



White Paper

Identity Management – an infrastructure task with measurable benefits

Axel Kern · Martin Kuhlmann

Beta Systems Software AG

Alt-Moabit 90d
D-10559 Berlin

Tel. +49 (0)30 726 118 – 0
Fax +49 (0)30 726 118 – 800

info@betasystems.com
www.betasystems.com

Summary

The term "Identity Management" includes all aspects of the administration of digital identities. This is initially an infrastructure task which is indispensable to the proper functioning of an organization. It is also a management task, since these activities affect data security and the efficiency of business processes. An investment decision for an Identity Management solution is therefore not based on a "need-to-have" perception, but is increasingly oriented towards measurable potential benefits: an increase in security levels and in the efficiency of identity administration. In this article we will be considering individual aspects of security and efficiency. We will demonstrate how and to what extent these aspects can be measured in money terms and can therefore be included in a reliable Return-on-Investment calculation. A model for costing the implementation of Identity Management solutions will be presented, using a concrete example. The calculation used as an example will be made using an MS Excel-based "return on investment calculator" which we have specially developed for this purpose.

This White Paper has been published in German language in the proceedings of the DACH Security Conference, Basel, March 2004.

Introduction

The term Identity Management includes all aspects of the administration of digital identities (see [Lewi03]). It includes a company's employees, business partners and customers, and "technical identities" such as identifiers, which computer programs use to access resources, also fall into this category.

The administration of digital entities consists of their initial creation, the provision of identities as a reference (e.g. typically as telephone books), the allocation of digital resources (access control) and controlling their activities. Numerous detailed tasks, such as Password Management, authorization request procedures, administration concepts (distributed administration), the enforcement of security and data protection regulations as well as the synchronization of identities and their attributes in various data bases and directories all have to be taken into account within the framework of administration.

Identity Management is therefore an infrastructure task which is indispensable to the proper functioning of an organization. An investment decision for an Identity Management solution is not based only on a perception of "need-to-have", but is increasingly oriented towards the measurable potential benefits of Identity Management; an increase in security levels and in the efficiency of identity administration.

In this article we will be considering individual aspects of security and efficiency, and demonstrating how and to what extent these aspects can be measured in money terms and thus be included in a reliable Return-on-Investment calculation. A model for costing the implementation of identity management solutions will be presented, using a concrete example.

We will not deal here with the additional benefits of "federated Identity Management", see <http://www.oasis-open.org>), since we have not yet had sufficient experience in this area.

Benefits and monetary measurability

In this section the most important benefits of Identity Management will be categorized and described. We will especially be considering the areas of,

- increasing efficiency and reducing costs, as well as
- increasing security levels.

Increasing security and reducing costs

Abolition or simplification of manual administration

Using suitable administration tools can simplify or completely automate many activities:

- Routine activities affecting a digital identity's life cycle, such as setting up a user account for a new employee, the allocation of resources, changes to resource allocations and the deletion of user accounts are all examples of administration procedures which can be extensively automated. New employees are usually entered into employee data systems (e.g. SAP, Peoplesoft). These entries and changes (such as change of workplace) can be drawn on by the employee data systems and automatically turned into user accounts and access authorizations on different systems by provisioning systems (as part of an identity management solution). Experience has shown that more than 90% of these routine tasks can be automated. The automation effect is directly measurable. The time required for every administration task (e.g. 5 minutes per administration task) on every system is determined, and the savings are calculated using the average cost per administrator.
- An electronic request procedure for identities and resources (workflow) reflects the enterprise's requests approval procedure. Administration tasks which are not completely automated can be easily and comprehensibly performed in this way - providing resources to members of a temporary project group, for example. This electronic requests procedure saves on administration processes. Without this procedure, requested resources must be individually allocated to end-users manually and separately for each IT system involved ("individual authorization") after approval. The requests procedure integrated into the Identity Management System does this after electronic approval automatically, synchronously and for all connected systems, based on access rules or for thematically grouped bundles of authorizations. The value of this can be calculated from the savings made on the average number of individual authorizations.
- Simpler rights administration through roles-based administration: For administration tasks which cannot be done completely automatically, or are done manually via an electronic requests procedure, a reduction in the number of administration processes can be achieved in the case of roles-based administration. Roles are bundles of authorizations instead of individual authorizations allocated to users. A roles hierarchy with rights inheritance mechanisms (see [FeKu01]) further increases efficiency. Detailed efficiency calculations based on a role model can be found in [Chan03].
- Reduced burden on help desks through the use of Password Reset Self Service and Password Synchronization or Single Sign-On. Savings can be particularly made here through a reduction in the number of calls to help desks. These can

be easily established by multiplying the number of calls saved by the length of an average help desk call and its costs.

- Easier auditing and reporting: Here the regular cross-platform reports must be distinguished from the ad-hoc reports. The savings can be calculated by determining the time required for reporting for each system for both types of report, and the time and effort involved in manual consolidation. Experience shows that using reporting on a cross-platform tool reduces costs by about 50-80%.
- Shorter training times: working with a consistent administration tool across a number of systems simultaneously makes administration easier. Only a few specialists for individual technical systems are needed. Training for administrators is usually limited to handling the central system. The training costs saved can be calculated from the number of administrators and the training costs saved for each of them.

Increased efficiency for end users

Fast provision of resources for internal and external employees can be critical for success (e.g. a partner needs access to resources for the issue of a joint business proposal). High costs can be incurred here if external employees are unproductive. Faster unblocking of blocked accounts (e.g. if a user has incorrectly typed in his password several times) reduces waiting times and increases productivity.

Measuring an increase in efficiency is usually difficult. The situations in which employees are unproductive if they are unable to access certain digital resources must first be defined:

- This is hard to define in the case of internal (permanently employed) employees because it's not usually clear how unproductivity correlates to the non-availability of resources. Comparative studies (see e.g. [WeSK01] for directories) have also demonstrated uncertainties in the order of magnitude which should be used here.
- High and clearly demonstrable costs can also be incurred if a new sub-contractor cannot work for several days due to lack of an account or authorization and is unproductive due to being stuck on one concrete task.

Further aspects

- Automated processes enable service levels to be improved, due to faster help desk reaction times, for example.
- Reduces superfluous user accounts: a central Identity Management System includes reporting functions which enable unused user accounts to be traced and deleted. This reduces outsourcing costs, particularly in the context of IT services, where the outsourcer's bill is based on the number of user accounts. The savings can be easily calculated from the price per account and the reduction in the number of unused accounts.

Increased security levels

In terms of Identity Management, increased security levels mean guaranteeing confidentiality and preventing data misuse. The prerequisites for guaranteed confidentiality include secure authentication and the correct issuing of rights, consistent administration, and regular auditing.

Without the "Single Point of Control" provided by an Identity Management System, it can be hard to keep track of a user's current resource allocations. Undesirable correlations between authorizations, which could lead to a violation of the principle of the separation of powers for example, are not recognized.

Methods from risk management can be used to quantitatively analyze increased security levels, but we will not go into detail on these here. These methods have recently been increasingly developed due to legal regulations and standards on risk reduction. The Basel Capital Accord, for example, requires the European banking industry to evaluate operative risk. A survey revealed that European banks hold on average 15% of their total capital for operative risk coverage (see [BrJR01]). Risk evaluation methods (see also [BrJR01]) are based on databases with experimental values for the losses caused by damaging events. Statistical models are drawn up from these and expanded by trend indicators where necessary.

Unfortunately in many companies there are no statistics available on the amounts of damage caused by data misuse, so an evaluation in money terms is difficult. Qualitative parameters for improvements in security levels can however be provided.

In the following sections some aspects of security which can be positively influenced by Identity Management solutions will be explained in more detail.

Targeted rights issue

Without an Identity Management solution, problems such as an accumulation of user rights often occur. When employees change workplaces they receive new resource authorizations and the old ones, which are no longer required, are often not deleted. When employees leave a company their user accounts are often not deleted or deleted incompletely.

An Identity Management system guarantees a targeted rights issue that reacts flexibly to changes.

An increase in security levels can be qualitatively evaluated as follows:

- The percentage of authorizations which have incorrectly accumulated is determined by a preliminary investigation (perhaps based on a spot check). If rights issuing is 80% automated, this value can be reduced by about the same percentage.
- The number of unused user accounts ("orphaned accounts") is determined and automatic deletion reduces the number of these.

Password Management

Processes such as Password Synchronization or Single Sign-On which are normally part of an Identity Management solution, reduce the number of passwords. This means that end users do not need as many passwords, which are usually very simple or written down. If a password is needed, it will satisfy the highest standards and thereby increase security.

Compliance with legal regulations

Identity Management also enables regulations to be implemented throughout the enterprise. These are often derived from legal guidelines (e.g. HIPAA or Sarbanes-Oxley in the USA, the Basel Capital Accord in Europe). Infringements of these regulations can damage a company's image and also lead to the imposition of heavy fines.

Further efficiencies

In this section we will mention some further benefits which we will not however quantitatively evaluate, either because evaluation is difficult or because existing methods for doing so exceed the scope of this article.

One-off effects

A system of access rights and security policies is stored in the repository of an Identity Management solution, which can be implemented on the new platform during events such as conversion/migration to new technical platforms (e.g. network, application system) via automated procedures.

Further savings can be made through organizational changes to the company. The necessary systems adjustments (rights structure, policies) can be prepared centrally, then promptly applied to the Identity Management System via batch programs and automatically propagated on all connected platforms.

Long-term strategic benefits

Increased networking among companies and the resulting increased use of Web services will also affect Identity Management. The implementation of new standards (e.g. SPML, XACML) and technologies provides a basis for companies to operate flexibly on the market. It will be much easier to introduce cross-company standards in the future if a company's internal Identity Management is standardized.

Reducing the costs of friction

We define friction costs as "The opportunity costs of a bad decision, resulting from a lack of information and an insufficient use of standards." (see [KoBu01]).

Identity Management solutions enable user administration to be standardized and contributes considerably to improving the quality of user and authorization data through automation and data synchronization. Cross-platform reporting provides information which would otherwise not be available, or which could only be obtained with difficulty. An area where this could impact security might be finding correlations in one person's rights in different systems, for example.

The costs of Identity Management

The costing of Identity Management solutions includes the following elements:

- software licenses and manufacturers' maintenance costs,
- external and internal implementation costs,
- implementation of a roles concept, where necessary
- operating costs.

Software licenses & manufacturer's maintenance costs

The core of an Identity Management solution is usually modular software providing the required functions (automated resource allocation or provisioning for all connected systems from the host up to web applications, workflow, password management, Single Sign-On, synchronization of directories etc.).

The pricing models of most manufacturers are based on the number of users administered by the software throughout the enterprise on the one hand, and on the number of modules used (administration components and connectors for the connected systems) on the other hand. Maintenance fees usually include upgrades of the connectors (e.g. connector upgrade from SAP 4.5 to SAP 4.6B).

External and internal implementation costs

The costs of implementation depend on a project's execution and the implementation methods chosen. In [KeKW02] we have described a process model which has been successfully used in many large enterprises. The implementation costs consist of internal and external costs.

The internal costs are determined by the following main factors:

- Preparation costs:
These include on the one hand the costs of the product evaluation and of at least one Proof of Concept for the product chosen or for the last two candidates. On the other hand costs for concept preparation are also incurred: considerations about a federated administration concept, selecting systems to be connected and analyzing data quality in those systems, determining which parts of the organization will be involved and setting up the project team.
- Costs of the implementation phase:
Technical employees (systems maintenance, architecture, maintenance and support for databases/directories, production) and employees from various areas of the organization (corporate organization, data security, auditing) are all involved in implementation. Project controlling, including coordinating the sections involved, must also be taken into consideration.
- Ongoing operational costs:
Here the costs of the system's productive operations and of change management need to be accounted for. The latter also includes the maintenance and upgrade of the necessary hardware and software, the maintenance of roles and their adjustment to organizational changes (see also [KKSM02]).

External costs are incurred for installation, setup, training and any customization of the product by a team from the manufacturer or by a systems integration specialist.

Experience has shown that implementation costs can only be correlated with software costs with some difficulty. A corridor of 20-40% percent of the total costs is usual for clearly defined medium-sized projects. Using the complexity of an implementation as an indicator of implementation costs is also difficult because of the many effects which, in the case of Identity Management, are included in this indicator, such as Directory Implementation for example, (see [WSO01]). We will not however be going into more detail on this issue in this paper.

Total costs

The total costs (license fees and internal and external implementation costs) of an average project for a company with 20.000 users, and 4 system types supported by an Identity Management System (e.g. Windows, Unix, Mainframe and SAP) usually exceed 1 mill. Euros.

The **Return on Investment** becomes evident when the costs and benefits for a specific period (for the operational calculation methods see [Woeh02]) are compared. In the case of Identity Management projects, this period should be about three years. In order to reach the break-even point as quickly as possible, a company should pursue the strategy of implementing and rolling out the Identity Management solution initially for 3 or 4 core systems connections. The benefits described above (automation etc.) will then be quickly achieved for these systems. This rollout could be completed within 3-4 months. After this, further target systems and administration modules can be successively integrated into the solution. Experience has shown that the break-even point will be reached in about 12-15 months.

Practical example

In this section we will present a model calculation for a fictive company comparing the costs and benefits as described above. The model calculation will be made using an MS Excel-based "return on investment calculator" which we have developed specially for this purpose.

The calculation is quite general, but also partly refers to functions and components of SAM Jupiter Identity Management software from Beta Systems (www.betasystems.com). The values presented are derived from the experience of productive operations using this software and have been verified in the orders of magnitude described.

This model calculation covers a period of 3 years from the solution's initial implementation. The enterprise under consideration has a total of 37.000 IT users.

For reasons of space we will only present the most important parts of the calculation here. The use of a Password Management component (User Self-Service Reset and/or Password Synchronization or Single Sign-On) will also not be considered here. It is easy to do separate calculations for these components, which usually reach break-even in less than a year.

Company characteristics data

The calculation is based on characteristic data on the company's IT users and its user administration (Table 1). Changes to the authorization structure ("MACs", i.e. "moves/adds/changes") also play a role in the ROI calculation. "Target systems" are those systems connected to the central Identity Management solution.

Table 1: Company characteristics data

Internal users	Number of employees	30.000
	Number of contractors	7.000
	Number of Internal Users (Employee/Contractor)	37.000
	Yearly growth rate (Employees/Contractors)	1%
	Yearly turnover rate (Employees/Contractors)	4%
	Number of requested MACs (moves/adds/changes) per employee/contractor	3
	Average number of Target Systems used by an internal user	4
External users	Number of External Users (Business Partners, Customers)	5.000
	Yearly growth rate (Business Partners, Customers)	2%
	Yearly turnover rate (Business Partners, Customers)	6%
	Number of requested MACs (moves/adds/changes) per partner/customer	2
	Average number of Target Systems used by an external user	2
Security administration staff	Current number of IT staff dealing with setup and administration	65
	Average percentage of time dedicated to setup/administration	70%
	Resulting number of FTEs for setup/administration	45,5
General parameters	Working hours per day	7,5
	Working day per year	210
	Working hours per year	1.575

Savings from automation

Table 2 shows the savings which can be achieved through the automation of security administration (here called "provisioning"). Then the number of individual changes ("Target system specific requests") for different user groups calculated from the basic information in Table 1. The automation potential is estimated for each user group.

Table 2: Savings from automation

Provisioning Savings	Year 1	Year 2	Year 3
Number of target system specific requests, ...			
... for internal users, resulting from growth and turnover rates	13.320	13.453	13.588
- Expected automation rate for these requests	40%	75%	85%
... for internal users, based on number of requested MACs	448.440	452.924	457.454
- Expected automation rate for these requests	10%	40%	50%
... for external users, resulting from growth and turnover rates	1.400	1.428	1.457
- Expected automation rate for these requests	40%	75%	85%
... for external users, based on number of requested MACs	20.400	20.808	21.224
- Expected automation rate for these requests	10%	20%	30%
Total number of target system specific requests	483.560	488.614	493.722
Number of requests which can be automated	52.772	196.492	247.882
Remaining requests to be handled	430.788	292.121	245.840
Number IT staff FTEs if Manual Work	46	46	46
Number of IT staff FTEs when SAM is implemented	41	27	23
IT staff savings	5	18	23
Yearly IT staff cost	86.625	88.358	90.125
Savings in €	430.138 €	1.632.887 €	2.100.195 €

Workflow

Administration tasks that are not completely automated can be partly dealt with using a workflow system. Table 3 shows the potential savings.

Table 3: Savings from Workflow

Savings from use of workflow	Year 1	Year 2	Year 3
Number of remaining target system specific requests to be processed because not covered by Provisioning, ...			
... for internal users	411.588	275.118	230.765
... for external users	19.200	17.003	15.075
Total Number of remaining target system specific requests to be processed	430.788	292.121	245.840
Total number of remaining requests, not target system specific, according to average number of target systems per user	112.497	77.281	65.229
- Estimated coverage of above requests with SAM Jupiter Workflow	10%	50%	70%
- Resulting number of above requests handled with SAM Workflow	11.250	38.641	45.660
Saved number of target system specific requests to be processed, thanks to Workflow and role- or profile-based administration	43.079	146.061	172.088
Time to process a target system specific request (minutes)	9	9	9
Time for a request approval using SAM Jupiter Workflow(minutes)	4	4	4
IT staff saved time (hrs)	5.634	19.060	22.436
IT staff FTE savings	3,6	12,1	14,2
Yearly IT staff cost	86.625,00 €	88.357,50 €	90.124,65 €
Savings in €	309.881,05 €	1.069.275,22 €	1.283.845,12 €

Increased productivity for end users

In this model calculation an increase in productivity for external employees only ("contractors") is quantitatively evaluated (Table 4).

Table 4: Increased productivity for external employees (contractors)

	Year 1	Year 2	Year 3
Saving Wait Time			
Number of setup operations for internal users resulting from growth and turnover	1.850	1.865	1.880
Number of moves/adds/changes (not TS-specific)	111.000	112.110	113.231
Setups/MACs covered by fully automated provisioning	11.840	46.243	58.213
Setups/MACs covered by workflow	10.290	34.390	40.384
Average number of days an internal user waits for his setup/MAC ...			
... without automation or workflow	5		
... with automation	1		
... with workflow	2		
Percentage of waiting time in which the user is completely			
- Employee	0%	(equals 0,0 hours)	
- Contractor	50%	(equals 18,8 hours)	
Percentage of contractors	19%		
Productivity Gain (hours) - Employees	0	0	0
Employees Costs per Hour	47,00 €	47,94 €	47,98 €
Productivity Gain - Employees	0,00 €	0,00 €	0,00 €
Productivity Gain (hours) - Contractors	7.400	27.256	33.487
Contractor Costs per Hour	90,00 €	91,80 €	93,64 €
Productivity Gain - Contractors	666.004,50 €	2.502.142,22 €	3.135.584,57 €
Total Wait Time Savings	666.004,50 €	2.502.142,22 €	3.135.584,57 €

Overview costs/benefits

The overview in table 5 shows a comparison of the costs and calculated savings or productivity efficiencies. As well as the benefits detailed above, role-based access control (RBAC), and reduced training and auditing savings are also included.

If the average software values are compared with the implementation costs, the break-even point is reached in about 15 months. After 3 years, about 230% return on investment is achieved.

Table 5: Overview

	Start-up investment	Year 1	Year 2	Year 3
Cost / Benefit Calculation				
Costs Software License Fees and Maintenance Costs	1.650.000 €	297.000 €	710.000 €	360.000 €
External and Internal Implementation Costs		600.000 €	400.000 €	200.000 €
RBAC introduction project costs		0 €	140.270 €	
Operational Costs		316.563 €	597.609 €	605.561 €
Total Cost per Year		1.213.563 €	1.847.879 €	1.165.561 €
Savings				
Provisioning Savings		430.138 €	1.632.887 €	2.100.195 €
Savings from use of Workflow		309.881 €	1.069.275 €	1.283.845 €
Efficiency increase through RBAC (manual administration)		86.625 €	88.358 €	90.125 €
Saving Wait time		666.005 €	2.502.142 €	3.135.585 €
Saved training costs		73.914 €	24.564 €	11.492 €
Audit savings		41.869 €	42.706 €	43.560 €
Total Savings		1.608.432 €	5.359.932 €	6.664.802 €
Interest Rate		5%		
Return on Investment				
Total Cost (per Year)	1.650.000 €	1.213.563 €	1.847.879 €	1.165.561 €
Discounted total cost (per year)	1.650.000 €	1.155.774 €	1.676.080 €	1.006.855 €
Total Saving (per Year)		1.608.432 €	5.359.932 €	6.664.802 €
Discounted total saving (per year)		1.531.840 €	4.861.616 €	5.757.307 €
Net Saving (Balance)		394.869 €	3.512.053 €	5.499.241 €
Discounted Net saving (Balance)	-1.650.000 €	376.066 €	3.185.536 €	4.750.451 €
Discounted Net saving (cumulated)	-1.650.000 €	-1.273.934 €	1.911.602 €	6.662.053 €

Conclusion

Identity Management solutions provide countless approaches for concretely and reliably calculating benefits and Return on Investment. The focus is on the abolition or simplification of user administration. Increased end user productivity can also be an important benefit. This can be reliably measured if the effects of the non-availability of resources on the productivity of end users in a company can be assessed.

Another important area is increased security levels. These can be evaluated in money terms using risk management methods. One-off effects and long-term strategic benefits can also be demonstrated.

Legal regulations, the growing influence of security aspects on the corporate business model and the economic necessity to make business processes more efficient will all increase the importance of quantifying the benefits of Identity Management.

Literature

- [Chan03] Ramaswamy Chandramouli: A Policy Validation Framework for Enterprise Authorization. In: 19th Annual Computer Security Applications Conference, Las Vegas, Nevada, USA, Dezember 2003.
- [KKSM02] Axel Kern, Martin Kuhlmann, Andreas Schaad, Jonathan Moffett: Observations on the Role Life-Cycle in the Context of Enterprise Security Management. In: Proceedings of the 7th ACM Symposium on Access Control Models and Technologies (SACMAT 2002), Monterey, California, USA, S. 43-51, Juni 2002.
- [FeKu01] David Ferraiolo, Richard Kuhn: Role-Based Access Control, presented at 15th NCSC National Computer Security Conference, Baltimore, 1992.
- [KeKW02] Axel Kern, Martin Kuhlmann, Rainer Wick: Ein Vorgehensmodell für Enterprise Security Management. In Patrick Horster [Hrsg.]: Sichere Geschäftsprozesse, S. 81-90. IT Verlag für Informationstechnik, Höhenkirchen, September 2002.
- [Lewi03] J. Lewis: Enterprise Identity Management: It's about the Business. Burton Group Research Overview, Juli 2003.
- [Woeh02] G. Wöhe: Einführung in die Allgemeine Betriebswirtschaftslehre. Verlag Vahlen, 2002.
- [WeSK01] Tim Weitzel, Sertac Son, Wolfgang König: Infrastrukturentscheidungen in vernetzten Unternehmen – Eine Wirtschaftlichkeitsanalyse am Beispiel von X.500 Directory Services. Wirtschaftsinformatik 43 (2001) 4, S. 371-381.
- [KoBu01] Wolfgang König, Peter Buxmann: Das Standardisierungsproblem - Ein ökonomisches Entscheidungsmodell zur Auswahl von Standards. In: Wirtschaftsinformatik 40 (1998) 2, S. 122-129.
- [BrJR01] Matthew Brown, John S. Jordan, Eric S. Rosengren: Quantification of Operational Risk. Federal Reserve Bank of Chicago, Proceedings, 2002, issue May, S. 239-248.