Digital Identity and Access Management:

Technologies and Frameworks

Raj Sharman
State University of New York at Buffalo, USA

Sanjukta Das Smith
State University of New York at Buffalo, USA

Manish Gupta
State University of New York at Buffalo, USA

Information Science
REFERENCE

Managing Director: Lindsay Johnston
Senior Editorial Director: Heather Probst
Book Production Manager: Sean Woznicki
Development Manager: Joel Gamon
Development Editor: Joel Gamon
Acquisitions Editor: Erika Gallagher
Typesetters: Mackenzie Snader
Print Coordinator: Jamie Snavely
Cover Design: Nick Newcomer, Greg Snader

Published in the United States of America by
Information Science Reference (an imprint of IGI Global)
701 E. Chocolate Avenue
Hershey PA 17033
Tel: 717-533-8845
Fax: 717-533-8661
E-mail: cust@igi-global.com
Web site: http://www.igi-global.com

Library of Congress Cataloging-in-Publication Data

Digital identity and access management: technologies and frameworks / Raj Sharman, Sanjukta Das Smith and Manish Gupta, editors.
p. cm.
Includes bibliographical references and index.
Summary: “This book explores important and emerging advancements in digital identity and access management systems, providing innovative answers to an assortment of problems as system managers are faced with major organizational, economic and market changes”--Provided by publisher.
ISBN 978-1-61350-498-7 (hbk.) -- ISBN 978-1-61350-499-4 (ebook) -- ISBN 978-1-61350-500-7 (print & perpetual access) 1. Computer networks--Security measures. 2. Computer networks--Access control. 3. Computer security. 4. Online identities. 5. Online identity theft--Prevention. I. Sharman, Raj. II. Smith, Sanjukta Das, 1978- III. Gupta, Manish, 1978-
TK5105.59.D54 2012
005.8--dc23

2011036891

British Cataloguing in Publication Data
A Cataloguing in Publication record for this book is available from the British Library.

Chapter 18
Selecting and Implementing Identity and Access Management Technologies: The IAM Services Assessment Model

Peter Haag
Utrecht University, The Netherlands

Marco Spruit
Utrecht University, The Netherlands

ABSTRACT

This chapter investigates how organizations can be supported in selecting and implementing Identity and Access Management (IAM) services. Due to the ever growing number of applications that are being used in organizations, stricter regulations and changing relationships between organizations, a new approach towards login- and password administration, security, and compliance is needed. IAM services claim to provide this new approach. Unfortunately, IAM selection projects have not been very successful in the recent past. Therefore, this chapter presents the IAM Services Assessment Model which provides a useful and usable tool to support organizations in the selection and implementation of IAM services.

INTRODUCTION

During the recent decades, organizations have changed tremendously. One of the most important changes has been the mass-computerization, which has forced organizations to change the way they operate. This mass-computerization has been one of the most important enablers of the ongoing increase in both the size and the complexity of organizations. It is self-evident that those developments have had a wide range of consequences. Most have been positive, but during recent years

DOI: 10.4018/978-1-61350-498-7.ch018

some negative consequences of those developments have surfaced as well.

Some of those negative consequences are related to the way organizations manage identities and the access to their buildings and their IT-infrastructure. To deal with those negative consequences, the way in which the identification and authentication for access to an application is organized needs to be changed. During recent years, several major IT-suppliers like Oracle, IBM, Sun Microsystems, Novell and CA have introduced IAM systems in order to support organizations in doing so.

An article on the website of Wall Street Technology (Wall Street Technology, 2008) reports that a new research from Forrester estimates the market for IAM solutions to grow more than 20 percent over the next years. The total market is expected to grow from 2.6 billion dollars in 2006 to more than 12.3 billion dollar in 2014.

Despite the fact that these figures show that a growing amount of organizations is planning to implement IAM technologies, efforts to select and implement the right solutions have proven to be little successful (Becker & Drew, 2005). Therefore, the question arises if there is any way in which organizations can be supported in making the right decision with regard to the type of IAM solution they should implement. This chapter is aimed at developing a method to support organizations and their consultancy partners in effectively and efficiently selecting the right tools to cope with the challenges they have identified in the field of Identity and Access Management.

BACKGROUND

IAM has a relatively brief history. The directory management tools that emerged in the 1990's can be seen as the start of the development of IAM systems (Rizvi, 2006), although that term was not introduced until much later. Single Sign-on and Identity Administration followed, growing along with the number of applications used in organizations.

The current IAM market has its roots in a wide range of domains, as many of the different product areas within the IAM market have started out as separate markets that flowed together over time (Cser, 2008). However IAM is nowadays often considered to be a single market, the fragmented history of the field explains why the IAM market still contains a variety of vendors, from pure players to companies that offer comprehensive IAM solutions. A quote from the research vice president at Gartner describes the situation within the current IAM market perfectly: "No company has bought tools from one vendor, or implemented them all at once, They tend to solve their problems one at a time so most organizations are somewhere along the automations track, but very few have done it all." (Everett, 2007).

MAIN FOCUS OF THE CHAPTER

As mentioned before, the rising interest in IAM solutions, in combination with the limited success of IAM selection and implementation projects, raises the question how organizations can be supported in making the right decision with regard to the type of IAM solution they should implement. This chapter will elaborate on the creation of the IAM Services Assessment Model that was developed as an answer to that question. To start creating the IAM Services Assessment Model, eight carefully selected IAM services will be elaborated upon. The selection of the services is mainly based on the adoption of the services. The services that were selected are widely adopted in organizations and have proved to be potentially beneficial in practice. Another selection criteria was the universality of the services. The services that were selected are all vendor-independent and can represent several specific services that are aimed at the same challenge and provide compa-

rable functionalities. The selection was validated during the expert interviews.

IAM CHALLENGES

As mentioned before, the ever increasing amount of applications that are being used in most organizations has some negative consequences. Those consequences are a challenge for organizations. This section will present the challenges in the field of IAM that were identified in literature.

During the analyses of the literature study results, and again during the introduction interviews, it became clear that the challenges in the field of IAM can be distinguished into several categories. In order to be able to present the challenges in a structured and conveniently arranged way, the challenge categories will be presented and elaborated upon first. The challenges will subsequently be discussed using the structure of this categorization.

The following types of challenges will be used: financial, security, regulatory compliance and ease of use. As mentioned before, the classification is based on both the literature found during the literature study and the introduction interviews. For instance, Becker & Drew (Becker & Drew, 2005) use exactly the same categorization. Furthermore, the categories are mentioned either as problem categories or as drivers for the implementation of IAM systems by others.

In the remainder of this section, the challenges will be discussed using the categorization described above. The challenges and the categorization of the challenges will be used together with the IAM services that will be elaborated upon later as a basis for the IAM Services Assessment Model.

Financial Challenges

Low user productivity: User productivity is negatively influenced by the wide array of login credentials that have to be managed by the user (Rizvi, 2006). Not only is valuable time lost if users have to log into every application separately, but productive time is also lost if an employee cannot enter an application or data that is needed for the execution of a task due to a lost or forgotten login name or password.

Redundant tasks: Because of the increasing number of applications, often in combination with an increasing number of users, it becomes very expensive to manage the login credentials for all applications, due to staff expenses, among others.

Many password calls: Every user in an organization has to remember all login credentials that are needed to access applications and data required for the execution of his or her job. As the number of applications increases, this is becoming impractical or even impossible. Especially for applications that are not used very often or require frequent password resets and strict password requirements, it is likely for the users to forget their login credentials from time to time. The helpdesk often has to manually reset the password every time a user forgets it. All those password calls combined account for a substantial part of the occupation of the helpdesk, and therefore for substantial costs (Rizvi, 2006).

Slow provisioning: Besides this, manual identity and access management processes cause an extensive lead time before new employees can be productive within the applications they need access to. This results in considerable loss due to a lower initial productivity of the new employee.

Security Challenges

Impractical security policies: A problem that surfaces more and more as the number of applications keeps growing, is that all login credentials need to be remembered by the users, and need to be securely stored by the system administrators. If users are forced to use more login credentials than they can reasonably remember, they are inclined to write the credentials down or record them in a text or spreadsheet document on their

computers. This is even more likely to occur if password resets are time- and effort consuming procedures. Although understandable, such behavior is obviously a serious infringement on the security of the organization and both its digital and material possessions.

Inconsistent security policies: If the security policies are not enforced, for instance by a role model that can be used to determine access rights, it is almost impossible to be sure to comply with the security policies in the entire organization (Becker & Drew, 2005).

Inconsistent identity data: If there are many applications in use within the organization that all use their own data repository to keep track of user identities, it is very likely that the identity data will not be consistent throughout the organization (Rizvi, 2006).

Slow de-provisioning: Furthermore, as a result of the growing number of applications and users, it becomes harder to make sure that employees who leave the organization are immediately denied access to confidential information and applications. Due to application centric administration and authentication, there are multiple (and often many) identities of the same employee in use in different applications within the organization. It is very difficult and labor-intensive to make sure every one of those identities is deleted or changed to make sure the employee cannot access data or applications he or she does not need anymore. However, this is vital to guarantee the confidentiality, integrity and availability (CIA) of sensitive information/data that is stored in applications or databases.

Regulatory Compliance Challenges

Need for auditing: In the recent past, there have been a series of corporate and accounting scandals that have caused multiple organizations to lose a lot of money, or even go bankrupt. As a reaction to these scandals, a number of laws and regulations have been introduced (such as the Sarbanes-Oxley Act (SOx), HIPAA, Basel II, etc.). Failing to satisfy the demands of these regulations may result in criminal or civil penalties, not only for the organization, but also for managers who are now held personally responsible for any fraud or other misconducts that have taken place under their area of responsibility. Apart from these legal consequences, not complying to these regulations can also have consequences for the organization that are comparable to those experienced by the organizations that gave rise to the introduction of these laws and regulations. Enron, for instance, went bankrupt in 2001 after an extensive accounting fraud. To prevent any of these consequences, organizations have to be able to show audit and control data to demonstrate their regulatory compliance (Becker & Drew, 2005).

Privacy control issues: The emphasis of regulatory compliance differs based on the parts of the world in which the organization is active. Where law requires segregation of duties in the USA, the focus in Europe and particularly the Netherlands is directed more towards privacy control (Nieuwenhuizen, 2008). As a result of the laws on privacy control in the Netherlands, any organization that allows unauthorized employees (like a receptionist) access to customer data is breaking the law. This means that organizations are forced to make often significant changes to their IT-systems, processes and procedures to avoid liability to prosecution.

Need for segregation of duties: Many of the regulations like SOx, HIPAA and Basel II require segregation of duties. This means that controlling and supervising tasks are not allowed to be performed by the same individuals who perform the tasks that are controlled or supervised (Rizvi, 2006). In other words, employees are not allowed to control or supervise their own activities. However, as mentioned in the elaboration of the 'privacy control issues', the extent to which the need for segregation of duties is required by law is dependent on the parts of the world in which the organization is active. Segregation of duties

is mainly an issue in organizations that are active within the USA (Nieuwenhuizen, 2008), but this doesn't mean that segregation of duties cannot provide advantages for organizations that are not operating in the USA.

Ease of Use Challenges

Increasing authentication complexity: when using application centric user authentication, the authentication to all applications that are needed for everyday operations becomes more complex. A user has to remember his or her login credentials for every application, and regularly also for (certain parts of) the building, operating systems, databases, etc. This obviously has a negative effect on the ease of use and the user experience of those systems.

Demand for personalized content: in many of today's organizations, knowledge is the main asset. It is therefore vital for the organization to be able to share the available knowledge among the employees. Many organizations have intranet sites or comparable initiatives to support knowledge sharing. As the amount of information in such a knowledge sharing environment increases, it becomes more difficult to find the specific piece of information that is required at that moment. Especially in large organizations with a wide variety of different expertise areas, making use of the knowledge gained by a colleague becomes difficult en time-consuming as a result. It would therefore be very convenient if the knowledge that is provided can be adapted to the roles of the users. Based on that role, information on the intranet site or any other knowledge sharing solution can be shown or hidden. The user is now only shown the information that is of interest for his role in the organization, instead of being overwhelmed with information that is not of interest for him.

Demand for self-service: as there are more applications in use that rely on application centric administration and authentication, the number of login credentials that need to be remembered grows accordingly. Therefore it becomes increasingly hard to remember all those credentials. Especially considering the fact that many applications require frequent password changes to ensure a high level of security. This results in employees forgetting some of the many credentials they need to memorize, and thus a password reset is needed before the employee has access to the application again. In those situations, employees would prefer to be able to arrange for a new password themselves, instead of being forced into a time- and effort consuming procedure to have their password changed by an admin. Other possibilities for self-service are enabling managers to make resource allocation decisions and allowing vendors to administer their own users (Becker & Drew, 2005). Providing users with this kind of self-service not only improves the ease of use and user experience, but also helps to make support for those activities more efficient. The same holds for the time and effort needed to get (and keep) access to the necessary applications. Not only is it inconvenient for the employee that he or she cannot access the application at that moment, but with a growing number of both applications and users it also gets very hard (and expensive) to have an efficient and fast procedure for passwords resets. Therefore, the employee is likely to write the password down. Again this is very likely to have a negative effect on their attitude towards the IT infrastructure and services.

Slow provisioning: Another effect of the increasing number of application in use within organizations is the frustration employees experience due to long start-up times and time and effort consuming procedures for password resets. The start-up time is the amount of time that is needed to provide a new employee with access to everything he or she needs, like access to the building, a pc or laptop, access to applications, etc. If an employee experiences that he or she cannot be as productive as possible right from the start, this will result in a negative effect on the attitude towards the IT infrastructure and services.

Final Notes on the Challenges in IAM

Most of the problems in the categories security, regulatory compliance and ease of use are likely to ultimately have financial consequences as well. However, the problems in the category financial have direct financial consequences, whereas the problems in the other categories primarily cause problems in their respective categories. Those primary problems may in turn cause financial consequences as well.

An example of a potential financial problem that is closely related to the problem described in the "compliance" and "security" sections is the loss of competitive advantage due to lacking compliance or security. If the increasing number of applications and users result in inadequate security, valuable and classified information may become available for competitors and other interested parties, resulting in potentially substantial losses for the organization. If compliance is compromised by the increasing number of applications and users, it may lead to a lack of control which in its turn can result in criminal or civil penalties and considerable financial losses.

IAM SERVICES

Following the elaboration on the challenges in the field of IAM in the section above, eight carefully selected IAM services will be elaborated upon to create the second dimension of the IAM Services Assessment Model. The selection of the services is mainly based on the adoption of the services. The services that were selected are widely adopted in organizations and have proved to be potentially beneficial in practice. Another selection criteria was the universality of the services. The services that were selected are all vendor-independent and can represent several specific services that are aimed at the same challenge and provide comparable functionalities. The selection was validated during the expert interviews.

The services that are elaborated upon in this section will be used together with the challenges as a basis for the IAM Services Assessment Model. As the IAM services will be linked to the IAM challenges in the model, this section sums up the 'Related IAM challenges' for each of the IAM services. Where applicable, it will be indicated for each of the related challenges from which literature reference this connection has been derived.

Provisioning

User provisioning systems "provide the administrative tools that link a user's business relationship to the electronic access privileges and physical resources (such as a telephone, credit card, or computer) required to perform a commercial function" (Becker & Drew, 2005). In other words, user provisioning makes sure that users have access to everything that is needed to do their jobs. This results in negative consequences on both the financial and ease of use aspects if the provisioning is not carried out fast enough. Therefore, user provisioning systems provide the tools for fast and efficient provisioning, even in complex environments. These tools are the most commonly used IAM tools, accounting for about 50% of the IAM expenditures in 2006. This number is even expected to further grow to 64% in 2014. (Wall Street Technology, 2008)

According to Becker & Drew (Becker & Drew, 2005) there are several functions provisioning systems perform:

- Detect changes in the user life cycle (hiring, role change, separation) by monitoring the key data elements in various systems.
- Define user access needs for electronic and physical assets based on those key data elements
- Create identities and credentials that provide access to electronic and physical assets before they are needed by the user.
- Apply the security policy organization-wide.

Table 1. Targeted IAM challenges by provisioning

IAM Challenge	Type	Key references
Low user productivity	Financial	Becker & Drew (2005)
Redundant tasks	Financial	
Slow provisioning	Financial	Becker & Drew (2005), Delio (2004)
Inconsistent security policies	Security	
Inconsistent identity Data	Security	
Need for segregation of duties	Compliance	Becker & Drew (2005), Delio (2004)
Increasing authentication complexity	Ease of use	

- Create an audit database to keep track of who has what access to applications and other resources, and who authorized it, when, and why.

There are several ways in which a user provisioning system can create and manage identities and credentials (Table 1). Most frequently, a network directory, like LDAP directory, Microsoft Active Directory or Novell eDirectory will be used. However, organizations often already have several of those systems implemented to manage the identification and authentication for various operating systems, applications and databases. Those different systems will very likely contain not only duplicate, but also proprietary data. There are two types of directory integration tools available to solve that problem: virtual directories and metadirectories (Delio, 2004). They will be elaborated upon below in the section Directory technologies.

Tools that provide provisioning services are also capable of de-provisioning (removing privileges). However, because provisioning and de-provisioning are related to different problem categories, they are discussed in separate sections in this document. De-provisioning will be discussed in the next section.

De-Provisioning

For de-provisioning, the same tools and services are used as for provisioning (Table 2). However, for de-provisioning purposes the definition that was given in the previous section can be adapted to "providing the administrative tools that remove a user's electronic access privileges and physical resources (such as a telephone, credit card, or computer) when they are not needed (anymore) to perform a commercial function.

As already mentioned previously, fast and efficient de-provisioning is very important for organizations to ensure the security of vital information. The same tools that enable fast and efficient provisioning can also make sure that an employee who leaves the organization or chang-

Table 2. Targeted IAM challenges by de-provisioning

IAM Challenge	Type	Key references
Redundant tasks	Financial	
Slow de-provisioning	Security	Becker & Drew (2005), Delio (2004)
Need for auditing	Compliance	Delio (2004), Rizvi (2006)
Privacy control issues	Compliance	Delio (2004)

Table 3. Targeted IAM challenges by credential management

IAM Challenge	Type	Key references
Redundant tasks	Financial	
Many password calls	Financial	
Inconsistent identity data	Security	
Increasing authentication complexity	Ease of use	

Table 4. Targeted IAM challenges by auditing

IAM Challenge	Type	Key references
Inconsistent security policies	Security	
Need for auditing	Security	Allan (2008)
Need for segregation of duties	Security	
Increasing authentication complexity	Ease of use	

es roles within the organization does not have access to any data or applications that are not needed anymore from the moment of the separation or role change.

Credential Management

Credentials management tools manage the life cycle of one or more type(s) of credentials, such as smart cards, certificates, biometric data, and proximity cards (Allan, 2008). This functionality is expected to be included into provisioning and single sign-on tools in the near future, but for now these are mostly separate tools that can only be integrated loosely into provisioning and single sign-on tools (Table 3). They support provisioning and single sign-on by offering an easy and time saving way to manage credentials over a broad range of target applications and systems.

Auditing

Auditing is "the process of documenting, reviewing and approving workflow, identity information and access controls (roles, segregation of duties rules and entitlements) for business applications and associated infrastructure components" (Allan, 2008).

The goal of auditing is to control aspects like workflow, identity information and access controls and making sure that those aspects are in line with both internal and external rules and legislation (Table 4). Obviously, this is vital for governance, and specifically for regulatory compliance.

In order to be able to accomplish that control, knowledge is required about (i) what privileges the user should have, based on the policy, (ii) what privileges the user has in practice (and is this consistent with the policy), and (iii) what privileges the user actually used.

(E)SSO (Enterprise) Single Sign-On

There are several disadvantages of having many different sets of login credentials:

Decreasing user productivity: If users have to log in to every application they need separately, this consumes valuable time and effort that can be used otherwise if a single sign-on is used. Furthermore, when users forget their password and have to contact the helpdesk to replace it, more time is lost due to both the time needed to

Table 5. Targeted IAM challenges by (Enterprise) single sign-on

IAM Challenge	Type	Key references
Low user productivity	Financial	Delio (2004)
Many password calls	Financial	Rizvi (2006)
Inconsistent security policies	Security	Delio (2004)
Increasing authentication complexity	Ease of use	Delio (2004)
Demand for personalized content	Ease of use	

contact the helpdesk and productivity lost because the user has no access to an application when needed. (Chinitz, 2000)

User inconvenience: It is inconvenient for a user to have many different sets of login credentials to remember, as it takes substantial time and effort to identify and authenticate time and time again for each application that is entered (Delio, 2004).

Ineffective or obvious passwords: When users have to sustain many different sets of login credentials, they are inclined to choose credentials that are easy to guess and therefore inherently insecure (Delio, 2004).

User negligence: If users are assigned strong passwords (for example by the IT department) they are likely to write down their credentials or record them in a digital file, which are often not kept in a secure place (Chinitz, 2000).

Lots of passwords resets: In many organizations, every time a user has forgotten a login credential, the IT-department has to be contacted to provide a new credential. In large organizations with application centric administration, this is a substantial burden on the IT department, which results in high support costs (Delio, 2004; Rizvi, 2006).

Off course, all these disadvantages will ultimately result in a financial disadvantage for the organization as well. The problems can be overcome by enabling users to access (almost) every operating system, application or database they need with a single set of login credentials.

Systems that provide that functionality have been around for quite some time (Table 5). However, early systems like Kerberos needed applications to be adapted to the use of the systems. With the broad landscape of security infrastructures in place at many organizations, this is not a practical solution anymore. Therefore, today's SSO systems need to be able to connect to every authentication system in use in an organization. They act as a authentication gateway (Chinitz, 2000).

However, not every organization should strive for a complete SSO. As mentioned by Delio: "The appropriate goal for many organizations will be reduced – rather than single – sign-on" (Delio, 2004). The decision on which information sources will be integrated into the SSO has to be taken based on a cost-benefit analysis. For a legacy system to which only a few people need access for a couple of times a year, it will probably not be worth the time and money to integrate it into the SSO system.

Authorization Services

Authorization services are responsible for providing privileges—such as permissions and access rights—o a user, based on the information that is available to the service (Table 6). There are different methods to determine which privileges have to be granted to a user. The most commonly used categories of methods are Discretionary Access Control (DAC), Mandatory Access Control (MAC), and Role-based Access Control (RBAC).

Discretionary Access Control: Identifies an owner for every object and delegates the distribution of privileges to that owner. In most cases, the

Table 6. Targeted IAM challenges by authorization services

IAM Challenge	Type	Key references
Redundant tasks	Financial	
Impractical security policies	Security	Delio (2004)
Inconsistent security policies	Security	Delio (2004)
Need for auditing	Compliance	
Need for segregation of duties	Compliance	
Increasing authentication complexity	Ease of use	Delio (2004)

owner is the user that created the object. As the owner is closely related to the object, he or she is expected to be able make a founded decision on who are allowed to access the object.

Mandatory Access Control: Relies on a combination of pre-established policies and security attributes of a user instead of the object owner to determine the access rights that have to be granted to a user. MAC compares the requirements for access to an object that are stated in a policy to the security attributes of a user. The user gets access to the object if his or her security attributes match the requirements for access to that object. Rule-based Access Control and Context-based Access Control are examples of authorization services that are based on this method.

Role-Based Access Control: Is by far the most commonly used method for user authorization. This method is based on a limited set of roles that are identified within the organization. Each of those roles is linked to a set of privileges. If a role is assigned to a user, that user automatically receives all privileges linked to the role.

Federation

Federated identity systems bring together two or more separately managed identity systems, often from different organizations, to perform mutual authentication and authorization tasks and to share identity attributes (Table 7). It "enables two organizations to administer their own users and interact with business partners utilizing industry standards" (Rizvi, 2006).

One of the most important parts of federation is to create solid and fair agreements between the federation partners. Those partners can be two different organizations, but also two departments form the same organizations, like the Human Resources and the Finance divisions (Windley, 2006).

Those agreements are vital for the success of federation, because each partner needs to be able to trust the other partner(s). For example, when two partners agree to provide access to their property and computer systems to employees of the other party, they have to be sure that their partner is careful enough in the employment, identification and authentication processes to be

Table 7. Targeted IAM challenges by federation

IAM Challenge	Type	Key references
Low user productivity	Financial	
Redundant tasks	Financial	
Slow provisioning	Financial, Ease of use	

Table 8. Targeted IAM challenges by directory technologies

IAM Challenge	Type	Key references
Inconsistent identity data	Security	
Need for segregation of duties	Compliance	Sturdevant (2005)

able to trust the employees of that partner. On the other hand, federation partners have to be careful to avoid creating agreements that are too strict, because this may cause the federation activities to become so expensive that the initial advantage of the federation is negated (Windley, 2006).

An example of the use of federation between organizations is provided by Chen (2005). She describes the way in which General Motors (GM) successfully used federation to make it easier for their 190.000 workers in the United States to access personal information, like health care and retirement benefits, through GM's employee portal MySocrates.

GM outsources many of the HR benefits they offer their employees. The result is that before the implementation of the federated identity management system, employees had to log in to everyone of those services separately. Now, as a result of the federated identity management system, users only have to log onto the MySocrates portal, and have access to all their personal information from there.

Directory Technologies

Directory technologies are products that "store and organize information about user identities and other resources within a network or domain and manage users' access to resources" (Allan, 2008). To enable these technologies to do this, they are equipped with extensive search possibilities and are optimized for reads. Directory technologies were once thought to be the answer to all IAM problems, but this has not come true (Table 8). However, many organizations use directory technologies as the backbone of their IAM architecture.

According to Gartner (Allan, 2008) many organizations can achieve about 60% of their functional IAM requirements with directory tools. However, there are some functions that cannot be provided by directory tools and have to be supplied by dedicated tools. There are several types of directory technologies, of which some are more established than others. The remainder of this section will elaborate on the most popular directory technologies, namely virtual directories and metadirectories.

Virtual directories: Virtual Directories are defined as "software products that create a logical (virtual) view of an LDAP directory by combining data from multiple repositories, or by combining multiple repositories into a single view" (Kreizman et al., 2007). In other words, a virtual directory is an intermediary between the data repository and applications. The virtual directory presents itself towards the application as a customized directory that provides exactly that information that is required by the application. To the data repositories on the other hand, the virtual directory presents itself as an application that asks for exactly the part of the needed information that can be supplied by the data repository in question (Sturdevant, 2005). By doing so, a virtual directory eliminates the need to synchronize multiple directories in order to provide a single view (Rizvi, 2006).

A virtual directory can pre-eminently be used to implement new applications or functionalities without the need to create a whole new physical data repository. An additional advantage of the fact that a virtual directory does not manipulate the data in any way can be found in situations in which ownership of the data is a delicate subject: "Virtual directories are excellent choices when

Table 9. Targeted IAM challenges by advanced self-service

IAM Challenge	Type	Key references
Low user productivity	Financial	
Many password calls	Financial	
Demand for personalized content	Ease of use	
Demand for self-service	Ease of use	

dealing with workgroups that have ownership issues concerning their data – since a virtual directory doesn't alter data, it just points to its location" (Delio, 2004).

Furthermore, as virtual directories are able to record which data has been accessed by which user, a virtual directory can help organizations to comply to regulation and legislation like SOx and HIPAA (Sturdevant, 2005).

Metadirectories: In contrast to virtual directories, which create a view in which data from different repositories is combined without moving the data, metadirectories create copies of directory data to combine data from several repositories into one large data repository (Sturdevant, 2005). "A metadirectory system establishes a single authoritative directory as the source of all data" (Delio, 2004).

While it can create an advantageous situation by physically storing all data on a single location, this solution requires a relatively complex and thus often costly infrastructure to enable replication and synchronization to ensure that the data are always up to date. It is especially useful when accuracy is considered the most important factor: "Metadirectories are ideal for situations where data accuracy across the board is critical. Everyone who has access sees the same information, period" (Delio, 2004).

Advanced Self-Service

Advanced Self-service functionalities enable users to perform tasks that were traditionally carried out by system administrators (Table 9). The reason why they are called 'advanced' self-services in this work is that some forms of self-service have been available for a long time, like the possibility provided by any operating systems to its users to change their password. The self-service functionalities in this section take over a task that was previously performed by system administrator, such as:

(SSO) Password resets: Users can reset their own passwords for applications, databases or even the entire Single Sing-On (SSO) system. The password is for instance changed to an automatically generated password that is sent to the e-mail address that is known by the system to belong to the user. The user can use this temporary password to change the password for a new, personal, password.

Requests for software licenses: A user who needs additional software often has to fill out a request and send that request to a system administrator. The system administrator then has to contact a manager or department staff to validate the request. Depending on the result of that validation, the administrator has to inform the user of a denial or provide the user with the requested software. Self-service functionalities can turn this into an automated process in which the request can be filled out digitally, and is redirected towards the manager (or staff) who is responsible for the validation of the request. The system administrator only receives a message that the user has to be provided with the requested software if the request is validated (electronically). This reduces the workload for system administrators and fastens the process for the user.

Table 10. Validation interview experts

Nr.	Position	Specialties
1	Principal Consultant at Capgemini	IS Architecture and Identity Management
2	Managing Consultant at Capgemini	Compliance governance architecture, Recertification, Authorisation Management, RBAC, Segregation of Duties, Recertification tools
3	Managing Consultant at Capgemini	Security, Security Convergence, Identity Management, Access Management, Access Control, Authorization Management
4	Managing Consultant at Capgemini	Identity and Access Management, RBAC, Security, GvIB
5	Managing Consultant at Capgemini	Specialist in Identity & Access Management
6	Principal Consultant at Domus Technica Editor of "Informatiebeveiliging" at PvIB	Identity and Access Management, Security Architecture
7	Managing Director at Domus Technica BV	Security, Risk Management, Compliancy, Business Continuity
8	Solution Architect at HP Computer & Network Security Consultant	Computer & Network Security

Requests for privileges: A request for privileges results in many cases in a process that is comparable to the one described above with regard to requests for software licenses. Self-service functionalities can therefore provide comparable services to reduce the workload for system administrators and fasten the process for the user.

Reporting problems and errors: Problems or errors that users encounter with systems can now be reported online, where they formerly were reported by phone. This saves system administrators lots of time, as the problems can be handled more efficiently this way.

The IAM Services Assessment Model

As both dimensions of the IAM Services Assessment Model have now been introduced and elaborated upon—i.e. IAM challenges and IAM services—the time has come to present the model itself. The objective of the model is to support organizations in selecting the right IAM service(s) to deal with their specific challenges with regard to IAM. The models shows the IAM services vertically (in the rows) and the challenges horizontally (in the columns). Each category of challenges was given a distinctive color to make it easier to read and use the model.

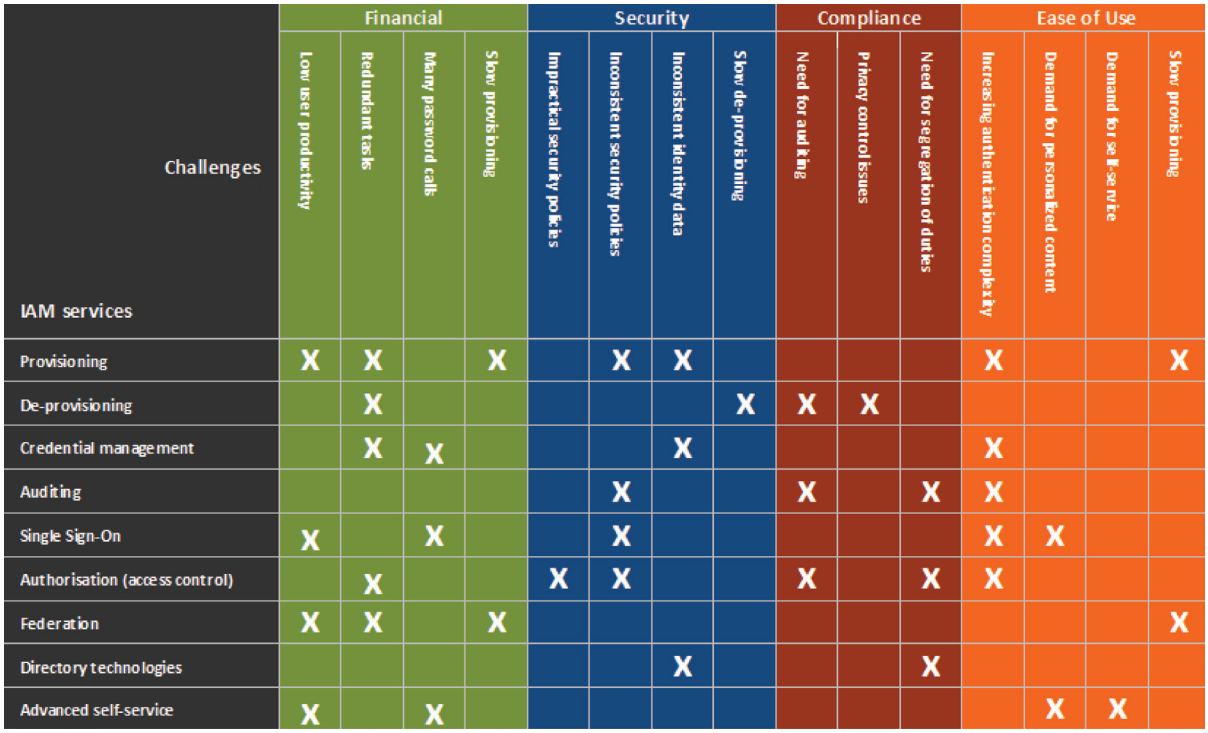
The IAM Services Assessment Model is depicted in Figure 1 and can be used bipartitely: the model can be used both service-centric and challenge-centric. The service-centric use of the model provides the user with an overview of the challenges that will be dealt with by a certain IAM service. The challenge -centric use of the model focuses on the challenges the user wants to deal with, and shows the user which IAM services are suitable to do so.

Validation

This section will elaborate on the validation of the IAM Services Assessment Model. A total of eight experts have been interviewed. During the interviews, the IAM experts were asked to fill out the IAM Services Assessment Model. They had no knowledge in any way about how the model in Figure 1 (that was based on the literature study) looks like. The only information that was given to the IAM experts was an explanation on the definition of the challenges and IAM technologies in the context of this research. The experts that were interviewed are shown in Table 10.

The model in Figure 2 shows the accumulated results of the model validation. The numbers in the cells show how many of the eight IAM experts

Figure 1. The concept IAM services assessment model based on literature



Challenges / IAM services	Financial				Security				Compliance			Ease of Use			
	Low user productivity	Redundant tasks	Many password calls	Slow provisioning	Impractical security policies	Inconsistent security policies	Inconsistent identity data	Slow de-provisioning	Need for auditing	Privacy control issues	Need for segregation of duties	Increasing authentication complexity	Demand for personalized content	Demand for self-service	Slow provisioning
Provisioning	X	X		X		X	X					X			X
De-provisioning		X						X	X	X					
Credential management		X	X				X					X			
Auditing						X			X		X	X			
Single Sign-On	X		X			X						X	X		
Authorisation (access control)		X			X	X			X		X	X			
Federation	X	X		X											X
Directory technologies							X				X				
Advanced self-service	X		X										X	X	

marked each cell, to indicate a direct link between the technology and the challenge. The red borders indicate which links are present in the model based on the literature study. The model was adapted based on the results of the validation in the following way:

- 0, 1 or 2 markings: the experts do not think that there is a direct connection between the technology and the challenge. If a connection was placed based on literature, that connection was removed.
- 3, 4 or 5 markings: the experts do not agree on if there is a direct connection between the technology and the challenge. No changes were made to the findings from the literature study.
- 6, 7 or 8 markings: the experts think that there is a direct connection between the technology and the challenge. If no connection was placed based on literature, a connection was added.

This method resulted in the changes shown in Table 11.

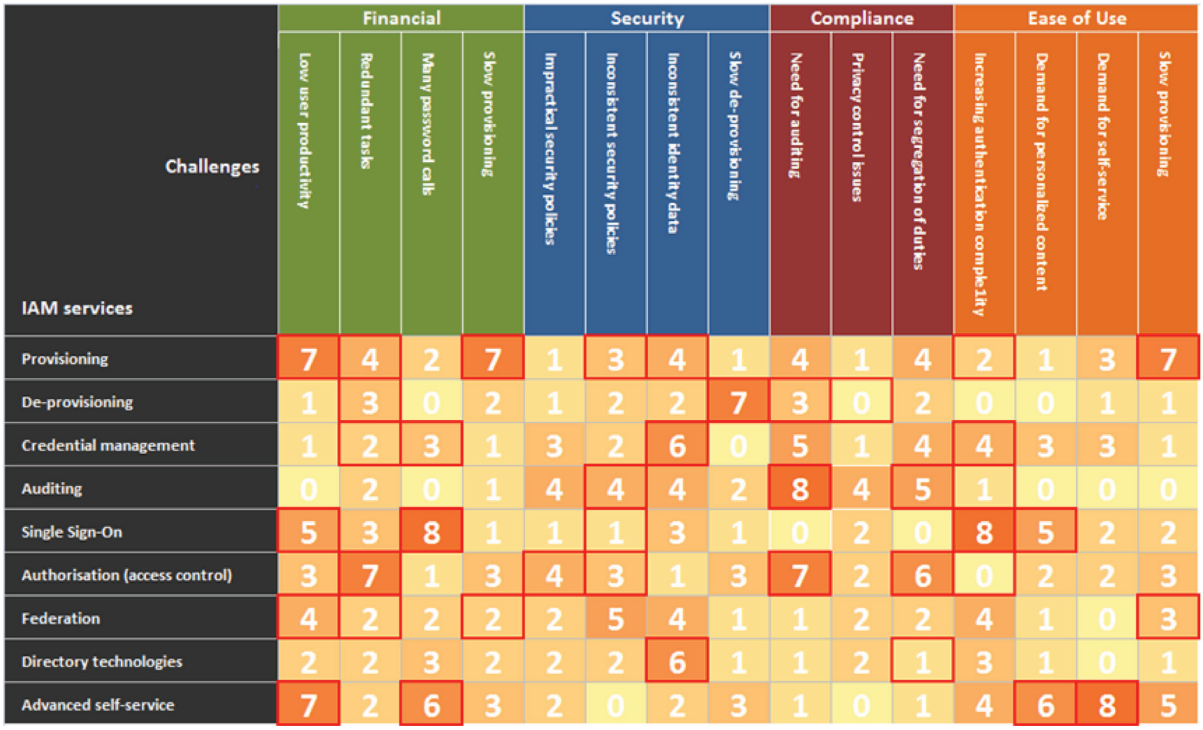
The adaptations result in the final IAM Services Assessment Model, which is shown in Figure 3.

FUTURE RESEARCH DIRECTIONS

Looking at the research that was carried out, there are some areas in which additional research can be performed.

The first and foremost is the validation of the IAM Services Assessment Model during actual selection processes in organizations that are planning to implement one or more IAM service(s). Due to time constraints and the limited set of organizations that are starting large IT-projects in

Figure 2. The IAM services assessment model with validation results



Challenges / IAM services	Financial				Security				Compliance			Ease of Use			
	Low user productivity	Redundant tasks	Many password calls	Slow provisioning	Impractical security policies	Inconsistent security policies	Inconsistent identity data	Slow de-provisioning	Need for auditing	Privacy control issues	Need for segregation of duties	Increasing authentication complexity	Demand for personalized content	Demand for self-service	Slow provisioning
Provisioning	7	4	2	7	1	3	4	1	4	1	4	2	1	3	7
De-provisioning	1	3	0	2	1	2	2	7	3	0	2	0	0	1	1
Credential management	1	2	3	1	3	2	6	0	5	1	4	4	3	3	1
Auditing	0	2	0	1	4	4	4	2	8	4	5	1	0	0	0
Single Sign-On	5	3	8	1	1	1	3	1	0	2	0	8	5	2	2
Authorisation (access control)	3	7	1	3	4	3	1	3	7	2	6	0	2	2	3
Federation	4	2	2	2	2	5	4	1	1	2	2	4	1	0	3
Directory technologies	2	2	3	2	2	2	6	1	1	2	1	3	1	0	1
Advanced self-service	7	2	6	3	2	0	2	3	1	0	1	4	6	8	5

these difficult economic times, it was unfortunately not possible to validate the model longitudinally in practice. Although the validation by IAM experts has produced a very usable and sound model, a validation based on multiple IAM service selections would make the model even more robust.

Something that was already mentioned in the validation section of this chapter, is that the IAM experts indicated that the challenges in the category Security are too similar to allow organizations to make a clear distinction between them. As a result of that remark, further research should be

Table 11. Removed IAM associations in the literature-based model shown in Figure 1 based on the expert validation results shown in Figure 2

Change #	IAM challenge type	IAM challenge	Removed IAM service link
1	Financial	Redundant tasks	Credential management
2	Financial	Redundant tasks	Federation
3	Financial	Slow provisioning	Federation
4	Security	Inconsistent security policies	Single Sign-On
5	Compliance	Privacy control issues	De-provisioning
6	Compliance	Need for segregation of duties	Directory technologies
7	Ease of use	Increasing authentication complexity	Provisioning
8	Ease of use	Increasing authentication complexity	Auditing
9	Ease of use	Increasing authentication complexity	Authorization

Figure 3. The validated IAM services assessment model

Challenges / IAM services	Financial				Security				Compliance			Ease of Use			
	Low user productivity	Redundant tasks	Many password calls	Slow provisioning	Impractical security policies	Inconsistent security policies	Inconsistent identity data	Slow de-provisioning	Need for auditing	Privacy control issues	Need for segregation of duties	Increasing authentication complexity	Demand for personalized content	Demand for self-service	Slow provisioning
Provisioning	X	X		X		X	X								X
De-provisioning		X						X	X						
Credential management			X				X					X			
Auditing						X			X		X				
Single Sign-On	X		X									X	X		
Authorisation (access control)		X			X	X			X		X				
Federation	X														X
Directory technologies							X								
Advanced self-service	X		X										X	X	

performed to assess the changes that can be made to the IAM Services Assessment Model to solve this problem.

A final suggestion with regard to further research based on this work concerns the adoption of the IAM Services Assessment Model with respect to the ongoing developments in the field of IAM services. The IAM services that were included in the model were selected based on their current level of adoption. However, some of the IAM services that were not included into the model at this time (because their current level of adoption is still rather low) may well develop into the leading IAM services of tomorrow. Therefore, especially in a few years from now, some additional research should be carried out to update the model in concordance with the IAM services that are leading in terms of adoption at that time.

CONCLUSION

The purpose of the research was to find an answer to the research question "How can organizations be supported in the process of selecting and implementing IAM technologies?". The answer to this research question was the development of the IAM Services Assessment Model that was presented in this chapter.

To come to this result, the research was started with a literature study. Based on that literature study, the initial IAM Services Assessment Model was developed as shown in Figure 1. Then, the model was validated with the help of eight IAM experts which were introduced in Table 10. Based on that validation, nine changes were made to the initial model as listed in Table 11. Figure 3, finally, shows the resulting validated version of the IAM Services Assessment Model.

The conclusion of this research—with regard to selecting the right IAM service to cope with the

challenges the organization is faced with—is that the IAM Services Assessment Model provides a useful and successfully validated tool that can be used both service-centric and challenge-centric. The service-centric use of the model provides the user with an overview of the challenges that will be dealt with by a certain IAM service, while the challenge-centric use of the model focuses on the challenges the user wants to deal with, and shows the user which IAM services are suitable to do so. The IAM Services Assessment Model supports organizations in selecting the right IAM services efficiently and effectively, thereby providing a satisfactory answer to our research question.

REFERENCES

Allan, A. (2008). *Identity and access management technologies defined*. Stamford, CT: Gartner.

Becker, M., & Drew, M. (2005). Overcoming the challenges in deploying user provisioning/identity access management backbone. *BT Technology Journal*, *23*(4), 71–79. doi:10.1007/s10550-006-0009-x

Chinitz, J. (2000). Single sign-on: Is it really possible? *Information Systems Security*, *9*(3), 33–45. doi:10.1201/1086/43310.9.3.20000708/31359.5

Cser, A. (2008). *The Forrester Wave: Identity and access management, Q1 2008*. Cambridge, MA: Forrester.

Delio, M. (2004, September 6). Better security through identity. *Infoworld.com*, 35-42.

Everett, C. (2007). Piecing identity together. [Elsevier.]. *Infosecurity*, *4*(6), 22–25. doi:10.1016/S1754-4548(07)70145-6

Kreizman, G., Enck, J., Litan, A., Wagner, R., Orans, L., & Allan, A. (2007). *Hype cycle for identity and access management technologies*. Stamford, CT: Gartner.

Nieuwenhuizen, M. (2008). *Role based identity- en access management is makkelijker gezegd dan gedaan [‘Role-based identity and access management is easier said than done’]*. Retrieved July 28, 2008, from http://www.marqit.nl/securityschool-compliance-artikel2.aspx

Rizvi, H. (2006). I am who I say I am. *Quarterly Journal of the EDS Agility Alliance*, *1*(2), 46–57.

Sturdevant, C. (2005, June 6). Virtual directories ease quest for identity data. *eWEEK.com*, 43-46.

WallStreet Technology. (2008). *Identity and access management market to reach $12.3 billion in 2014.* Retrieved October 24, 2008, from http://www.wallstreetandtech.com/showArticle.jhtml?articleID=206904330

Windley, P. J. (2006, March 27). The hidden challenges of federated identity. *InfoWorld.com*, 27-33.

KEY TERMS AND DEFINITIONS

Authentication: the entity proofs that it is the rightful ‘owner’ of the identity by providing one or more credential(s).

Authorization: the entity is allowed a particular set of actions to be performed in the secured environment based on the combination of the identifier and the credential(s) provided by the entity.

Federation: linking two or more separate IT systems, enabling them to share authentication data and perform mutual identification, authentication and authorization services.

IAM system: a single set of hardware, software, databases, telecommunications, people, and procedures configured to collect, manipulate, store, and process data into information, supporting identifying individuals and controlling their access to resources, services and systems.”

Identification: an entity claims an identity by providing an identifier.

Provisioning: linking a person (for example through his role) to the access rights (both physical and electronic) that are needed to do his/her job properly.

Single Sign-On (SSO): enabling users throughout the organization to log onto every system, application or database with a single set of credentials.