabling some or all of these objectives (see section 3.2) and in facing these challenges.

Identity management is a much used term that refers to a set of technologies intended to manage a basic issue: information about the identity of employees, contractors, customers, partners and vendors is distributed among too many systems, and is consequently difficult to manage. Furthermore, companies nowadays often possess a vast array of different IT systems, providing access and controlling these systems is a complex task. Moreover; digital identities, profiles and their management are increasingly required to enable interactions and transactions on the Internet among people, enterprises, service providers and government institutions. By consolidating user data from a variety of disparate sources, Identity Management systems can improve security provisioning across fragmented application environments and dramatically reduce administration and maintenance costs. Research conducted by The Radicati Group, Inc. shows that an Identity Management solution can reduce administrative costs by up to 78% [12]. With an Identity Management infrastructure in place, organizations are also able to develop new business models for communication and application access.

2.2.1 Evolution of Identity Management

Identity Management is a relatively new concept. The name Identity Management actually appeared around the year 2000, and was cited as such by important consultancy companies such as the Burton Group and Gartner. It had become a common denominator for a variety of technologies focusing on information security. A technology worth mentioning is Public Key Infrastructure (PKI). PKI enables users of a network (such as the Internet) to securely and privately exchange data through the use of a public and a private cryptographic key pair that is obtained and shared through a trusted authority. The public key infrastructure provides for a digital certificate that can identify an individual or an organization and directory services that can store and, when necessary, revoke the certificates. PKI is often still implemented in Identity Management. Another example is account management, technology based on the management of IT accounts within a system. These technologies focused on digital entities. Identity Management focuses on the human behind the digital entity, thus the management of digital identities. Previously these technologies where stand alone solutions, however the shift of focus on managing information about humans accessing IT systems gave birth to the concept Identity Management.

As explained these information security technologies evolved into modern Identity Management. The first "IDM" technology was conceived by David Chaum in 1984 [4]:
"The roots of identity management in digital communication are about 30 years old. First ideas of a multi-purpose identity management are mentioned by David Chaum 1984 who wanted to give each individual a card-computer to handle all payments and other transactions [cf. Chaum 1984]."
David Chaum made the first mathematical identity management model. He had in fact written about a privacy-enhancing Identity Management application. He wanted to ensure the individuals privacy and protect its information when making payments and other transaction. Identity Management has evolved a great deal since then.

Regulations (see section 3.2.6 Regulatory Compliance) such as Sarbanes-Oxley Act of 2002 implemented in the U.S.A. forced businesses to keep track of sensitive data. At the same time, various technologies that fell under the umbrella of ID management have started to mature. Identity management is a critical measure for long-term security. Specifically, it refers to controlling the digital representation of users across an organization. Issues ranging from legal and regulatory forces to business requirements are driving businesses toward an identity management solution. In most cases, this means adopting an identity management system to coordinate the management of the digital identities that define users on virtually every electronic system used. Modern enterprises often own a great variety of IT systems. Within this complexity of systems it is difficult to maintain high standards for security and internal control. Moreover, it is very likely for a company to lose efficiency, time and money if an Identity Management solution is not adopted.

2.2.2 Definition

Identity Management is defined as follows:

Identity Management is a comprehensive set of processes that enable end users to securely access a broad range of internal and external IT systems, control the digital representation of users and manage information about identities.

In section 2.1.2 the concept digital identity was described as the digital representation of a human identity. The previous definition of Identity Management talks about the digital representation of users, thus it is referring to digital identities. When Identity Management is implemented, users are controlled by managing their digital representation, managing information about these identities and providing secure access to different IT systems.

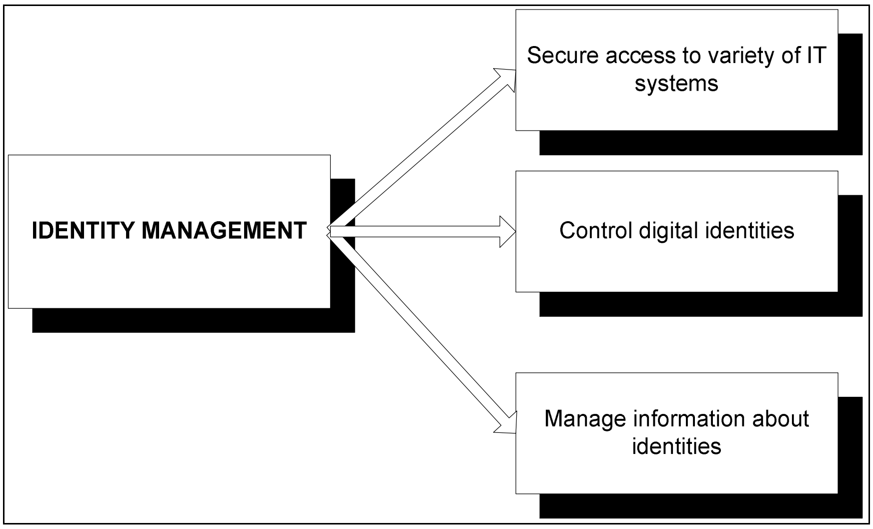

IDENTITY MANAGEMENT
Secure access to variety of IT systems
Control digital identities
Manage information about identities

Figure 9: A representation of the definition of Identity Management

Figure 9 shows the functionality of Identity Management as described in the definition. The definition consists of three components: secure access to different IT systems, control of digital identities and management of information about digital identities.

The first part of the definition consists of all processes that have the goal of giving users *secure access* to different IT systems. IT systems are often very dispersed and companies tend to have a large variety of different systems. Accessing al this different systems can be a time consuming and inefficient task. Moreover secure access to external systems enables companies to form strong alliances with others by sharing information. IDM solutions enable better access: increasing the user experience, efficiency and lowering security risks.

The control of digital identities focuses on the control of the digital representation of the users of the IT system. The workload of IT managers and system administrators can be reduced considerably when an IDM system is implemented. The users of the system are administered by the IDM system and given tools to increase user experience, efficiency, among others.

The management of information of digital identities leads to a number of benefits. Better privacy management is one of these aspects. Moreover, from a business perspective, the logging of information of user actions increases the possibility of auditing and internal control.

These three components globally describe the areas of operability of IDM. Each of these three areas comprise a wide range of technological IDM solutions. Each of this solutions serve a specific goal that lies within the scope of the globally defined three components. Identity Management is often defined as a combination of its technical components, based on the management of digital identities and/or the roles (see section 2.1.3) they represent. A definition based on this perspective is:

Identity Management (IDM) represents a category of interrelated solutions that are employed to administer user authentication, access rights, access restrictions, account profiles, passwords, and other attributes supportive of users' roles/profiles on one or more applications or systems.

The previous definition defines Identity Management as a combination of solutions; therefore it clearly shows how broad the concept of Identity Management actually is. However, Identity Management is more than just a collection of its technical components. The previous definition focuses on the technical IDM solutions. According to this definition Identity Management can be looked upon as a global denominator of a set of processes concerning the management of identities. Identity Management is a broad subject, comprising many different applications. There is a vast array of technical IDM components available nowadays (see Figure 10). To fully grasp the full functionality of Identity Management a framework is constructed in section 2.3.

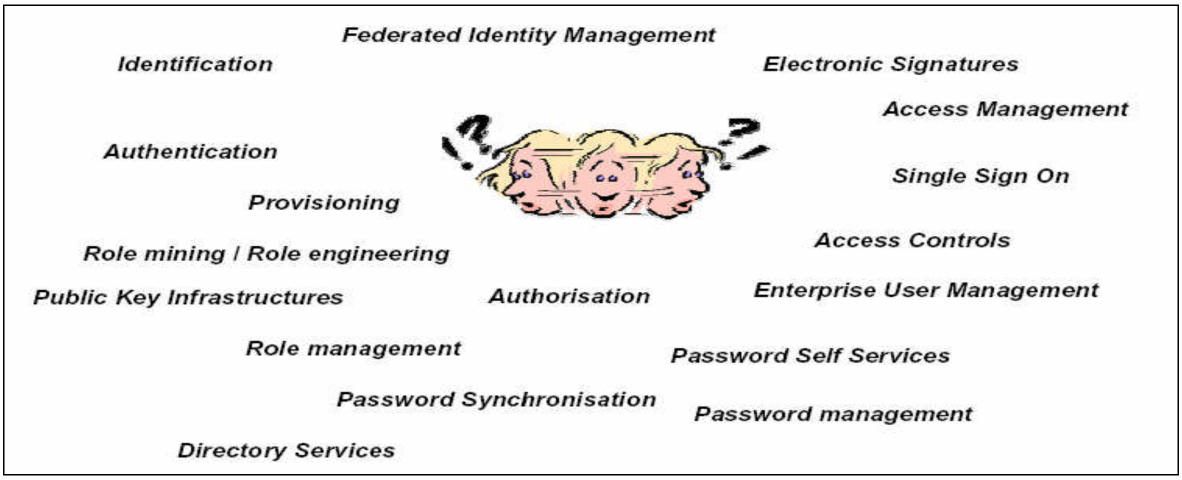


Figure 10: The vast array of interrelated IDM solutions, a clear modular overview of IDM technologies is needed.

2.3 Identity Management Framework

In order to describe all the technological features of Identity Management a framework is constructed. The components described in the framework have several objectives. These objectives lie within the scope of the globally defined components in the definition of IDM (see section 2.2.2 Definition).

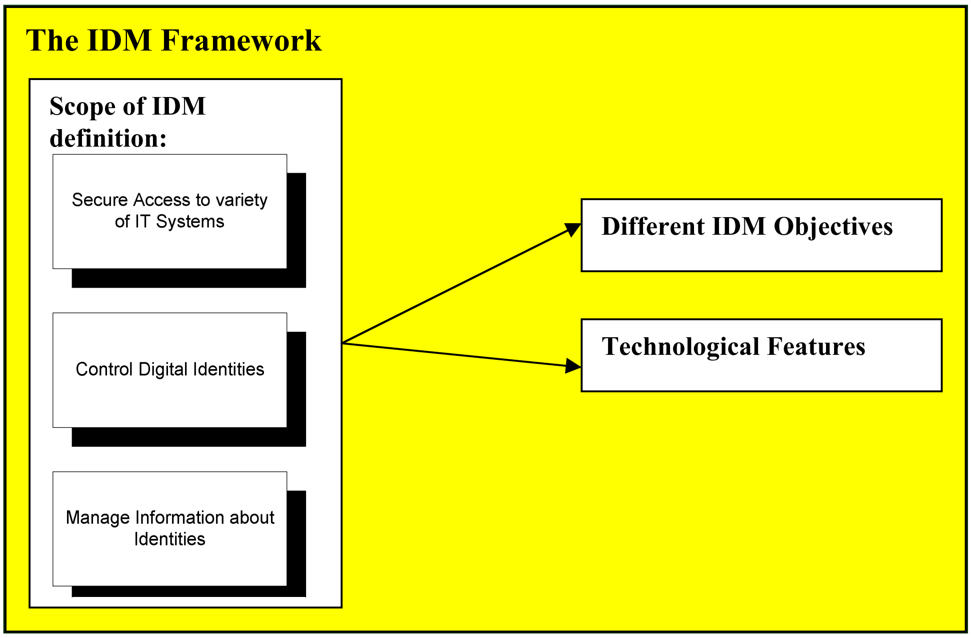

The IDM Framework
Scope of IDM definition:
Secure Access to variety of IT Systems
Control Digital Identities
Manage Information about Identities
Different IDM Objectives
Technological Features

Figure 11: The Identity Management framework describes the IDM technological features. These features serve an objective that is comprised within the scope of each of the three components of the definition.

To asses the basic framework for an Identity Management solution several aspects have to be taken into account. The Identity Management framework consists of a large scale of technology features such as provisioning, authentication, single sign-on, access controls, directory services, password management, role management, authorization, password synchronization, password self-services, enterprise user management, logical access management, identification, among others. The technology features of Identity Management will be described in this section.

In order to comprehensively classify all these features the overall framework for Identity Management must be broken down into different layers. The result is a modular framework that consists of a set of components each serving a specific objective.

Following a modular overview of the components is given. This analysis is based on the framework made in the paper *An Introduction to IDM* [9]. This framework was chosen due to the effective capture of all areas of IDM operability. The framework will be extended with further information on the different topics as well as a description of available technologies. Figure 12 depicts an overview of the framework.

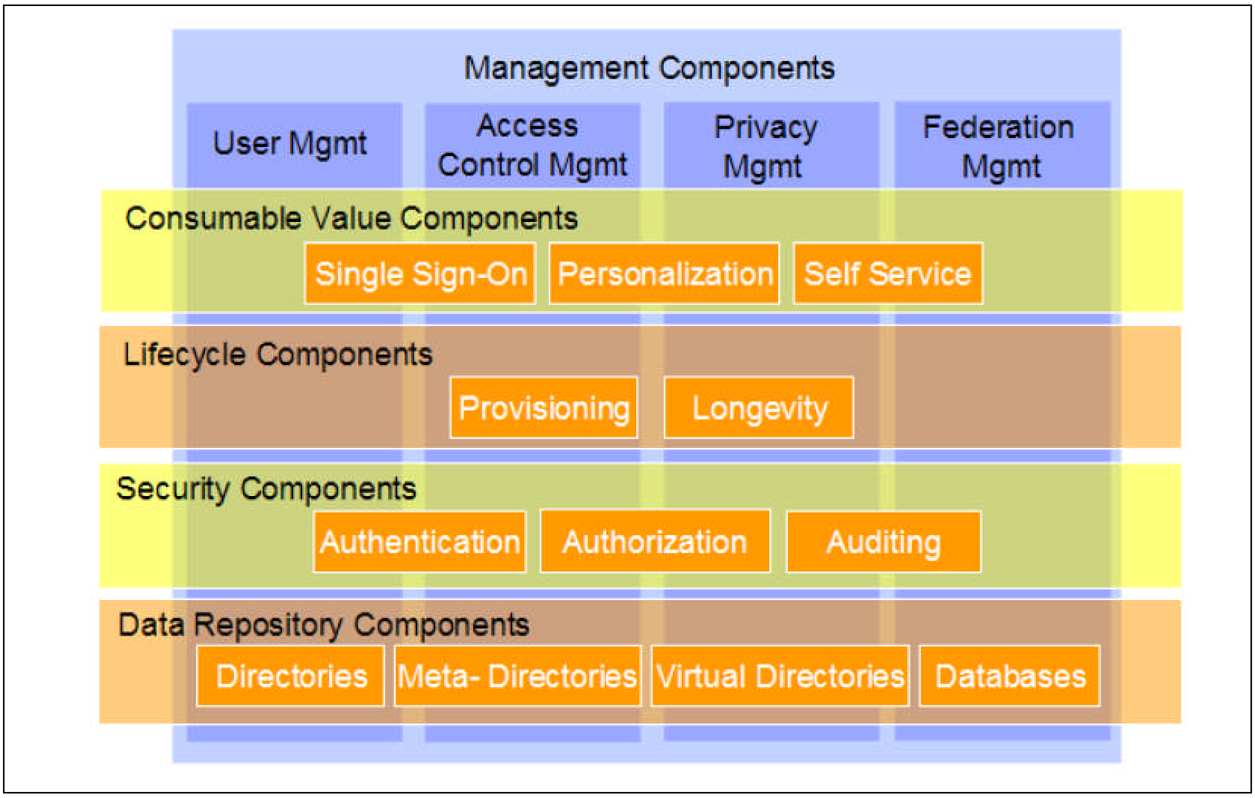


Figure 12: An Identity Management framework, a modular overview of IDM solution components [9].

First of all it can be observed that the framework (Figure 12) is broken down into management components and four layers, namely: consumable value components, lifecycle components, security components and data repository components. Each of the components will be described in the following sections. The data repository component will be referred too as repository in the explanation of the other components. The data repository component plays an important role for the representation, storage and management of identity and profiling information and provides standard APIs[2] and protocols for access [9].

In the following sections each component of the Identity Management framework will be explained.

[2] API (Application Programming Interface): A standard interface between a communications device and a software application operating in a computer.

2.3.1 Management Components

The management components are made up of the areas where IDM solutions apply. These areas are *user management*, *access control management*, *privacy management* and *federation management*. These components adequately describe the specific areas of IDM operability. The management components will be explained in this section. The explanation makes it possible to form an clear idea of the existing technologies explained in the remainder of this chapter.

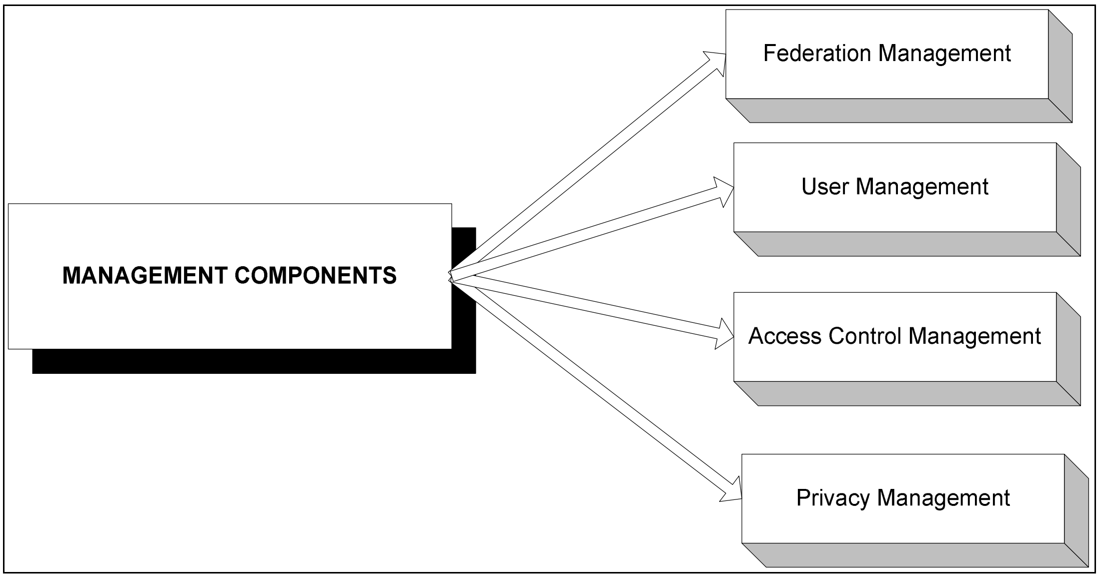


Figure 13: A representation of the different management components.

-User Management:

User management provides IT administrators with a centralized infrastructure for managing user profile and preference information. Moreover it enables organizations to decrease overall IT costs by providing user self-service capabilities and also enhance the value of their existing IT investments through directory optimization and profile synchronization capabilities [9].

The objectives component is made up of those technological components that apply for controlling digital identities and managing information about digital identities.

It closely relates to the other management components since at the core of user management lies managing information about the user's identity and then in return granting access, privileges or even maintaining control of the identity's PII (privacy aspect). In Figure 12 it can be observed what layers and technological components relate to user management.

-Access Control Management:

The access control management service increases security, reduces complexity and overall IT costs by automating access policies for employees, customers, and partners [9]. This component grants access to end users to different applications. Access control consists of three essential components: *identification, authentication* and *authorization* (see section 2.3.4 Security Components).

Identification allows the IDM system to identify a digital identity through the use of an identifier. For example, when a user accesses the IDM system he provides a name. Through this name he claims to be a digital identity that point to him. The IDM system now knows which digital identity has presented itself. The next step is controlling if that identity is who he claims to be (authentication).

Authentication validates the identity of users (or other digital entities), through authentication mechanisms such as a passwords, digital certificates, biometric devices, or tokens.

Authorization is the process of granting privileges to the identity once authentication is established. Once an end user is authenticated, the Identity Management system is aware of a user's identity and grants access and privileges to enterprise applications. For example, if an employee of a company has authenticated his identity in the IT system by entering his password (or biometric identification such as fingerprints or retinal scan) he will then be allowed thanks to the authorization mechanism to perform actions for which he is authorized.

These three components will be explained in detail in section 2.3.4 Security Components. Security in this layer is critical to ensure that only authorized parties gain access to enterprise resources. To this end, the user authentication process is often augmented with a *Public Key Infrastructure (PKI)* - an enterprise-wide framework that provides encryption-based security for a wide range of electronic transactions [12].

-Privacy Management:

"Privacy is one of consumer's most important concerns about using the Internet for e-commerce and other purposes." [10]

A great variety of IDM solutions focus on the management of privacy. This affects both companies as consumers. Companies want to ensure privacy and data protection for regulatory compliance (see section 3.2.6 Regulatory Compliance). Consumers demand secure management of their personal information. When a consumer is surfing the Web, he generally likes to be in control of his PII (Personal Identifiable Information).

There are several ways in which a website can violate privacy compliance [10]:

- *Unintended disclosure of PII.*
- *Uncontrolled collection of PII, failure to post privacy policies.*
- *Having multiple privacy policies.*

Privacy protection affects three major areas [14]:

- *E-mail privacy.*
- *Access and security.*
- *Personal information.*
- *Unsolicited marketing.*

IDM solutions typically focus on the above described areas of privacy protection.

Several standards have emerged for the protection of privacy on the Internet. The most widely recognized standards are:

- *P3P:* The World Wide Web Consortium's (W3C´s) platform for privacy preferences P3P standard enables the user to view the company's privacy statement (tagged in XML).
- *CPEX:* Customer Profile Exchange uses an XML-based approach that applies privacy-related metatags for different pieces of PII it collects of consumers. It also defines rules for the exchange of information between organizations.
- *XNS:* Extensible Name Service is a global naming and directory service that performs name and address delegation keeping in account consumers and businesses´ online privacy policies.

Typical IDM privacy management applications include anonymizers (eliminate all information and tracking possibility of the user when browsing), P3P compliant browser, among others. These solutions are often referred to as *Privacy Enhancing Technologies*, or *PET* (see section 2.4.1).

-Federation Management:

Many organizations need to manage the identities of external users as well. For these businesses, an Identity Management solution is complemented with *Federation Services*, which enables the secure sharing of information with external systems, thereby extending the Identity Management infrastructure to external parties [12].

Federation management, also known as Federated Identity Management, is the collection of agreements, standards, technologies that make identity and entitlements portable across autonomous domains [18]. It enables the establishment of trusted relationships between distributed identity providers. Often this involves the sharing of things like web service endpoints, X.509 certificates, and supported/desired authentication mechanisms [9].

The adoption of new distributed computing models (federation) are requiring enterprises to recast their view of themselves as a component of a larger interdependent construct. With the emergence of inter-company computing, more transparent movement of the individual or company between control boundaries is becoming possible. While it's entirely possible to control the costs and complexity of identity federation on a limited scale, within small circles of trust, wide-scale federation introduces new costs, complexity and challenges which exist on an entirely new scale [17]. Moreover several areas exist which should be successfully dealt with for successful federation management, namely: legal compliance, liability, risk, mutual confidence and effective communication between the different parties. Federation management is still developing and consolidating nowadays.

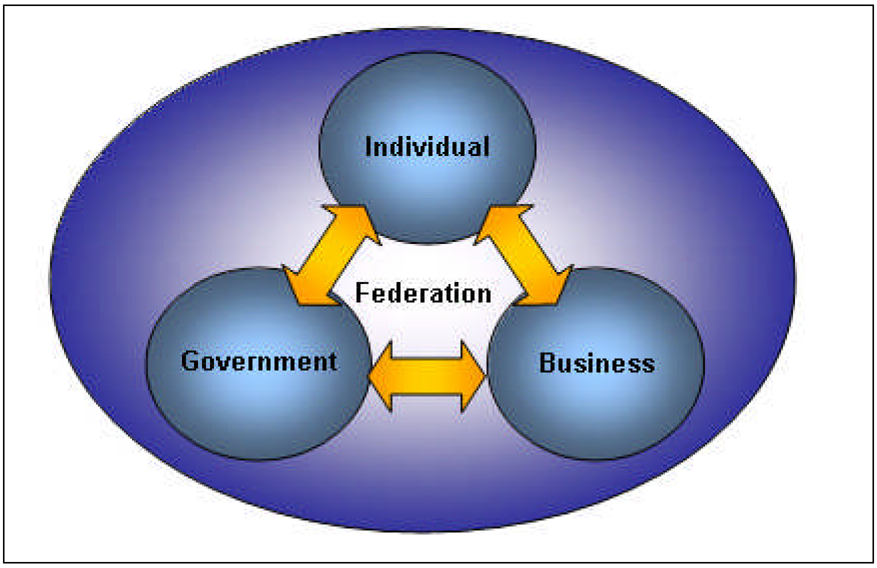


Figure 14: Successful implementation of federation management means the needs are met of all parties involved, namely the individual, the business and the government.

2.3.2 Consumable Value Components

The component referred to as consumable value components refers to three generic types of technology, namely: *SSO* (Single-Sign On), *Personalization* and *Self Service.* The component serves objectives related to the control of digital identities.

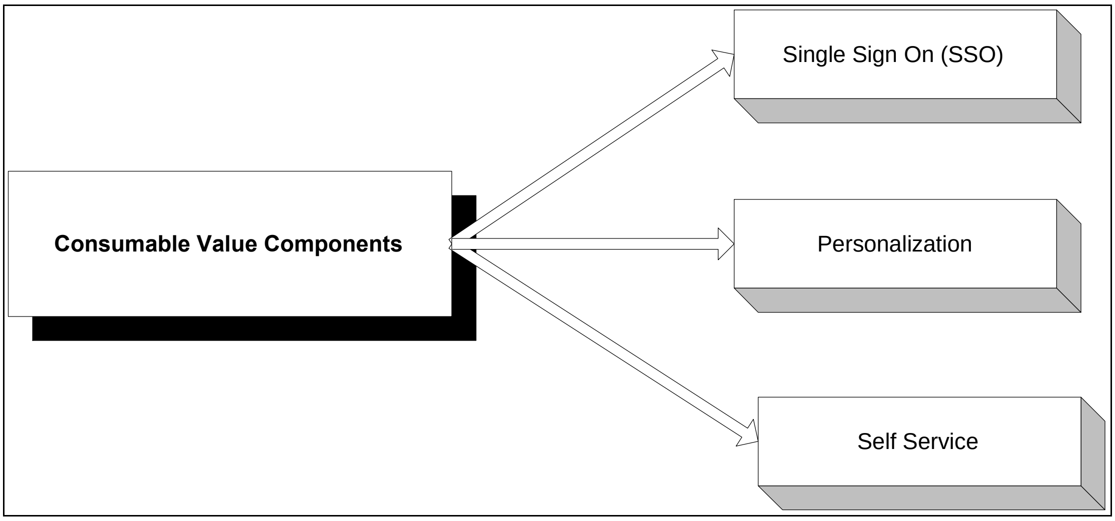


Figure 15: The consumable value components represented.

First of all the concept *password management* will be introduced since it plays an important role in the consumable value components. As the name describes it deals with the management of passwords. Password management forms a part of the consumable value components as well as a part of the IDM framework and as will be shown in the remainder of this section, is a global denominator of some of the consumable value components such as SSO, password reset and synchronization. Following each type of the consumable value components will be explained and an overview is provided of their functionality linked to the management components.

-SSO or Single Sign-On:

Single sign-on (SSO) is mechanism whereby a single action of user authentication and authorization can permit a user to access all computers and systems where he has access permission, without the need to enter multiple passwords. SSO forms part of the earlier described password management. Single sign-on reduces human error, a major component of systems failure and is therefore highly desirable but difficult to implement [19]. This difficulty is due to the great variety of different systems companies often posses, and the difficulty is increased in a federated IDM scenario where multiple parties are present, each with their own variety of systems. The SSO server stores individual passwords for each system that a user accesses. A user authenticates once with the SSO server, for example, when logging on to a network or an enterprise portal. When an application challenges a user for credentials, the SSO server intercepts the request and responds on behalf of the user. SSO servers work directly with Web-based applications intercepting HTTP traffic and responding to password requests. Legacy applications, however, typically require specialized, sometimes custom, code to implement SSO. Nonetheless it is seen that SSO technologies are greatly improving and innovating, moreover a consolidation of password management applications can be observed in the marketplace. SSO applications typically refer to the user management and access management components.

-Personalization:

Personalization and preference management tools allow application-specific as well as generic information to be associated with an identity. These tools allow applications to tailor the user experience for a given individual leading to a streamlined interface for the user and the ability to target information dissemination for a business [9].

Thanks to personalization IDM application users are enabled to adjust the IT system used to their own preference. Take for example a typical Intranet Web portal application within a large organization. Different users leads to different usage depending on their responsibilities. When they are enabled to personalize their access and use of the Web portal this generically leads to time savings, increased user experience, an increase of efficiency and in result a reduction in cost since less time is spent on starting up applications. Personalization applications have a strong user management context, increasing user experience and are also effective when deployed in a federated scenario.

-Self Service:

Enables users to self-register for access to business services and manage profile information without administrator intervention. It also allows users to perform authentication credential management: assigning and resetting passwords, requesting X.509 certificates, among others [9].
Some self service applications form a part of password management. For example, the resetting of passwords by users without having to contact an system administrator or help desk. Another example is password synchronization, these systems set all user passwords to the same word. Basically it synchronizes all the different passwords the user owns for a great variety of IT systems into one single password, resulting in an efficient, secure and quick access to a great variety of systems. Doing so saves the user from having to remember multiple passwords, but at a relatively high cost: If someone discovers the password to any one of those systems, that person has the password to all of them. Therefore it is often recommended to implement SSO instead.
Several business cases and research have shown that self-service component applications can dramatically reduce helpdesk calls and therefore increase efficiency and reduce IT costs.

Organizations today are feeling intense pressure to lower the costs of doing business while satisfying stakeholder demands for real-time, personalized access to sensitive information. Delivering information and services through a Web portal helps to foster strong relationships with customers, partners, employees or citizens. As well, leveraging a Web services architecture that integrates business processes both within the enterprise and between partners provides faster and more automated business processes. Self service applications are deployed for user management, facilitating access management and used effectively in a federated scenario.

2.3.3 Lifecycle Components

The lifecycle components have one main objective: fully manage, supervise and control the lifecycle of an identity.

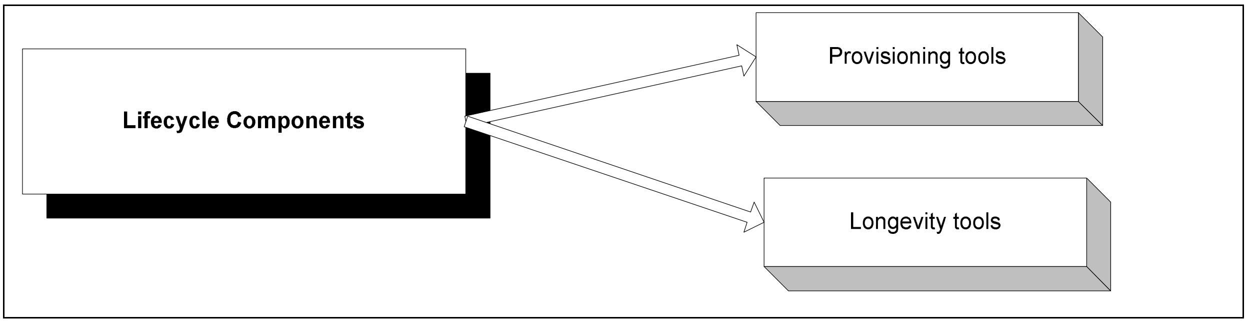


Figure 16: The lifecycle components represented.

In order to fully grasp the objective of these components let’s take a look at the concept of the so-called *ghost accounts*. Ghost accounts are accounts within the IT system that cease to be active but at some point are not eliminated. This often occurs to the lack of supervision of accounts (digital identities) in the system and as a result can lead to serious security problems. Imagine former employees who due to an administration failure still have access to enterprise resources. Therefore IDM lifecycle components focus on the control of the creation, propagation, maintenance and termination of digital identities which leads to increased internal control and a reduction in security risks. Moreover, accounting principles state that there must exist a clear separation of duties within a company, lifecycle components allow for just that; the creation of roles based on digital identities for a clear overview of duties and actions undertaken by each role (will be explained following).

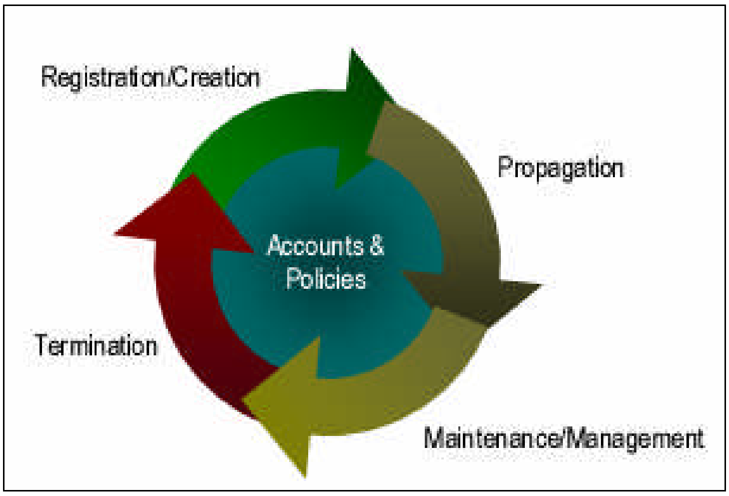


Figure 17: The process of identity lifecycle management. Lifecycle component enable total control over the creation, propagation, maintenance and termination of the identity [18].

- Provisioning:

Provisioning is the automation of all the procedures and tools to manage the lifecycle of an identity: creation of the identifier for the identity; linkage to the authentication providers; setting and changing attributes and privileges; and decommissioning the identity. In large systems, these tools generally allow some form of self-service for the creation and ongoing maintenance of an identity [9].

Typical provisioning functionality is coordinating the creation of user accounts, e-mail authorizations in the form of rules and roles, and other tasks such as provisioning of physical resources associated with enabling new users or disabling old users.

Industry standards for identity management and provisioning systems should include a workflow component. Workflow allows administrators to specify a sequence of events to add users based on the users' roles and the approval of others in the organization. The automated process ensures consistency and allows auditing of each step in the provisioning process.

The common return-on-investment (ROI) case for such identity management tools lies in a reduction of administrative workload combined. Other benefits are more consistent and auditable access policies, fewer unintended access/entitlement errors and legacy accounts (ghost accounts), and reduced delays in enabling/disabling user access to information and processing resources [22].

-Longevity:

Longevity tools create the historical record of an identity. These tools allow the examination of the evolution of an identity over time.
Longevity is linked to the concept of attestation (the act of witnessing the execution of an instrument) or the ability to attest what actors had access to what resources in what timeframe (irrespective of whether they exercised access, which is a matter of auditing) [9].
Longevity component applications focus on the total supervision of identity usage within the company. This functionality is effective for controlling who had access to what resources over time, in result this leads to an increase in security and a better overview of user privileges and actions.

2.3.4 Security Components

The security components focus on information security. They enable secure access to different IT systems and manage the integrity of data.

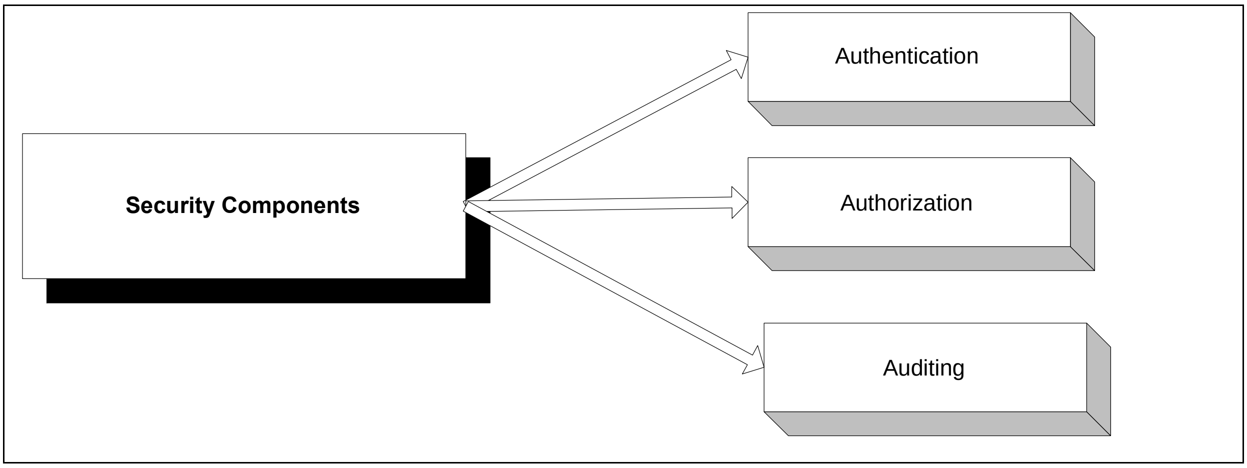


Figure 18: The security components represented.

The security components contain an access control part formed by three processes: identification, authentication and authorization. Identification is considered to be a part of the authentication tools. When a digital identity is supplied to the IDM system the authentication tools already incorporate an identification component.

The auditing component focuses on tools for auditing purposes and regulatory compliance. Nonetheless security components have extra added value apart from increased security. Enabling effective and quick access to IT systems also leads to better efficiency and cost reduction among others. The security components and their implications will be explained following.

-Authentication:

Authentication is the process of identifying an identity and establishing if that identity in fact is who he claims to be.

Authentication is central to information security because access to different IT systems must be properly verified [23]. Authentication is the following step after identification: first an identity must be supplied, then the authenticity of this identity can be established. Authentication services are crucial to authorization and auditing. If the true identity is not properly established the whole security infrastructure becomes ineffective, no matter how good it is. Following an overview of the most common authentication methods within the IDM framework is provided. These methods are stated in Gartner report on authentication [23]:

- *Passwords:*

  Passwords are a inexpensive and flexible solution for authentication. Within the IDM framework password management focuses completely on the management of this type of authentication. *PIN*, or Personal Identifiable Number are also considered a form of passwords.
- *Authentication Tokens:*

  This include hardware tokens such as *smart cards*, *USB tokens* and *OTP* (One Time Password) *tokens*.
- *Public Key Infrastructure*:

  Also referred to as PKI. It is an enterprise-wide framework that provides encryption-based security for a wide range of electronic transactions [12]. It is defined by Ford and Baum as [23] the set of infrastructural services that support the wide-scale use of public-key-based digital signatures and encryption.
- *Biometrics:*

  Biometric identification uses certain biological characteristics or behavioral traits of individuals to verify their identity electronically [23]. Typical biometric technologies are: fingerprint recognition, voice recognition, handwriting recognition, face recognition, retinal scan and hand geometry recognition, among others.

-Authorization:

The authorization component enforces access control when an identity accesses an IT resource. Enforcing access always depends on a established policy towards access and privileges. For example, an employee might be enabled to have access to a certain IT system depending on his privileges and the company's policy, the authorization components make sure he is granted (or denied) that access.

Role management plays an important part of authorization. Role management allows for better management of authorization by creating roles an then assigning identities to those roles, allowing to specify the resources users are allowed to access. Some example of created roles are manager, employee, sales, customer, etc.. *Role-based access control (RBAC)* has become an important part of identity and access management strategies. Driven by advanced technology and built on secure data repositories, the RBAC model provides a scaleable, enterprise-wide control process for managing IT assets and controlling user access according to their roles and the attributes attached to those roles. As users change roles within an organization, their access privileges to different applications change as well.

An authorization component can support simple access control management at the OS level, more sophisticated role-based access control (RBAC) up to flexible, distributed, policy-driven authorization, at the application and service levels [9]. Authorization components allow applications to make authorization and other policy decisions based on privilege and policy information stored in the repository [9].

-Auditing:

Auditing tools provide the mechanism to track how information in the repository is created, modified and used.

This is an essential enabler for forensic analysis, which is used to determine how and by whom policy controls were circumvented [9]. The auditing components relate to the longevity lifecycle component, but the difference is that the auditing components actually check which actions were undertaken and by whom instead of just controlling who had what privileges.

2.3.5 Data Repository Components

The big challenge concerning Identity Management remains how to aggregate and synchronize user identity information across multiple directories and identity stores in a heterogeneous environment. The result is to enable centralized administration of user identities across an organization's identity stores.

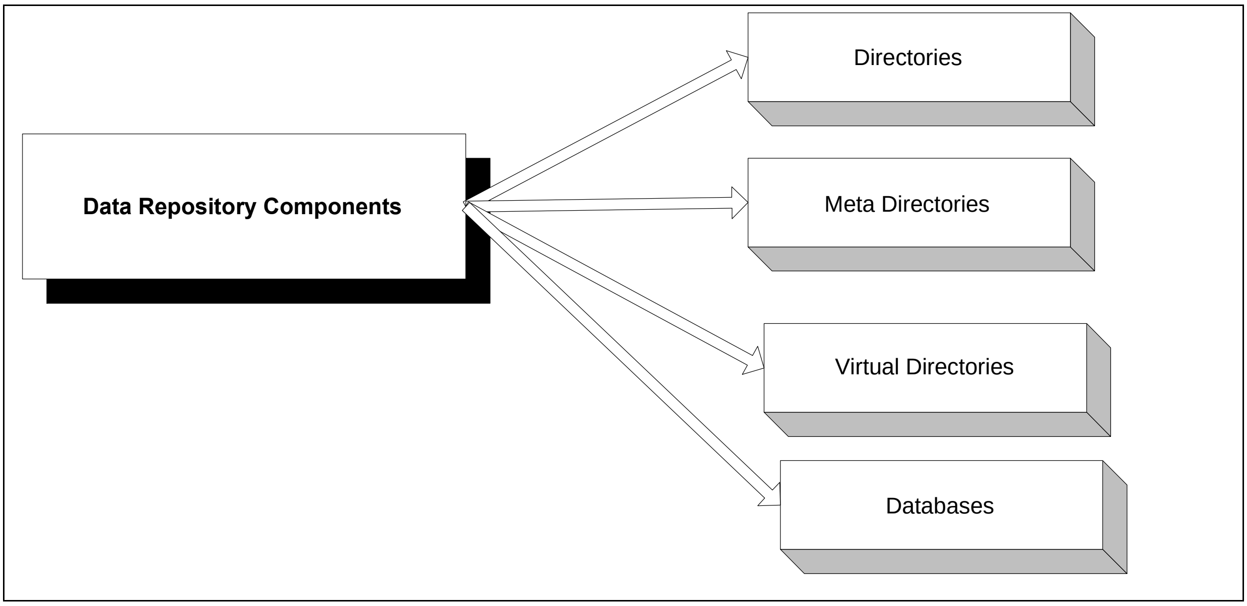


Figure 19: Data repository components represented.

Data repository components act as a central repository for user information by gathering data from enterprise applications. The repository components consolidate data from disparate applications, this process provides connectors to different applications and directories, allowing user data to be centrally managed by the Identity Management system. This process is also know as *directory integration services.* The following data repository components are mostly used:

-Directories:

The type of directory mostly used in an Identity Management System is that of a *LDAP (Lightweight Direct Access Protocol)* directory. LDAP (Lightweight Directory Access Protocol) is a software protocol for enabling anyone to locate organizations, individuals, and other resources such as files and devices in a network, it has proven to be quite effective and is therefore frequently used in an IDM context.

-Meta-Directories:

A meta-directory is a service that collects identity information from different data sources throughout an organization and then combines all or part of that information into an integrated, unified view [25].

-Virtual Directories:

Virtual directories solve a similar problem to meta-directories (access to scattered identity data) but it is a subtly different problem. a way of allowing applications access to existing identity data, when that data may reside in incompatible stores, with incompatible schemas and protocols. This is where the virtual directory comes in. Rather than sitting below the datastores (e.g. ldap directories), virtual directories fit between the datastores and applications that need to use them, smoothing out any schema or other compatibility issues [25].

-Databases:

A database is a collection of information stored in a computer in a systematic way, such that a computer program can consult it to answer questions. The software used to manage and query a database is known as a database management system (DBMS) [6].

2.4 Identity Management Standards

Standards play an important role by providing the common set of protocols, semantics, and processing rules that allow the various components of an identity management solution to interoperate. Following an overview of the most important current standards in Identity Management is provided.

The main IDM standards are [26]:

- *The World Wide Web Consortium (W3C):*
  Development of XML (Extensible Markup Language, SOAP (Simple Object Access Protocol) and HTTP (HyperText Transfer Protocol).
- *OASIS:*
  They have developed standards such as SAML (Security Assertion Markup Language), CIQ, DSML, SPML, XACML, XCBF, WSS.
- *Liberty Alliance:*
  Important project in IDM. Provided a framework and business models for Identity Management Federation.
- *WS*:*
  Developed a different concept of federation than Liberty Alliance. Responsible for numerous standards and models.
- *PRIME Project:*
  Addresses research issues of digital identity management and privacy in the information society. It’s an European initiative, started in March 2004 and will continue for four years.
- *Others*:
  New standards in IDM keep emerging.

2.5 Identity Management Systems

In the following section *Identity Management Systems* and their technological components are defined.

Identity Management Systems, a definition [4]:

> *The term "Identity Management System" (IMS) describes the infrastructure in which Identity Management Applications (IMA) as components are coordinated.*

The definition considers an IMS to be formed by logically constructed Identity Management Applications (IMA). The definition given above of *Identity Management Systems,* or *IMS,* will be used throughout the thesis. Observing the available products in the IDM market, a distinction can be made between two types of Identity Management Applications, *Point Identity Management Products* and *Full Suite Identity Management Solutions* [12]. In the following sections the both types of IMA are explained.

2.4.1 Point Identity Management Products

Point identity management products typically focus on delivering only part of a complete Identity Management infrastructure. Point Identity Management products must be integrated with each another to form an Identity Management System. For each of the described IDM components (see section 2.3 Identity Management Framework) a stand alone solution exists.

Point IDM products are developed by a great variety of producers, each with their own specialty area of IDM. It can be observed that the point IDM marketplace is consolidating. Some point IDM product vendors have been taken over by companies who wish to sell a complete range of IDM solutions and thus incorporate point IDM products into their product range.

The applications in this category include *Privacy Enhancing Technologies (PET)* that enhance the privacy and autonomy of users of existing applications. Privacy continues to gain ground as a mainstream business and consumer issue. These applications provide users with technology in order to guarantee their desired level of privacy and disclosure of personal data. Their main field of use is through the Internet, which includes services such as e-commerce, secure mailing, cookie managers, among others. *PET* products provide a stand alone solution for the maintenance of privacy.

2.4.2 Full Suite Identity Management Solutions

Full suite IDM solutions are a structured set of IDM solutions that together form a complete IDM framework. They provide complete Identity Management framework functionality, from user authentication to directory integration services.

Full Suite Identity Management solutions, feature components that, unlike point products, come pre-integrated by a single vendor and can therefore be deployed in supported configurations. This simplifies the deployment and integration process, and can dramatically reduce deployment costs. A complete and efficient Identity Management System can be deployed by using a full suite IDM solution.

The IDM marketplace has been changing in the past years, many full suite IDM vendors are taking over smaller, point IDM producing companies to further complete their own product or extend their range. In some cases, full suite solutions may also be available as individual components, for those companies who wish to focus on a specific component of the IDM framework.

CHAPTER 3: THE NEED FOR IDM

Chapter three elaborates on the need for Identity Management. The possible drivers for adoption of IDM solutions will be addressed and explained. The drivers will be based upon the benefits obtained from investing in IDM. Identity Management offers a great variety of benefits. Some of these benefits are improved efficiency, customer retention, legal compliance, among others. In this chapter it will be shown how widespread the scope of IDM is and the great variety of possible benefits will be discussed.

First of all a distinction is made between the two contexts of Identity Management (mentioned in section 2.1.3 Contexts of Identity) namely, consumer context and work context. From a consumer's point of view the need for IDM is different than from a business perspective. The need for Identity Management in both perspectives will be explained.

3.1 Consumer Perspective

Consumers have a specific need for IDM. They also benefit from the business benefits of IDM investment in a B2C[3] scenario (section 3.2). The main arguments for consumers for adoption of Identity Management solutions are *privacy* and *secure access control.*

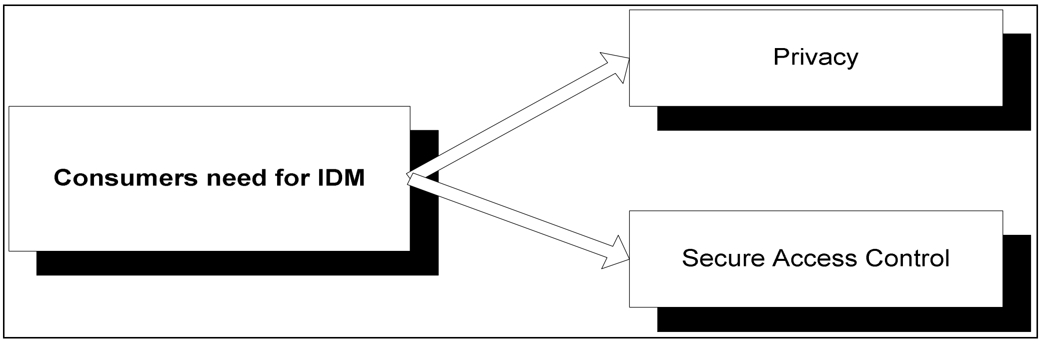


Figure 20: The consumers need for IDM

[3] B2C (Business to Consumer)

-Privacy:

Privacy is one of consumer's main issues when making use of the Internet. Online transaction, whether financial or exchange of information, could be greatly improved by the adoption of IDM solutions which focus on privacy. PET solutions (Privacy Enhancing Technologies) are such IDM applications. They range from secure mailing (using PKI or digital signatures) to anonymizing the IP address and even include P3P compliant browsers.

-Secure Access Control:

When making use of e-commerce, e-government, e-health, online banking, etc. secure access and confidentiality of data is of the utmost importance. For example, when using online banking, the consumer wants to feel secured by the IDM solutions adopted by the bank to guarantee safe access and confidentiality of data. Some of the aspects to achieve this are strong authentication models (often combining a variety of authentication methods) and enforcement of data protection, among others.

The consumer will ultimately benefit from the adoption of a good Identity Management System by businesses. For personal use, privacy enhancing technologies offer value added for the privacy aware consumer.

3.2 Business Perspective

The need for Identity Management from a business perspective will be based on the obtainable hard and soft benefits from an IDM investment. The following sections will analyze the hard and soft benefits [27] which give an incentive for adopting Identity Management.

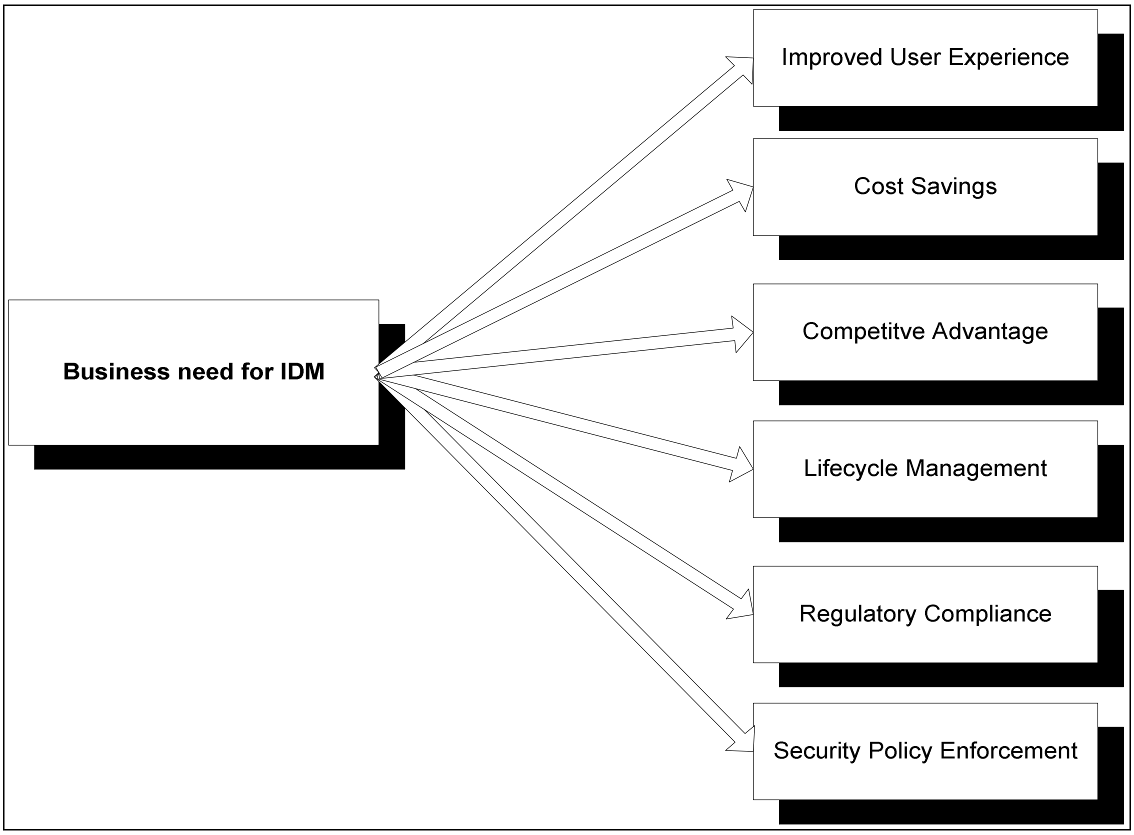


Figure 21: The business need for IDM [27].

3.2.1 Improved User Experience

Improved user experience is a benefit to be obtained from investment in Identity Management solutions. Identity Management applications enable users to increase their experience and in turn increase efficiency, productivity and customer retention and loyalty. The "users" are members of the company, customers, suppliers and other individuals who have access to the IT resources.

Following an overview of the main benefits and the IDM applications causing it [27]:

- SSO applications and other password management solutions often lead to an increase in *efficiency, productivity and time (costs) savings*. Users often posses a great variety of IDs and passwords, these applications substantially simplify this process.
- *Personalization* such as portal software and self-service solutions cause an increase in user experience.
- Simplified and personalized access leads to greater *customer loyalty and retention*.
- *Improved quality of experience (QoE)* due to the perception of ease of system accessibility.
- *User management* and *provisioning* benefit both system administrators as other users.
- *Federation* reduces the need to manage all user attributes and credentials on every system. This increases usability of the system and in turn cause strong alliances with the parties using the federation system.
- *Flexible remote access* permit users to access systems from a variety of locations. A good example of an IDM solution which allows for flexible remote access and improved user experience is the so called *Location Based Services*.

3.2.2 Cost Savings

The investment in Identity Management can lead (when done correctly) to a considerable reduction of operating costs (hard quantifiable benefit) and an improvement of productivity (soft benefit). Following an overview of the benefits to be obtained [27]:

- *Increased user productivity* and a *reduction of time:* Password management has shown to lead to a *reduction of help desk calls* for password related issues. A reduction of 30% to 90% have been shown in surveys. One enterprise estimates the reduction of time spent resetting passwords from an average of 17 minutes per incident to 2 minutes [27]. Estimated savings equals 15 minutes per password incident per user and can be extrapolated by factoring in the number of users and salary costs [27].
- *Centralization of user administration* over multiple systems caused by provisioning systems has led to a reduction of administrative costs.
- *Access to resources* are completed through automation in a matter of minutes or hours instead of days.
- Enterprises have calculated that application development time was reduced by 10% or more by integrating with a *directory service* instead of building unique security components into every application.
- Implementing an organized directory services architecture eliminates redundant directories and *reduces the administration burden*, thereby lowering the cost of operation.

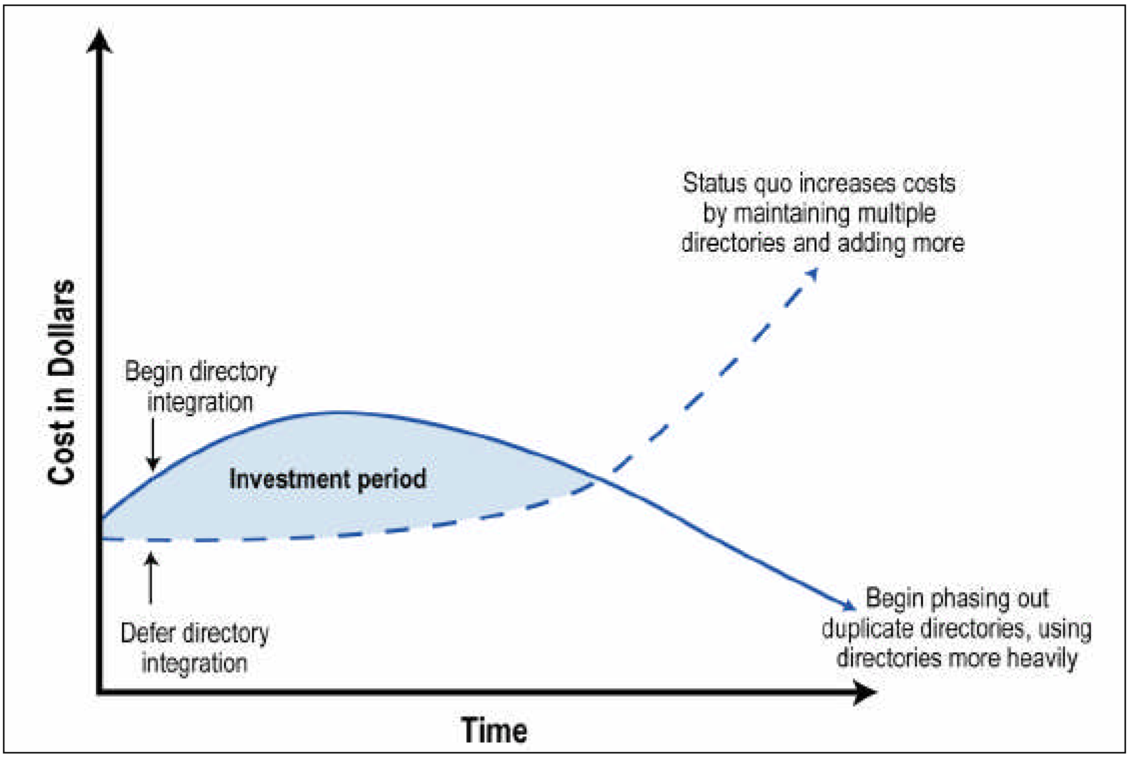


Figure 22: Costs savings realized by investing in directory integration schematically represented [27].

- *Identity federation* standards eliminate the need for proprietary point-to-point network and application connections to partner and supplier sites. Federation also reduces or eliminates the need to manage accounts for external users and reduces help desk calls from partners.

3.2.3 Lifecycle Management

The better management and administration of identity data thanks to IDM lifecycle components cause several business benefits. Some of the benefits of IDM lifecycle components such as provisioning and role management have been introduced in section 2.3 Identity Management Framework. This section provides an overview of the benefits [27]:

- *Reduction* in the potential for *errors, redundancies,* and *omissions* in identity data across systems thanks to the lifecycle components that provide a structured and clear overview of identity data. Ghost accounts become non existent, thus reducing the potential for fraud.
- *Automation* in management of the lifecycle of an identity. *Provisioning* systems and *role management* allow for better management of identities and delegation of administrative responsibilities.
- *Increase in logging and auditing capabilities.* The IDM solution help to improve internal control, determining inventory, auditing, detection and/or prevention of fraud, among others.

3.2.4 Competitive Advantage

The adoption of Identity Management technology can lead to competitive advantage for the investing company. Taking into account that Identity Management is still considered to be relatively new and the market is still innovating, this can lead to a considerable advantage gained over competitors when successfully adopting IDM in comparison with the competition. Following an overview of aspects that cause competitive advantage [27]:

- *Rapid deployment* of applications is caused by the presence of an IDM framework.
- Due to better *internal control* some actions such as mergers, acquisitions, and divestitures can be carried out more effectively and quicker.
- *Federation* causes better relationships with external parties, giving an advantage over other companies.
- *Increased customer satisfaction* and *retention* thanks to personalization and self service components.

3.2.6 Security Policy Enforcement

Strong enforcement of the company's policy is essential for business operation and compliance. Following an overview of the benefits [27]:

- Ability to demonstrate *legal compliance* (see section 3.2.6).
- For financial institutions, lower operating capital levels are awarded to enterprises that can show advanced security control systems.
- Secure *access control* leads to better maintenance of sensitive resources and intellectual property.
- Centralized *authorization* framework provides consistent implementation of security policy.
- *Federation* allows for mitigation of risks.

3.2.6 Regulatory Compliance

One of the main drivers for adoption of Identity Management is regulatory compliance. In this section the main legal and regulatory implications that give an incentive for investment in Identity Management will be addressed.

Regulations governing customer privacy (in the health care, financial and retail industries), sound business processes and good corporate governance (publicly traded companies) generally require basic security practices: the ability to securely authenticate users; the ability to control user access to sensitive systems; the ability to ensure that user access to systems and data is only granted when appropriate; and the ability to measure and prove all of the above.

The vast majority of laws and regulations address privacy, integrity of data and access control to data. There has been a shift from the traditional model based on “tell me” and “show me” towards a new standard based on “prove me”. Compliance is a matter of proof nowadays, companies are obliged to demonstrate that laws and regulations are met. Following an overview will be given of the main laws and regulations [29] that relate to Identity Management:

-BASEL II:

In 2003 the BASEL Committee on Banking Supervision (the Committee) outlined the framework of 10 sound practice principles for managing operational risk . These principles include: board oversight. regular monitoring, policies and practices to control and mitigate operational risk, periodic review of risks and controls, adjustment of risk management strategies, public disclosure of operational risk to the market [29].

-California Senate Bill 1386:

In 2002, the State of California enacted Bill Number: SB 1386 requiring state agencies, and others who conduct business through computerized collection of personal information, to immediately disclose any breach of data security to any California resident whose personal information may have been compromised [29].

-FISMA (Federal Information Security Management Act):

The act of 2002 (FISMA) was enacted in the United States in 2002. It provides a framework to ensure comprehensive measures are taken to secure federal information and assets [29].

-GLBA (Gramm Leach Bliley Act):

The GLBA is a comprehensive law requiring financial institutions to protect the security, integrity, and confidentiality of consumer information [29].

-HIPAA (Health Insurance Portability and Accountability Act):

The act of 1996 (HIPAA) mandates that providers, health plans, clearinghouses, and their business associates establish appropriate administrative, technical and physical safeguards to protect the privacy and security of sensitive health information [29].

-BS 7799:

The Information Security Management System Specification, BS 7799, sets the standard for handling the Confidentiality, Integrity and Availability (CIA) of information. BS 7799 was developed as a result of industrial, governmental and commercial demands for a common framework enabling companies to develop, implement, and effectively measure security management practices and to inspire confidence in inter-company trading [30]. Information Security is designed to protect something of value against unauthorized access and changes. BS 7799 refers to protection of information in terms of [30]:

- Confidentiality: only authorized users can gain access to relevant information.
- Integrity: accuracy and completeness of information and processing methods.
- Availability: information is available when required in the correct context.

-ISO 17799:

The ISO organization has developed a guideline ISO/IEC 17799:2000 as a "Best Practice" for implementing Information Security. These guidelines elaborate on the requirements in BS 7799-2:2002 which remains the specification used for certification [30]. ISO 17799 is intended to serve as a single reference point for identifying the range of controls needed for information systems used in industry and commerce. ISO 17799 requires processes to ensure that the security controls for a system are fully commensurate with its risks [29].

ISO 17799 requires the existence of a system for:

- Monitoring access to IT systems.
- Retaining integrity.
- Establishing sufficient audit trails to address threats or problems.
- Reporting material events to both upper manage and board of directors.

-PCI (Payment Card Industry Data Security Standard):

Sponsored by collaboration between MasterCard, Visa, American Express, Diners Club and the Discover Card, the Payment Card Industry Standard (PCI) is an effort to protect consumer information and fight Internet fraud through required best practices for securing credit card data that is stored, processed, or transmitted by an online retailer [29].

-Sarbanes-Oxley:

The Sarbanes-Oxley Act (often shortened to SOX) of 2002 passed in the U.S.A. is legislation enacted in response to the high-profile Enron and WorldCom financial scandals to protect shareholders and the general public from accounting errors and fraudulent practices in the enterprise [28]. Specifically, under Section 404 of the Sarbanes Oxley Act, executives need to certify and demonstrate that [29]:

- Files containing accounting information have not been compromised.
- All significant technical controls, including security authorizations and critical configuration files have not been compromised.

Identity Management components effectively tackle the demands of SOX by improving overall security and access, and by improving internal control.

-US Patriot Act:

After 9-11, Congress passed the Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001 (USA PATRIOT Act) to fight terrorism and protect our financial systems from terrorist money laundering schemes and other acts of terrorism. This Act made it critical for financial institutions to verify the identity of customers. As a result, security plays a vital role for compliance under the USA Patriot Act [29].

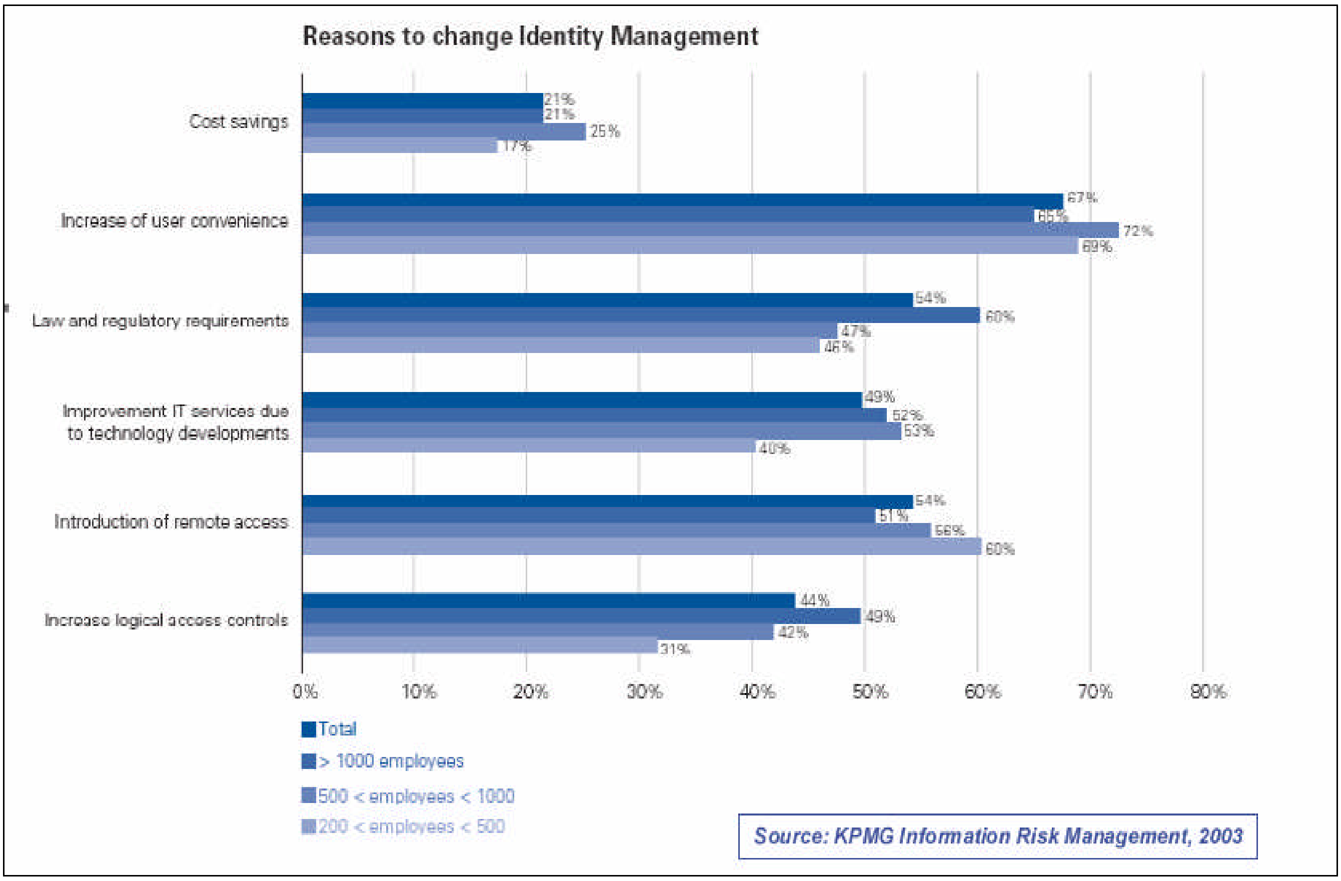
-European privacy laws, upcoming laws on data protection and other future legislation:

Identity Management should take into account future legislation and therefore the market keeps innovating.

3.2.7 Research on IDM Investment

KPMG conducted research on he reasons for investing in Identity Management among a number of companies in 2003 [8]. IT managers from a number of companies were sent a questionnaire which they had to fill out, in order to observe what the main drivers are for IDM adoption. A range of companies were interviewed, ranging from less than five hundred employees up to more than a thousand employees. In Figure 23 the outcome of the research can be observed. What is noticeable is that most managers did not mention cost savings as there primary reason for IDM adoption (a total of 21%). This is due to unawareness among IT managers of the effects IDM adoption can have on cost reduction as was described earlier in this section. An emphasis can be observed on increasing user experience, regardless what size the company is. IDM can play a key role in increasing customer loyalty as well as increasing user productivity, this is acknowledged by most IT managers. Another striking fact is importance that is given to regulatory compliance and federation (remote access). It has become increasingly important to meet laws and regulations and form strong and secure alliances with partners through federated services.

By observing the outcome of the research in Figure 23 the benefits explained in the previous section are reflected.



Source: KPMG Information Risk Management, 2003

Figure 23: Research conducted by KPMG [8] among companies on the reasons for investment in Identity Management.

CHAPTER 4: THE IDM POSITIONING MODEL

Chapter four provides an explanation of the IDM positioning model. Different type of businesses have distinct characteristics such as strategic objective, size and information need. This differences result in different benefits to be obtained from an investment in Identity Management. The IDM positioning model is developed to define what the specific IDM focus should be of different types of enterprises. The model provides a categorization of different types of businesses. For each of these types the model determines a specific Identity Management approach. The positioning model is based on the strategic analysis report The Price of Information Security [15] developed by Gartner Inc. .

4.1 Creating The IDM Positioning Model

Investing in Identity Management becomes a real issue for companies nowadays. However, the Identity Management marketplace is often quite unclear for managers responsible for IT investment. Different types of companies have distinct needs, depending on strategic objective, size and information need. In order obtain the desirable benefits from an investment in Identity Management, the solutions acquired must meet the specific needs of the enterprise.

The positioning model described in chapter four provides a categorization of different types of businesses. For each of these types, the model states on what component of the Identity Management framework the business should focus (see section 2.3 Identity Management Framework) in order to obtain the desirable benefits (see section 3.2 Business Perspective). Figure 24 provides an overview of how the IDM positioning model is structured.

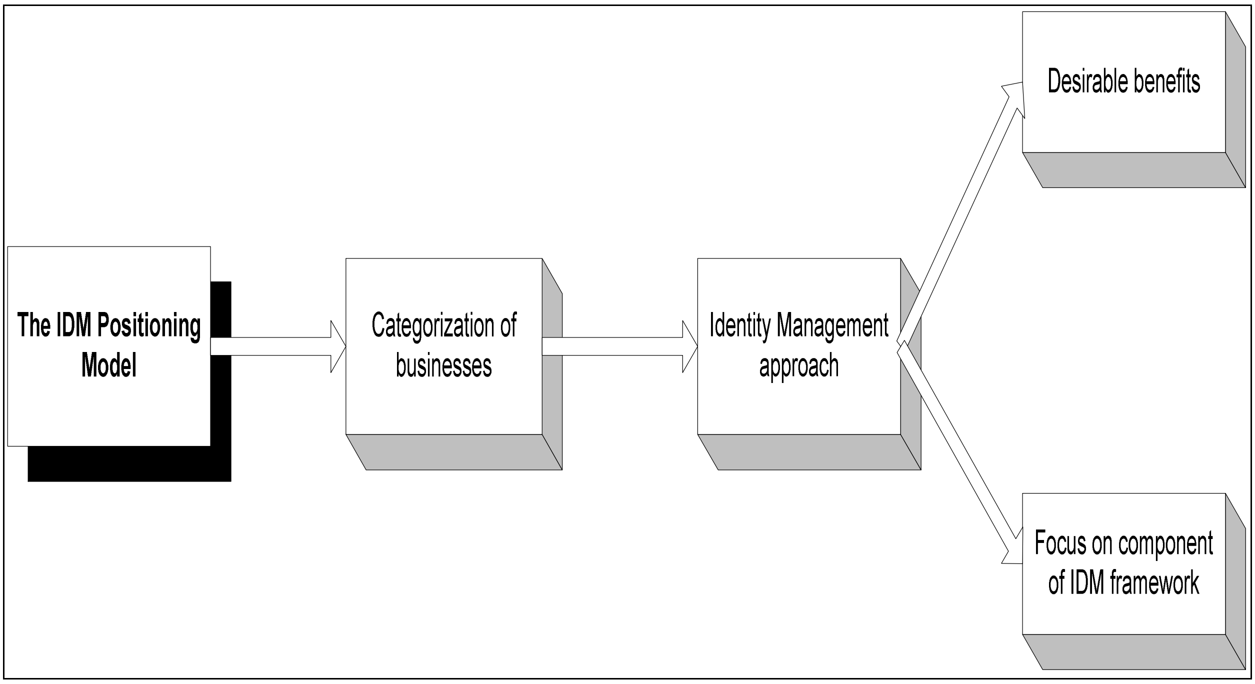

The IDM Positioning Model
Categorization of businesses
Identity Management approach
Desirable benefits
Focus on component of IDM framework

Figure 24: An overview of the structure of the IDM positioning model.

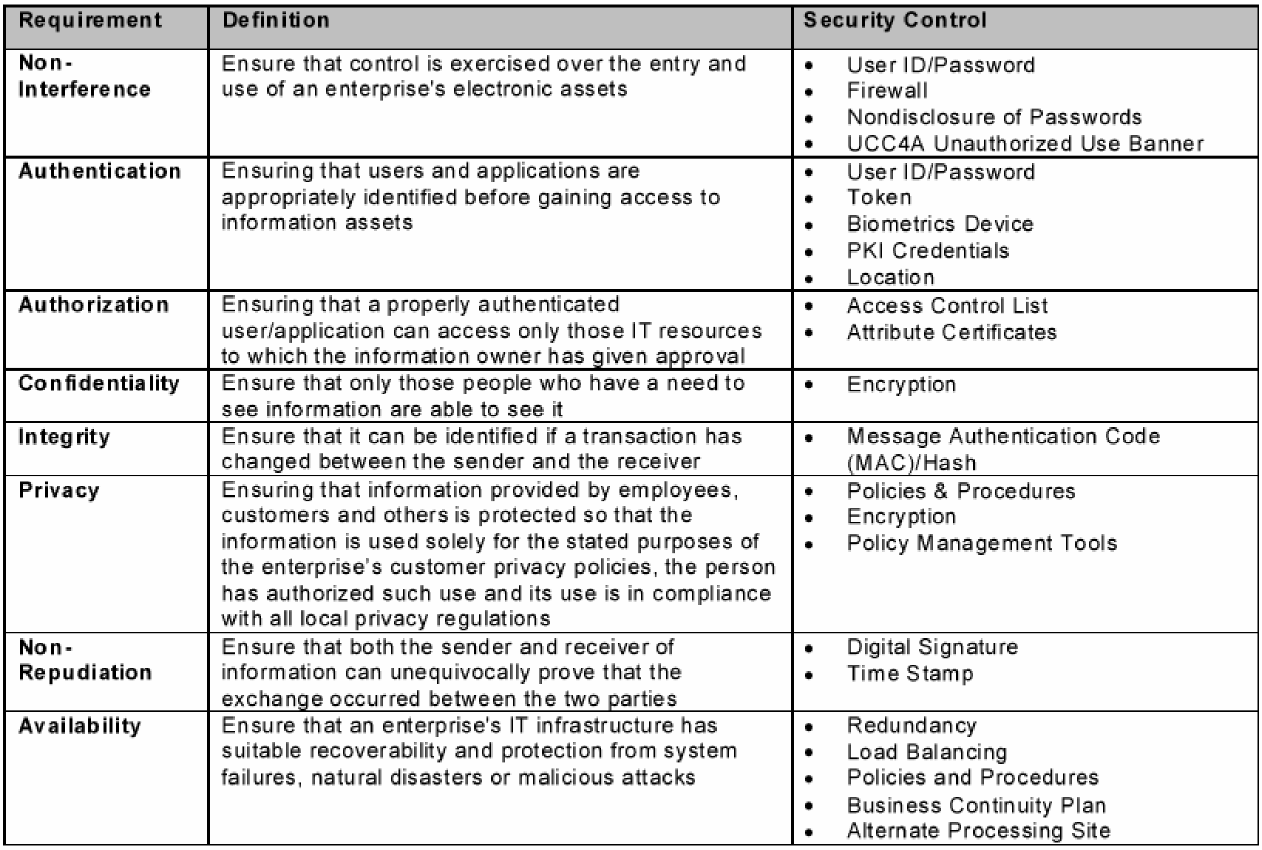
The model enables IT investment decision makers to determine what the appropriate IDM approach is for their business by describing the desirable benefits to be obtained and the specific IDM component they should focus on. This is achieved by determining to which category (described in the model) their business belongs too. Each category is determined by a collection of characteristics. A business belongs to a category when it best fits the characteristics of that specific category.

The model is based upon the paper *The Price of Information Security* [15] by *Gartner Inc.*. The paper analyzes the Total Cost of Ownership (TCO) of investing in information security. It looks at a variety of aspects within a company concerning information security. Basically it describes "*best practices for information security expenditures, including the costs for people, hardware, software, external services and physical security for all information security activities in which an enterprise might be engaged*" [15].

Identity Management is an essential part of Information security. Information security comprises several IDM components such as access management, security components, privacy and federation management (see section 2.3). Legislation and regulation also play an important role in information security, it is observed that nowadays the emphasis lies on *proving* that a company is in compliance. One component of the definition of Identity Management (see section 2.2.2 Definition) consists of managing information about (digital) identities. Much like other information security methods, IDM is a structured methodology of managing information assets. Therefore there is a clear link between the research objective discussed in the paper The Price of Information Security [15] and Identity Management.

The paper The Price of Information Security [15] was chosen for the following reasons:
First of all because information security is an important aspect of Identity Management. Many principles in information security apply to IDM. Identity Management forms an integral part of information security. The Information Security Management System Specification has set the standard for handling of information. The standard is implemented in IDM solutions, therefore the objective of the paper directly relates to the content of this thesis.
Secondly, because in the paper a classification of enterprises is made based on information security. The classification is made based on the need for information security solutions of different businesses. This need is based on IT control requirements defined in the paper. IDM solutions enable businesses to meet these requirements. The classification provided by Gartner will be used, extended with other factors influencing the Identity Management investment decision. These factors are desirable benefits to be obtained from IDM solutions and regulatory compliance.
Last but not least, the paper was chosen due to the good reputation of Gartner Inc.. Gartner [31] provides research and analysis of information technology companies, products, and services, and of several industry sectors. Their custom research and consulting services are widely recognized in the Information Technology industry. Gartner offers the combined brainpower of more than 1,200 research analysts and consultants who advise executives in 75 countries every day.

In the paper [15] Gartner Inc. distinguishes between a number of aspects that have to be taken into account when investing in information security. The IT control requirements for information security are among these aspects. The IT control requirements are a list of information security controls needed to adequately and comprehensively protect an enterprise. Figure 25 depicts an overview of the IT control requirements described in the paper.



Requirement	Definition	Security Control
Non-Interference	Ensure that control is exercised over the entry and use of an enterprise's electronic assets	• User ID/Password • Firewall • Nondisclosure of Passwords • UCC4A Unauthorized Use Banner
Authentication	Ensuring that users and applications are appropriately identified before gaining access to information assets	• User ID/Password • Token • Biometrics Device • PKI Credentials • Location
Authorization	Ensuring that a properly authenticated user/application can access only those IT resources to which the information owner has given approval	• Access Control List • Attribute Certificates
Confidentiality	Ensure that only those people who have a need to see information are able to see it	• Encryption
Integrity	Ensure that it can be identified if a transaction has changed between the sender and the receiver	• Message Authentication Code (MAC)/Hash
Privacy	Ensuring that information provided by employees, customers and others is protected so that the information is used solely for the stated purposes of the enterprise's customer privacy policies, the person has authorized such use and its use is in compliance with all local privacy regulations	• Policies & Procedures • Encryption • Policy Management Tools
Non-Repudiation	Ensure that both the sender and receiver of information can unequivocally prove that the exchange occurred between the two parties	• Digital Signature • Time Stamp
Availability	Ensure that an enterprise's IT infrastructure has suitable recoverability and protection from system failures, natural disasters or malicious attacks	• Redundancy • Load Balancing • Policies and Procedures • Business Continuity Plan • Alternate Processing Site

Figure 25: Overview of IT control requirements described in *The Price of Information Security* [15] by Gartner Inc..

The IT control requirements depicted in Figure 25 indicate possible information security risks. If one of the controls is breached or not met this implies a breach in the information security of the enterprise. In Figure 25 security controls are mentioned to meet the IT control requirements. The IDM positioning model updates these security controls with technological IDM features (described in section 2.3 Identity Management Framework) depending on the desirable benefits to be obtained.

Gartner Inc. [15] categorizes enterprises into five different types depending on their need for information security solutions based on their characteristics. All types have different information needs, risks and threats. The characteristics of the businesses need for information security is based on a set of categories [15]:

- *Use of IT for Business Processing*: The extent to which an enterprise uses IT for mission-critical business processing.
- *Technology Profile*: The types of technology used by an enterprise, ranging from stand-alone PCs to mainframes.
- *Trust Establishment*: The process used by an enterprise to establish a relationship with its business partners, i.e., "Know Your Customer".

- *Information Asset Value Outside of the Enterprise, or "Hacker Value"*: The value to a hacker/external party of an enterprise's information assets if its infrastructure is infiltrated
- *Information Security Coverage*: The personnel and controls in place to protect the information assets of an enterprise
- *Security Breach Impact*: The impact on an enterprise if a security breach occurs.
- *Business Continuity Coverage*: The level of disaster recovery and business continuity plans in place for an enterprise to recover from a disaster/emergency rendering its production site(s) inoperable for a defined period of time.
- *Disaster Impact*: The impact on an enterprise if a disaster/emergency occurs.

Based on the characteristics enterprises posses in each of the above mentioned categories, Gartner defines five types of enterprises [15]:

1. Small business with slow growth.
2. Small/midsize business (SMB) with fast growth.
3. Dot-Com enterprise.
4. Middle-market retail.
5. Financial institutions, large multinationals and institutions holding sensitive information for others (e.g. social security administration).

Each of these types has a distinct profile based on their information security needs.\The five types mentioned above are the five types of businesses defined in the IDM positioning model. The characteristics of the five types of are determined in the literature [15] according to their need for information security solutions. The IDM positioning model further elaborates the profile of the five types by focusing on desirable benefits to be obtained from an Identity Management investment. The KPMG research on IDM investment [8] (see section 3.2.7 Research on IDM Investment) stated an overview of the main reasons for adoption of IDM among different companies varying in size. These results have been taken into account when constructing the positioning model. The reasons for adoption stated in the research are part of the desirable benefits of each of the different types of businesses.

In the following section the IDM positioning model is provided and explained.

4.2 The IDM Positioning Model

The following table depicts the IDM positioning model:

THE IDM POSITIONING MODEL			
Type	**Description**	**Desirable Benefits**	**Focus on IDM Component**
1.	Small business with slow growth.	• Improve IT infrastructure. • Increase user experience.	• Data repository component. • Personalization components.
2.	Small/midsize business (SMB) with fast growth.	• Improve IT infrastructure. • Improve user experience. • Increase internal control.	• Data repository component. • Personalization components. • Lifecycle components.
3.	Dot-Com business.	• Adhering to privacy regulations and proof compliance. • Improve user experience. • Competitive advantage.	• Security components. • SSO, Personalization and self service components.
4.	Middle-market retailer.	• Competitive advantage. • Improve user experience. • Cost savings. • Centralized administration.	• Directory integration. • SSO, personalization and self-service. • Lifecycle components.
5.	Financial institutions, large multinationals and institutions holding sensitive information for others.	• Increase internal control. • Security policy enforcement • Cost savings. • Improve user experience, productivity and efficiency. • Form strong alliances through federation.	• Consumable value components. • Lifecycle and security components. • Data repository component. • Federation Management.

-Explanation of the model:

The IDM positioning model consists of four parts: type, description, desirable benefits and focus on IDM component. The type depicts the category of business described. The description part supplies a sample enterprise which fits the characteristics of the specified type. The desirable benefits depict the benefits to be obtained from an investment in IDM. The final part depicts on what components of the IDM framework the business should focus on.

Five types of enterprises have been determined based on the Gartner research on the need for information security solutions among different types of businesses. The five types of businesses are [15]:

1. Small business with slow growth.
2. Small/midsize business (SMB) with fast growth.
3. Dot-Com enterprise.
4. Middle-market retail.
5. Financial institutions, large multinationals and institutions holding sensitive information for others (e.g. social security administration).

Each of these types has a distinct profile based on their need for information security solutions which is based on the Gartner research [15]. The characteristics of the businesses need for information security is based on a set of categories described in section 4.1 Creating The IDM Positioning Model. Moreover, based on their characteristics a number of desirable benefits are determined. In order to reach these benefits the business should focus on a specific part of the Identity Management components. This focus is stated in the model. Following each of the specified types is explained:

-Type 1:

Characteristics based on Gartner research based on the need for information security controls [15]:

Sample enterprise:

Small business with slow growth.

Use of IT for Business Processing:

Strong paper trail.

Technology Profile:

PCs, NT or Novell. Internet used for e-mail, research, purchase of supplies, usually through dial-up access, cable modem or DSL.

Trust Establishment:

Personal recognition.

Hacker Value:

Vulnerable as a hacker launch-pad (nothing worth stealing).

Information Security Coverage:

No information security expertise in house. Virus protection may or may not be in place. Majority of security protection is through physical security controls.

Security Breach Impact:

Limited damage due to lack of enough mission-critical IT processing.

Business Continuity Coverage:

No disaster recovery/business continuity plans in place.

Disaster Impact:

Major damage, up to and including business failure.

Profile:

The profile of the type of enterprise is constructed based on a summary of the characteristics of the need for information security controls.

The type 1 enterprise represents those enterprises small in size with no strong growth expectations in the near future. Business processing is accomplished through a strong paper trail. Most commercial activities are documented without the use of IT systems. The use of IT is focused on communication through the use of e-mail and research, and other components of non-critical business activities such as online purchasing. The relationship with business partners is established through personal recognition, no formal procedures to enforce trust with other parties is established. The enterprise's information assets do not represent a substantial value for hackers or external parties when the IT infrastructure is infiltrated. In result no serious damage is done to the business processing in case information security is compromised. No recovery plans are in place in case business continuity is uncertain due to external factors. The impact a disaster has on the business is great and could lead up to business failure.

Desirable Benefit and Focus On IDM Component:

Based on the analysis of characteristics of the Gartner research [15] the desirable benefits to be obtained from an investment in Identity Management solutions is determined:

- Improve IT infrastructure > Invest in data repository component:

  The IT infrastructure of the type 1 enterprise is loosely organized. Even tough no critical business processes are done trough the use of IT, benefits can be obtained from investing in a data repository component. The use of a database which centrally stores all business processing information will considerably reduce the strong paper trail. In turn, this will lead to a central storage point of information. A central reference point simplifies access for users and in turn reduces potential security threats.

- Increase user experience > Personalization components.

IT systems are used for non critical business processing. If the use of IT is increased for business processes such as research and purchasing, this leads to higher efficiency. Moreover, by implementing personalized web access linked to all necessary information and to the data repository component, simplifies the use of the system and yields higher user productivity.

-Type 2:

Characteristics based on Gartner research based on the need for information security controls [15]:

Sample enterprise:

Small/midsize business (SMB)/fast growth.

Use of IT for Business Processing:

Strong paper trail.

Technology Profile:

PCs, NT or Novell. Internet used for e-mail, research, purchase of supplies, usually through dial-up access, cable modem or DSL.

Trust Establishment:

Personal recognition.

Hacker Value:

Vulnerable as a hacker launch-pad (nothing worth stealing).

Information Security Coverage:

Information security expertise through system administration. Limited information security controls on internal systems, e.g., virus protection, desktop firewalls on PCs with cable modem and access to the Internet. Majority of security protection is through physical security controls.

Security Breach Impact:

Limited damage due to lack of enough mission-critical IT processing.

Business Continuity Coverage:

No disaster recovery/business continuity plans in place.

Disaster Impact:

Major damage, up to and including business failure.

Profile:

The profile of the type of enterprise is constructed based on a summary of the characteristics of the need for information security controls.

The type 2 enterprise represents those small, midsize enterprises going through strong growth. Business processing is in general, accomplished through a strong paper trail. Some commercial activities are documented without the use of IT systems. The use of IT is focused on communication through the use of e-mail and research, and other components of non-critical business activities such as online purchasing. Due to the strong growth there is some level of account management in place, although the security controls on internal systems are limited. Security controls are based on virus protection and firewalls. The relationship with business partners is established through personal recognition, no formal procedures to enforce trust with other parties is established. As the number of users of the IT system grow, it becomes increasingly difficult to maintain control over user access to systems. The enterprise's information assets do not represent a substantial value for hackers or external parties when the IT infrastructure is infiltrated. In result no serious damage is done to the business processing in case information security is compromised. No recovery plans are in place in case business continuity is uncertain due to external factors. The impact a disaster has on the business is great and could lead up to business failure.

Desirable Benefit and Focus On IDM Component:

- Improve IT infrastructure > Invest in data repository component:

  Even tough no critical business processes are done trough the use of IT, benefits can be obtained from investing in a data repository component. The use of a database which centrally stores all business processing information will considerably reduce the strong paper trail. In turn, this will lead to a central storage point of information. A central reference point simplifies access for users and in turn reduces potential security threats.
- Increase user experience >Invest in personalization components.

  IT systems are used for non critical business processing. If the use of IT is increased for business processes such as research and purchasing, this leads to higher efficiency. Moreover, by implementing personalized web access linked to all necessary information and to the data repository component, simplifies the use of the system and yields higher user productivity.
- Increase internal control > Invest in lifecycle components:

  Due to the fast growth of the type 2 enterprise the numbers of users of the IT systems can grow exponentially. Therefore it becomes a difficult task for the system administrators to maintain an overview of personnel accessing the system. Proofing which individual has access to what resources becomes virtually impossible. An investment is IDM lifecycle components provides the tools to achieve increased internal control. The provisioning and longevity tools supply system administration with an overview of the creation, propagation, maintenance and termination of digital identities within the system.

-Type 3:

Characteristics based on Gartner research based on the need for information security controls [15]:

Sample enterprise:

Dot-Com enterprise.

Use of IT for Business Processing:

Many transactions only exist in electronic form.

Technology Profile:

PCs, NT, Novell, Unix. Internet used for B2B/B2C, e-mail, research, purchase of supplies, etc.

Trust Establishment:

Formal procedures, contracts, pursuing use of PKI.

Hacker Value:

Attacker stays when security is breached, i.e., enough to steal here.

Information Security Coverage:

Information security expertise through consultant, system administration and external audit. Limited information security controls, mostly on external systems, e.g., virus protection, Web apps, firewall, proxy server, Web filter.

Security Breach Impact:

Major damage due to all mission-critical processing done on IT.

Business Continuity Coverage:

Disaster recovery plan for Web server(s) may be in place with external service.

Disaster Impact:

Major damage, up to and including business failure.

Profile:

The profile of the type of enterprise is constructed based on a summary of the characteristics of the need for information security controls.

The type 3 enterprise represents those businesses that focus on e-commerce. Their strategic objective is to perform commercial activities through the use of the Internet. Business processing is in general, accomplished through the use of IT systems. Most transactions only exist is electronic form. The use of the Internet is extensive; from B2B and B2C purposes to research, communication and purchasing activities. The relationship with business partners is established through formal procedures, contracts and in some cases PKI is implemented. Information security plays an important role and expertise is often outsourced. Internal control is limited and mostly based on external systems. Some examples are: virus protection, Web apps, firewall, proxy server, Web filter. The enterprise's information assets represent a substantial value for hackers or external parties when the IT infrastructure is infiltrated. In result, serious damage is done to the business processing in case information security is compromised. Business recovery plans focus primarily on the maintenance of the Web server, which is considered critical to business processing. The impact a disaster has on the business is great and could lead up to business failure.

Desirable Benefit and Focus On IDM Component:

- Adhering to privacy regulations and proof compliance > Invest in security components.

Due to the use of the Internet for e-commerce purposes, proofing compliance to privacy regulations is of the utmost importance. Access to resources by consumers and employees must be thoroughly controlled. Authentication, authorization and auditing tools provide the possibility of enforcing secure access and proof compliance to regulations.

- Improve user experience and competitive advantage > Invest in consumable value components:

Achieving customer retention and loyalty is essential for the type 3 business. Because of the non-physical aspect of the e-commerce activities, special emphasis is needed on the IT system. The system (Website) provide the same functions a physical shop would provide in a traditional commerce model. To achieve this goal an investment is needed in consumable value components, namely: SSO, personalization and self-service components. This will benefit both customer as employees, increase the user satisfaction and ultimately user experience. Greater customer retention and loyalty means that more customers are willing to use the services of the enterprise which increases market share and in turn leads to a competitive advantage.

-Type 4:

Characteristics based on Gartner research based on the need for information security controls [15]:

Sample enterprise: Middle-market retail.

Use of IT for Business Processing:

Limited paper trail; majority of business processing done on IT.

Technology Profile:

PCs, NT, Novell, Unix. Internet used for e-mail, research, purchase of supplies, usually through ISP, starting to get into B2B and B2C.

Trust Establishment:

Personal recognition and trade relationships, contracts.

Hacker Value:

Attacker stays when security is breached, i.e., enough to steal here.

Information Security Coverage:

Information security expertise through consultant, system administration, internal audit. Information security controls on internal and external systems, e.g., virus protection, access control at system level/application level, remote access, Web apps, firewall,
proxy server, Web filter.

Security Breach Impact:

Major damage due to all mission-critical processing done on IT.

Business Continuity Coverage:

Disaster recovery plans in place for some departments.

Disaster Impact:

Major damage, up to and including business failure.

Profile:

The profile of the type of enterprise is constructed based on a summary of the characteristics of the need for information security controls.

The type 4 enterprise represents the middle-market retailers. They are depicted by considerable size and a variety of IT systems and users. Their strategic objective is to perform commercial retailing activities, based on trade. Business processing is in general, accomplished through the use of IT systems and there exists limited paper trail. The use of the Internet is extensive; from B2B and B2C purposes to research, communication and purchasing activities. The relationship with business partners is established through formal procedures, trade relationships and contracts. Information security plays an important role. Information security is accomplished through outsourcing of expertise, system administration and internal audits. Controls are in place on both internal and external systems. Access control is established at the system level. The enterprise's information assets represent a substantial value for hackers or external parties when the IT infrastructure is infiltrated. In result, serious damage is done to the business processing in case information security is compromised. Business recovery plans are in place for some of the department, although not defined enterprise wide. The impact a disaster has on the business is great and could lead up to business failure.

Desirable Benefit and Focus On IDM Component:

- Centralized administration > Invest in directory integration:

The type 4 enterprise characterizes itself by a variety of IT systems containing sensitive information critical to business processing. Information is often stores on a variety of directories connected to the different systems. By investing in directory repository components the different directories can be integrated en access to the different systems will be considerably simplified. A central repository components makes it possible to adequately control access to resources and protect sensitive data.

- Competitive advantage, cost savings and improved user experience > Invest in consumable value components and lifecycle management components:

To achieve this goal an investment is needed in consumable value components, namely: SSO, personalization and self-service components. This will benefit both customer as employees, increase the user satisfaction and ultimately user experience. Greater customer retention and loyalty means that more customers are willing to use the services of the enterprise which increases market share and in turn leads to a competitive advantage. Moreover, investing in SSO yields rapid and efficient access to the different system which in turn yields cost savings.

An investment in the lifecycle components will considerably reduce the workload of the system administration and in turn lead to cost savings. In addition, internal control and auditing capabilities are increased through a structured overview of the lifecycle of the digital identities.

-Type 5:

Characteristics based on Gartner research based on the need for information security controls [15]:

Sample enterprise:

Financial institutions, large multinationals and institutions holding sensitive information for others (e.g. social security administration).

Use of IT for Business Processing:

Many transactions only exist in electronic form.

Technology Profile:

PCs, NT, Novell, Unix, Mid-Range, Mainframe Internet used for B2B/B2C, e-mail, research, purchase of supplies, etc..

Trust Establishment:

Formal procedures, contracts, some use of PKI for wholesale
transactions.

Hacker Value:

Attacker stays when security is breached, i.e., enough to steal here.

Information Security Coverage:

Full-time information security staff; high security awareness. Full-scale information security controls on internal and external systems, e.g., virus protection, access control at system level/application level, remote access, Web apps, firewall, proxy server, Web filter, PKI.

Security Breach Impact:

Major damage due to all mission-critical processing done on IT.

Business Continuity Coverage:

Full business continuity program in place.

Disaster Impact:

Limited damage; not going out of business.

Profile:

The profile of the type of enterprise is constructed based on a summary of the characteristics of the need for information security controls.

The type 5 enterprise represents enterprises and institutions large in size. They often operate on a wide (international scale). Type 5 enterprises have strong emphasis on information security due to the critical information they handle. Some examples are financial institutions, large multinationals and enterprises that hold sensitive information for others. The type 5 enterprises are subjected to strict auditing and compliance regulations. They possess a variety of IT systems and great number of users. An extensive IT infrastructure is in place. Business processing is in general, accomplished through the use of IT systems and there exists limited paper trail. The use of the Internet is extensive; from B2B and B2C purposes to research, communication and purchasing activities. The relationship with business partners is established through formal procedures, contracts and a security framework is established (e.g. PKI) for wholesale activities. Information security plays an important role. The type 5 enterprise typically possesses an IT department with high security awareness. Extensive information security controls are in place on both internal and external systems. The enterprise's information assets represent a substantial value for hackers or external parties when the IT infrastructure is infiltrated. In result, serious damage is done to the business processing in case information security is compromised. Full business recovery plans are in place enterprise wide. The impact a disaster has on the business is limited and business continuity is not compromised.

Desirable Benefit and Focus On IDM Component:

The type 5 enterprise benefits from all components of the Identity Management framework. The benefits and need for IDM explained in section 3.2 Business Perspective typically apply to the type 5 enterprise. Information security is of the essence; due to the large size of the enterprise combined with a strategic objective linked to sensitive information make the type 5 enterprise the ideal platform for Identity Management investment. The consumable value components, security and lifecycle components and data repository components will provide benefits in each of the areas of operability of IDM (see section 2.3 Identity Management Framework). The type 5 enterprise must enable secure access to their IT systems, manage the digital identities within the IT system and manage information about these identities.

4.3 Summary

The IDM positioning model categorizes several types of enterprises according to their profile based on their need for information security solutions. For each of the specified types the desirable benefits obtained from an investment in Identity Management is determined. The benefits to be obtained are derived from section 3.2. In turn, based on the desirable benefits, the appropriate IDM components are stated in which the enterprise should invest. These components are described in the IDM framework described in section 2.3.

The five types of enterprises defined have distinct information security needs. What can be observed that the size and strategic objective of the organizations influences this need. For example, the enterprises based on e-commerce benefit greatly from an increase of the user experience, whereas large multinationals need to focus on all IDM components and especially on security components.
In the following chapter an non-exhaustive overview of available IDM vendors and their products will be provided. The functionality of the products fit into the IDM framework (section 2.3) and therefore serve as practical examples of products to implement as described in the IDM positioning model. Chapter six describes the IDM investment decision based on a sample case studies. The IDM positioning model will be evaluated based on these cases.

CHAPTER 5: THE IDM MARKETPLACE

Chapter five provides an non-exhaustive overview of some of the main vendors of the IDM market and their products. The overview depicts an array of products in which can be invested based on the IDM positioning model explained in chapter four.

5.1 Overview of vendors

Following a non-exhaustive list of vendors and products will be provided in the following market segments: point IDM products and full suite IDM products (see section 2.4 Identity Management Systems). It is a sample of vendors with interesting products monitored as part of a market study.

Point IDM vendors	*Full suite IDM vendors*
Blockade Systems	Verisign
Business layers	Computer Associates
M-Tech Information Technology	IBM Tivoli
Imprivata	Oracle
Passlogix	HP
Protocom Development Systems	Sun Microsystems
NetIQ	
Netegrity	
RSA Security	
Safestone Technologies	
SafeNet	
-PET Solutions:	
A sample of privacy management solutions vendors:	
iPrivacy	
Incogno SafeZone	
Privada	
BMC	
Courion	
Maxware	

5.2 Full Suite Vendors and Products

In the following section an overview is given of some of the main vendors of full suite Identity Management products. All information described is based on the vendors documentation provided on their respective Web sites.

5.2.1 Verisign Inc.

Verisign Inc.
http://www.verisign.com.
Verisign provides complete Identity Management services which solve issues around:
Password resets, password synchronizations, numerous logins and passwords for network/system access, remote access to systems, employee access to physical buildings, employee identification badges and confidentiality of data.

Their products focus on user management and access control management. Within the user management component of the IDM framework they specialize in providing SSO solutions and password management solutions. Within the access control component they focus on authentication and authorization.

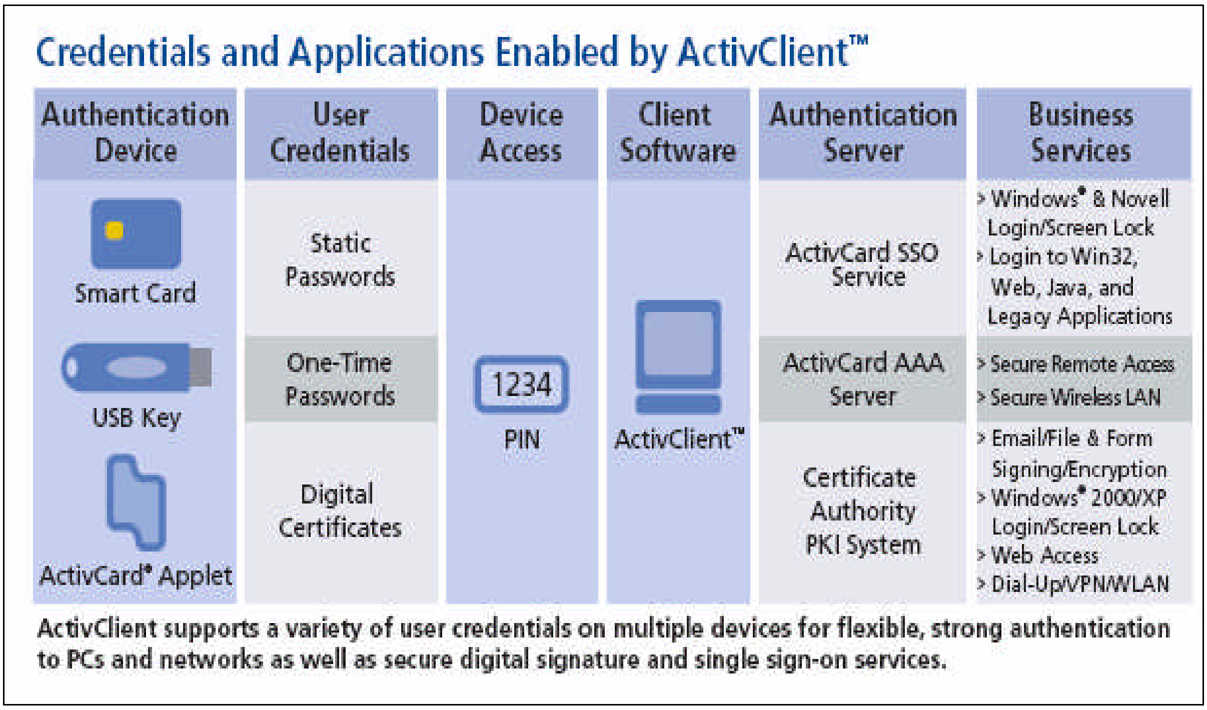
-IDM product and features:

-ActivClient:
Software client that resides on desktops and notebooks to manage communication between the smart card and enterprise applications, such as network login, remote access, web login, e-mail and electronic transactions.

Features:
PKI Services: Cryptographic Windows Login, secure dial-up / VPN.
Secure web access, Email signing/decrypting.
Use PKI certificates stored on smart cards and USB keys to electronically sign documents and forms.
Remote Access & One-Time Password Services
Password-Based Single Sign-On Services:

Management Services: User console for end-users to view and manage their smart card and credentials.

Digital Certificates: Certificate viewer, import user certificates, import/export CA certificates. One-Time Passwords: Generate password, card re-synchronization. SSO and personal information viewer



Credentials and Applications Enabled by ActivClient™

Authentication Device	User Credentials	Device Access	Client Software	Authentication Server	Business Services
Smart Card	Static Passwords	1234 PIN	ActivClient™	ActivCard SSO Service	> Windows® & Novell Login/Screen Lock > Login to Win32, Web, Java, and Legacy Applications
USB Key	One-Time Passwords			ActivCard AAA Server	> Secure Remote Access > Secure Wireless LAN
ActivCard® Applet	Digital Certificates			Certificate Authority PKI System	> Email/File & Form Signing/Encryption > Windows® 2000/XP Login/Screen Lock > Web Access > Dial-Up/VPN/WLAN

ActivClient supports a variety of user credentials on multiple devices for flexible, strong authentication to PCs and networks as well as secure digital signature and single sign-on services.

Figure 26: An overview of the credentials and applications enabled by Verisign's ActivClient.

ActivCard:

VeriSign Australia partners with ActivCard to offer strong authentication and smart card solutions. ActivCard products enable VeriSign to deliver complete token, USB key and smart card-based two-factor authentication solutions that can be seamlessly integrated with leading firewalls, applications and VPNs. The combination of the ActivCard strong authentication technology combined with VeriSign's managed PKI services provides customers with a cost-effective and reliable framework for securing business applications and information without adding complexity to infrastructure and user interaction.

Features:

Extends PKI to smart cards and USB keys for increased security, mobility and convenience. Consolidates all passwords, remote access tokens, physical access cards and PKI credentials in one smart card or USB Key reducing overall costs.

Provides a smooth bridge and migration path from legacy style function two-factor authentication tokens to future multi-application smart card solutions.
For authentication purposes the framework is augmented with *Activcard AA server* .For Single Sign-on *Activcard SSO server* is used.

5.2.2 Computer Associates International, Inc (CA)

Computer Associates International, Inc
http://www.ca.com/
They deliver a full suite Identity Management solution, covering all areas of the IDM framework.

IDM products and features:

eTrust Identity and Access Management Suite:
It is a complete set of products which offer a full scale Identity Management solution for businesses. It is delivered through the following modular set of solutions:
*e*Trust Admin for automated user provisioning and identity management.
*e*Trust™ Access Control for resource security.
*e*Trust™ Web Access Control for extranet access management.
*e*Trust™ Single Sign-On for single sign-on to all authorized Web services and enterprise-wide. applications through a single login.
*e*Trust™ Audit for end-to-end, enterprise-wide identity and access auditing.
*e*Trust™ Directory, the virtual directory infrastructure for *e*Trust Identity and Access Management Suite.

Features:
Provisioning.
Access Management and Authentication.
Password Management and Single Sign-On.
Directory Services.
Security Management.
Federation Services.
Role Based Access control (RBAC).

5.2.3 IBM Tivoli

IBM Tivoli

http://www-306.ibm.com/software/tivoli/

IBM Tivoli provide integrated identity management solutions - IBM's new Integrated Identity and Access Management Services use IBM software, IBM business consulting experts and business partner solutions to enable organizations to automate and administer complex, labor intensive identity management business processes. The cover all components of the IDM framework.

IDM products and features:

IBM Tivoli Identity Management Solution:

A full suite Identity Management Solution, is a component of IBM of IBM Integrated Identity and Access Management Services.

Features:

Lifecycle management (provisioning).

Identity control (access and privacy control, single sign-on and auditing).

Identity federation (sharing user authentication and attribute information between trusted Web services applications, federation services) .

Identity foundation (directory repository component, directory integration and workflow).

Role based access control.

Security Management (security components).

Products included:

IBM Tivoli Access Manager for Business Integration.

IBM Tivoli Access Manager for e-Business.

IBM Tivoli Access Manager for Operating Systems.

IBM Tivoli Directory Integrator.

IBM Tivoli Directory Server.

IBM Tivoli Identity Manager.

IBM Tivoli Privacy Manager for e-Business.

IBM Tivoli Security Compliance Manager.

5.2.4 Oracle

Oracle

http://www.oracle.com/index.html

Oracle Identity Management is an integrated, scalable and robust identity management infrastructure. A central component of Oracle Application Server Security, Oracle Identity Management includes an LDAP V3 directory service, directory synchronization service, identity provisioning service, delegated administration service, authentication and authorization services, and an X.509 V3 certificate authority.

IDM products and features:

Oracle Identity Management:

Full suite Identity Management Solution which is made up of the following components.

Oracle Internet Directory.

Oracle Single Sign-on

Oracle Identity Provisioning

Oracle Secure Federation Services

Oracle Certificate Authority

Oracle Security Developer Tools

Oracle COREID Access and Identity

Oracle COREID Provisioning

Oracle COREID Federation

Features:

Provisioning.

Access Management and Authentication.

Password Management and Single Sign-On.

Directory Services.

Security Management.

Federation Services.

Role Based Access control (RBAC).

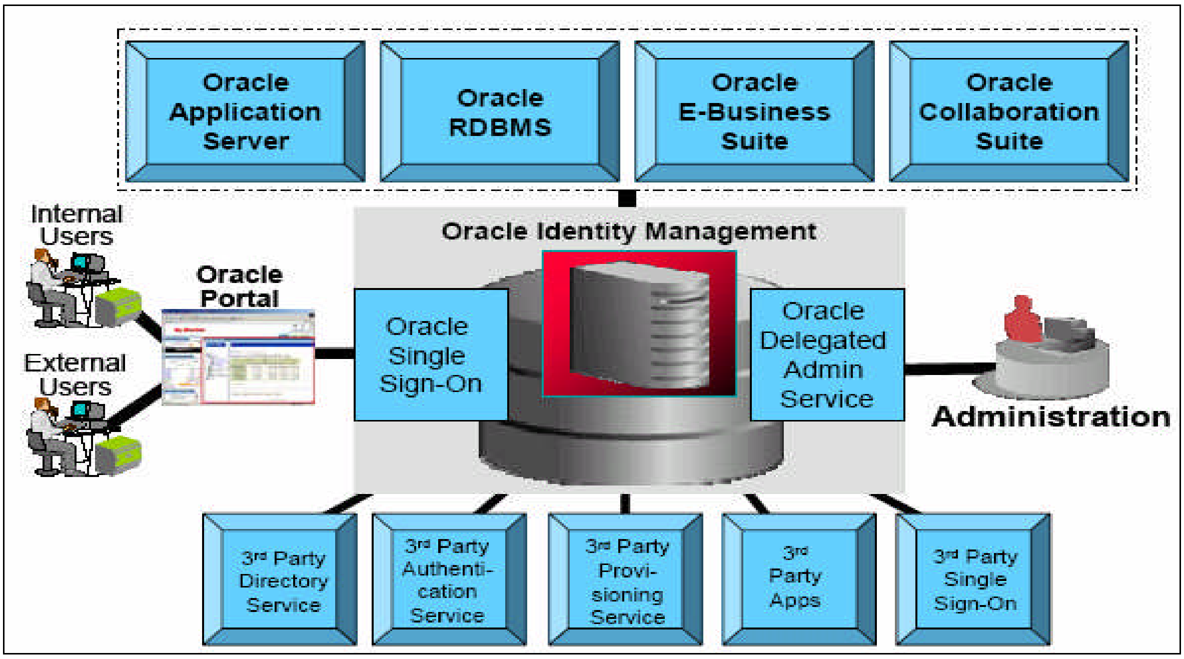

Oracle Application Server
Oracle RDBMS
Oracle E-Business Suite
Oracle Collaboration Suite
Internal Users
External Users
Oracle Portal
Oracle Identity Management
Oracle Single Sign-On
Oracle Delegated Admin Service
Administration
3rd Party Directory Service
3rd Party Authenti-cation Service
3rd Party Provi-sioning Service
3rd Party Apps
3rd Party Single Sign-On

Figure 27: An overview of the Oracle Identity Management infrastructure.

5.2.5 Hewlett Packard (HP)

Hewlett Packard

http://www.hp.com

IDM products and features:

HP OpenView Identity Management:

Full suite IDM solution. Consists of:

Select Access

Features:

Complete web-based single sign-on.

Access and principal management for users and devices.

Automated network and resource discovery.

Flexible delegated administration.

Support for SAML (Security Assertion Markup Language).

Highly scalable, standards-based architecture.

Select Federation

Features:

Works with any federation protocol.

Works with any vendor's identity systems.

Smart User activation & provisioning.

Enables compliance with privacy regulations.

Architected for scalability, reliability and performance.

Select Identity

Features:

Centralized provisioning.

Integrated workflow.

Password management.

Audit and reporting.

Delegated administration.

5.2.6 Sun Microsystems

Sun Microsystems

[*http://www.sun.com/*](http://www.sun.com/)

The Sun Java Identity Management Suite a complete and integrated suite of tools to secure and manage user identities across a variety of computing infrastructures and application environments.

IDM products and features:

The Sun Java Identity Management Suite provides all of the core functions and services required by enterprises to use, share and manage identity information, and includes the following:

Identity Manager

Features:

Integrated user provisioning and identity synchronization services for efficiently and securely managing identity profiles and permissions throughout the entire identity lifecycle.

Access Manager

Features:

Open, standards-based access control, single sign-on and federation services that help control costs and minimize the security risks of conducting business more openly.

Directory Server Enterprise Edition

Features:

A secure, highly available, scalable, and easy-to-manage directory infrastructure that effectively manages identities in growing and dynamic environments.

Identity Auditor

Features:

Enables repeatable, sustainable and cost-effective compliance with internal and external regulatory requirements across critical enterprise applications and across the identity management infrastructure.

CHAPTER 6: IDM IMPLEMENTATION CASES

Chapter six focuses on the Identity Management investment decision supported by case studies. The cases are based on real Identity Management implementations. The validity of the IDM positioning model developed in chapter four will be checked in comparison to the cases described.

6.1 IDM Case Studies

The business cases depicted in this section are extracted from the paper *Successful Real-World Implementations of Identity and Access Management* developed by RSA Security Inc.. implementations. The case studies profile leading enterprises in a wide range of industries which have implemented various components of Identity Management to meet their specific business objectives. Their stories reflect the experiences of companies across the globe that are successfully using IDM to reduce costs, increase profitability, build competitive advantage and meet the requirements of regulations [32]. The case studies are based on research conducted by RSA Security Inc..

-Diversified Financial Services Company [32]*:*

Business and Technical Objectives:

As with most companies today, this financial services organization is outsourcing HR functions to an outsourced service provider. The primary objective of this project was to drive bottom-line savings through systems management and increased employee productivity. They wanted to implement an employee self-service model and improve access to information through SSO to the outsourced HR applications. It was important for them to create an infrastructure that would allow consistent, repeatable processes for authentication and authorization that followed industry standards. The solution had to be scalable to accommodate additional users and future applications since HR applications were the first of many. The company required a strategic partner with a strong reputation in the Identity and Access Management space, with specialized knowledge in Federated Identity Management.

IDM Solution Components:

The company implemented a total IDM solution including Access Management with the central component being Federated Identity Management. It enabled the bank to share employee’s identity information outside their corporate network with their outsourced service provider.

Results:

The bank realized substantial ROI with the time saved in application development and a quicker time to market than building a proprietary solution. Cross-company authentication has worked very well and with employee self-service, the bank saw an increase in overall productivity. They were also able to implement consistent protection across all applications and improve their auditing capabilities.

-Large Financial Services Organization [32]:

Business and Technical Objectives:

This financial services organization aimed to facilitate business growth and provide superior service to their members. Goals also included meeting regulatory compliance by improving their auditing capabilities and access controls. They were also looking to heighten overall security levels and provide a better method of authenticating users while increasing administrative efficiency. The solution had to integrate well with multiple applications and provide SSO to those applications. One of the bank's main concerns was to implement a robust IDM solution that would not create unnecessary burden on their IT resources.

IDM Solution Component:

They implemented a total IDM solution including Access Management, User Management and Strong Authentication which provided the key elements to meeting regulatory compliance. Other components included Federated Identity Management which will carry employees' and partners' identity information across multiple domains and business units.

Results:

They have seen significant reductions in password resets and overall administrative burdens. Most importantly, they were able to implement a unified front-end with SSO to multiple applications for their users which has increased productivity and has improved the quality of their services.

Large Wholesale Bank [32]:

Business and Technical Objectives:

To enhance their competitive position, this bank made a bold strategic decision to move key applications to the web. As part of this, they required upgrading their security framework in order to provide access to three separate applications inside different security zones. Each zone required different levels of authentication, using digital certificates and tokens. In addition, they also had to address requirements for regulatory compliance. To accomplish this, the bank needed an IDM system that offered a high level of security with non-repudiation and online signing capabilities. One of the other main goals was to strike the right balance between security and convenience by upgrading their entire security framework and simultaneously improving their web offerings for clients. In the end, they wanted a trusted IDM advisor that could provide one comprehensive solution that addressed multiple challenges.

IDM Solution Components:

Strong Authentication factored heavily into this comprehensive IDM solution to meet the need for higher security levels and regulatory compliance requirements. Besides Access Management, their solution also included Federated Identity Management and Provisioning components.

Results:

The bank was able to bring new services to market as a result of IDM and increase their bottom line by improving operating efficiency. They managed to upgrade their security framework successfully and to satisfy regulatory compliance requirements while improving key client services.

6.2 Summary and comparison to the IDM positioning model

The case studies mentioned where extracted from the paper *Successful Real-World Implementations of Identity and Access Management* developed by RSA Security Inc. and are based on extensive research conducted by the company. They depict successful implementation of IDM solutions among financial institutions

.

The enterprises described relate to the type 5 enterprises describe in the IDM positioning model. Their characteristics match the characteristics of the type 5 organizations. The following desirable benefits to be obtained for type 5 where described in the IDM positioning model:

- Increase internal control.
- Security policy enforcement
- Cost savings.
- Improve user experience, productivity and efficiency.
- Form strong alliances through federation.

The case studies show that the benefits described in the model relate to the objectives the enterprises desired. Each of the stated obtainable benefits is stated in the IDM positioning model for a type 5 enterprise. In order to obtain these benefits an investment is needed in multiple components of the IDM framework. The IDM positioning model described the necessity of investing in the whole IDM framework. To obtain all benefits, an investment should be made in each of the components of the framework. In contrast to the model, the case studies show that an investment in partial components of the framework, like federation management or SSO, yielded high returns without having invested in other components. The enterprises focused on specific component, according to their technical objectives. Some of the enterprise do not pursue all of he desirable benefits described in the IDM positioning model. Even tough they might benefit from full investment, they put special emphasis on a part of the benefits. This is due to the fact that some of the benefits are derived from their technical objectives, management has set priorities and wishes to emphasize on some of the benefits to be obtained.

CHAPTER 7: CONCLUSION

Chapter seven sums up the subjects explained throughout the thesis. The validity of the Identity Management positioning model will be discussed based on the cases explained in chapter six. Furthermore an overview will be given of topics concerning Identity Management for further investigation.

7.1 Evaluation of the IDM positioning model

The model attempts to adequately depict an IDM investment approach for general categories of enterprises. When the model is compared to the case studies it can be observed that the model can not be taken as a rigid guideline. Some enterprises, which correspond to the defined types in the model, wish to emphasize on a specific component of the IDM framework instead of investing in all components which the model indicates. By doing so, they only obtain partial benefits, in contrast to all the obtainable benefits the model indicates for that specific type of enterprise. This is caused by a number of reasons: limited (financial resources), different priorities among higher management and external factors such as stakeholders that are unfavorable of big investments, among others. From this fact we can infer that the model indicates a general approach. It indicates an ideal investment decision in order to obtain all the possible benefits. IDM investment is a costly issue, even tough high returns are expected, the initial investment requires a strong financial position. IDM investment can be recommended for larger organizations like type 3, 4 and 5 as explained in the IDM positioning model.

It can be concluded that the desirable benefits to be obtained from an investment in IDM described by the positioning model are adequately represented in the case studies. Even tough the IDM positioning model adequately describes the obtainable benefits from an IDM investment, it remains difficult to asses the adequate IDM approach for a general category of enterprise. Moreover, no small or midsize businesses where included in the case studies. Throughout the extensive literature review no business cases were encountered on IDM investment among small or midsize enterprises. In result no comparison could be made to the IDM positioning model.

Each enterprise should discuss their need for IDM based on an extensive IDM business case, discovering the flaws in their framework and tackling them with the adequate IDM component. Investing in Identity Management often is a large scale decision making process involving millions of euros. Business cases are tools that help company executives make decisions regarding significant investments for the corporation. An Identity Management investment decision should be supported by a business case to adequately assess the decision. The business case is a structured proposal that describes the costs and benefits associated with a potential technology investment over a particular period of time. It also outlines risks, assumptions, alternatives, and other factors involved in order to gain management support for project funding [27].

7.2 General conclusions

The concept Identity Management is broad and comprises many different technological solutions. An extensive literature review was made for the development of the thesis. A striking fact was the lack of literature providing an in depth analysis of Identity Management combined with an analysis of all IDM components, drivers for adoption and practical information on how to approach the IDM investment decision.

The thesis provides an in depth analysis of Identity Management. It follows a structured approach. Identity Management focuses on digital identities with IT systems. It allocates extra emphasis on the fact that a digital identity is a representation of a human identity. This link is enforced and management of information about the identities is properly controlled. Firstly the concept Identity Management is introduced by analyzing the concept identity. With this notion in mind Identity Management is explained in detail in chapter two. A framework of the IDM components is constructed in order to provide a detailed overview of the available IDM technology and the relationship among them. To further define the importance of Identity Management, the main drivers for adoption are depicted in chapter three, based on the IDM framework. The previous information leads the way for a positioning model defining several categories of enterprises and indicating the desirable benefits to be obtained from an investment in IDM, stating the desirable IDM components as practical information. Further practical information is provided in chapter four by providing an non-exhaustive list of available IDM vendors and their products in the current marketplace. These products relate to the different components described in the framework. Finally real case studies are provided on IDM implementation and the model is evaluated in comparison to the case studies.

To sum up, the thesis provides an in depth analysis on the concept Identity Management as well as practical information on how to position enterprises within the IDM framework.

7.3 Proposals for further investigation

Identity Management is constantly evolving. Many topics remain unexplored and several areas are interesting for further investigation.

First of all, the IDM positioning model could be further analyzed by comparing it with case studies on small and midsize enterprises. Few literature is available on the IDM adoption among small midsize enterprises. This is a potential area for further investigation.

Another interesting subject is federation management. This component of the IDM framework is still relatively new. Even tough theoretical models exist on federation management, in real life implementations several problems arise around the allocation of responsibilities. Federation management is based on a trust model concerning several parties. A analysis of the trust models used in federation management is another interesting topic for further investigation.

A subject relating directly to Identity Management is privacy. With the evolution of IDM solutions new possibilities and problems arise in the area of e-government. In the near future governments will be enabled to provide a wide scale of services based on IDM solutions. Civilians will be fully digitally represented and a privacy analysis is another potential are of interest.

To sum, Identity Management is a broad, interesting and continuously evolving subject which leads to a variety of possible investigations.

REFERENCES

[1] Scott Berinato; Enron IT: A Tale of Excess and Chaos;2002
URL: http://www.cio.com/executive/edit/030502_enron.html

[2] Joe F. Thompson; Identity, Privacy and Information; 2002.

[3] PRIME Project website: http://www.prime-project.eu.org/

[4] ICCP/ ULD Schleswig-Holstein and SNG;
IMS: Identification and Comparison Study; 2003.
URL: http://www.datenschutzzentrum.de/idmanage/ study/ICPP_SNG_IMS-Study_Summary.pdf

[5] George H. Mead; Self and Society; Chicago Press 1934.

[6] Wikipedia website: http://en.wikipedia.org/wiki/Main_Page

[7] http://wordnet.princeton.edu

[8] Presentation J. Hermans, Security Plaza Utrecht 31-03-2005, © 2005 KPMG Information Risk Management.

[9] Jan De Clercq and Jason Rouault; An Introduction to Identity Management; HP devResources; 2004.
URL: http://devresource.hp.com/drc/resources/idmgt_intro/index.jsp#authors

[10] George Lawton; Is Technology Meeting the Privacy Challenge?; 2001

[11] HP Laboratories Bristol; Identity Management: a Key e-Business Enabler; 2002

[12] The Radicati Group; Reducing Costs and Improving Productivity with an Identity Management Suite; Oracle whitepaper, 2004

[13] Wang, Lee and Wang; Consumer Privacy Concerns About Internet Marketing; 1998

[14] Kruck, Gottovi, Moghadami, Broom, Forcht, Protecting Personal Privacy on the Internet; 2002

[15] Gartner Inc. Strategic analysis report; The Price of Information Security; 2001

[16] http://www.ehealthinitiative.org/

[17] Andre Durand, Towards Federated Identity Management; 2002

[18] Burton Group; Jamie Lewis; Interoperability and Federation: The Emerging Identity Management Infrastructure; 2002

[19] http://www.opengroup.org/security/sso/

[20] Technische Universität München; Michael Koch; Global Identity Management to Boost Personalization; 2002

[21] http://www.identitymanagement.net.au/

[22] Burton Group; http://www.burtongroup.com/coverage_areas/identity/management_user_provisioning_research.asp

[23] Gartner Inc.; C. Hirts, R. Wagner, V. Wheatman; Assess Authentication Methods for Strong System Security; 08-2004

[24] W. Ford, M. Baum; Secure Electronic Commerce; 2001

[25] http://www.dimreport.com/dimreport/Reports/1103.htm

[26] http://www.opengroup.org/directory/idmstds.htm

[27] Burton Group; Gerry Gebel; Building the Business Case for Identity Management Investment; 2004

[28] http://searchcio.techtarget.com/sDefinition/0,,sid19_gci920030,00.html

[29] http://www.network-intelligence.com/solutions/compliance

[30] http://www.dnv.com/binaries/BS7799_brochure_sept03_tcm4-9012.pdf

[31] Gartner Group; http://www.gartner.com

[32] RSA Security, Inc; Successful Real-World Implementations of Identity and Access Management; 2004