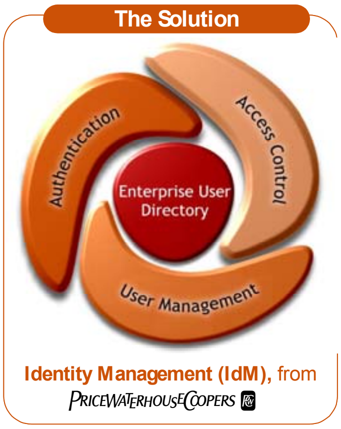
Identity Management

Marc Sel - 2003-01

Introduction

At first sight, identity management seems like a natural thing we all do within the ICT world as we do in the real world. After all, user-id's and passwords fairly well replace our natural credentials in such an electronic world. Or don't they?

In fact there are a wide range of situations where identity management and its components such as authentication and access control are not so trivial. Consider transactions where monetary value is involved. Or where medical records are updated. Or where sensitive items such as drugs for hospitals or arms for a policy force are traded. And the more granular you want your controls to be, the more complex their management becomes. Consider the exponentially increasing number of features to manage when you want to control access to a building, to an individual room, to a transaction, to a field in a database etc. Needless to say that in many cases, the situation is actually much less under control than desirable.



Identity Management (IdM), from PRICEWATERHOUSECOOPERS

On the other hand your reading of this article does not seem to imply much identity management. Unless the article would be published e.g. electronically, in a subscriber-only magazine, and the editor would like to be sure that only paying subscribers can read it.

State-of-the-Art

Historically, mainly user-ids and passwords were used to demonstrate a user's identity, with assistance of cryptographic techniques such as one-way hashes and encryption to protect their transport and storage. Access control was mainly an application-specific matter.

Today the state-of-the-art in identity management is built on a set of technologies, including smartcards and cryptography, with biometrics slowly moving to the foreground. The other key components are access control mechanisms, directories and user provisioning (i.e. making sure all users and their rights are adequately defined during their entire life-span in the systems).

For banking applications, smart cards became quite accepted as an authentication mechanism within Europe and many parts of Asia. Within private companies the use of smart cards is not (yet) so wide spread, mainly due to the overhead cost for buying readers and installing driver software. Smart cards are however in operation for access control in many different situations, including football stadiums such as the one at the Olympic sporting grounds in Barcelona. In countries such as Finland, Sweden, Estonia there are already national Electronic ID-cards in operation. In Belgium, the government allocated contracts for the various components of the system to different parties, and we will normally see the card being distributed from September 2003 onwards. For Belgium, a sophisticated Java-card from Schlumberger has finally been selected. This card will offer its owner two RSA keypairs, one for authentication (e.g. login) and another one for electronic signing of documents or transactions. Other countries such as Spain and Italy are performing pilot tests. And even the UK, where there is an historical distrust in identity cards, there seems consensus that the benefits today out wage the disadvantages, but it will still require a great deal of energy and political goodwill to introduce an identity card.

With regard to access control, there seems consensus that Role Based Access Control (RBAC) is the most realistic way forward. Unix/Linux, Microsoft Windows and SAP (to mention only a few of today's software components) all have this built in. It remains of course up to the user community to make sure that adequate roles are implemented. All of these systems come with some predefined roles, which need minor or major elaboration depending on the actual deployment. Also in this field, XML (eXtended Mark-up Language) technology is applied, and roles can in many cases be described via XML statements. Even more sophisticated XML use is achieved via SAML (Security Assertions Mark-up Language), which allows 'assertions' with regard to authentication or access control to be put in cryptographically secured XML statements. This allows their transmission over networks such as the Internet, which facilitates business-to-business co-operation in the context of e.g. federated portals.

Directories have been promoted to corporate level since users and services equally need a place to store their attributes. And since many companies depend on various technologies from different vendors, the quest began for a solution that was sufficiently universal. However, in the 1970's the public telecom operators launched X.400 email, which became the backbone for many successful EDI implementations. And from X.400 sprang the X.500 directory concept, which was universally acceptable, but far too rich in features to become successful. However, the X.500 access protocol (called the DAP or Directory Access Protocol) was taken onboard by the Internet community and turned into a lightweight version, called LDAP. Today LDAP-based directories are abundantly present, and most client software supports it. So we can now store large amounts of attributes for large amounts of user or service objects in a simple way, that everybody can access (if we chose to allow so).

Finally user provisioning is the process that allows the effective and efficient allocation of ICT resources (and optionally also others) to workers. It became quite common to provision users by actually storing their attributes in an LDAP tree, where these attributes can then be picked-up by the various applications. The provisioning process complements centralised policy setting with decentralised allocation of attributes by staff operating 'in the field' where appropriate.

Return on investment

The major reason why Identity Management is coming into the spotlights these days is the convergence of different factors leading to a cost effective solution of a real problem. The cost of establishing end-user accounts across different platforms and systems, the cost of updating multiple Name & Address Books and directories, the cost of providing helpdesk and problem management processes to support it, the cost of non-productivity when the system does not work, all quickly add up to six or more digit numbers. This is specially the case in an environment where there is a high turnover of staff, or where contractors are heavily used. Did you know that at various large Belgian companies, up to seventy or eighty persons are almost full-time working on keeping the authorisations 'in-sync' with the business needs?

The benefits arise from two facts: many companies don't know exactly how much they are paying to have their authorisations managed today, and their authorisations are actually badly managed as well. By leveraging a single solution, the operational costs can drop significantly. And the quality of the security service improves, because the decentralised workflow allocating the authorisations can be controlled with more granularity, while at the same time being enforced much faster.

For firms that employ Belgian citizens, incorporating the Belgian EID-card as an authentication token might actually add to the ROI. The government will take care of all aspects of card management. The efforts required by a company or SME will be reasonably limited, while the increase in new possibilities such as electronic archiving, document signing, etc, will be steep. Also the increase in security level will be very steep.

Conclusion

Identity Management is probably the first information security solution to achieve the promise of a measurable ROI. It is the answer to a challenge businesses have been grappling with for years: how to ensure security, increase productivity and reduce operating costs in an environment requiring an ever increasing flow of information within and across company borders via the Internet.