DATAMONITOR

# The ROI case for smart cards in the enterprise

## The benefits of a converged logical and physical access solution

A Datamonitor white paper prepared for


Publication Date: November 2004

www.datamonitor.com

**Datamonitor USA**
4th floor, 245 Fifth Avenue,
New York,
NY 10016
USA

t: +1 212 686 7400
f: +1 212 686 2626
e: usinfo@datamonitor.com

**Datamonitor Europe**
Charles House
108-110 Finchley Road
London NW3 5JJ
United Kingdom

t: +44 20 7675 7000
f: +44 20 7675 7500
e: eurinfo@datamonitor.com

**Datamonitor Germany**
Messe Turm
Box 23
60308 Frankfurt
Deutschland

t: +49 69 9754 4517
f: +49 69 9754 4900
e: deinfo@datamonitor.com

**Datamonitor Asia Pacific**
Room 2413-18, 24/F
Shui On Centre
6-8 Harbour Road
Hong Kong

t: +852 2520 1177
f: +852 2520 1165
e: hkinfo@datamonitor.com

# INTRODUCTION

This Datamonitor white paper illustrates the return on investment (ROI) argument for investment in secure access smart card-based solutions in the enterprise. The paper focuses on the ROI benefits of smart cards for both authenticating users to IT networks and systems (logical access) and controlling access to facilities (physical access), with a further assessment of converged solutions that combine the two. Datamonitor's analysis is supported by a recent survey of 53 enterprises in North America, which assesses the real and potential cost savings that can be realized from smart card deployments.

## *The importance of strong authentication*

The ability to verify a user's identity, typically referred to as authentication, has become an essential basis for trust in business relationships. Authentication establishes trust by proving the identity of a participant in any communication, or in the case of conducting electronic business, any transaction. Simply put, authentication solutions within the enterprise environment are designed to ensure that a person is who he/she claims to be.

Authentication solutions are typically used as the basis for critical security mechanisms such as access control. Based on the authentication of a user's identity, most enterprises have implemented business policies that define the relationships between authenticated users and information, through the control of access to applications and services. The authentication mechanism can also be integrated with solutions that understand who did what, where and when with the enterprise IT resources (auditing) and technology that customizes users' IT experience based on their trusted identities (personalization). In short, authentication and access control are both integral to what is now increasingly termed as identity management.

## *Uses for authentication solutions*

There are two primary uses for authentication solutions within the enterprise. These are:

- **Logical access** – Enterprises must ensure that they have effective mechanisms for controlling access to networks, systems and applications. Logical access solutions cover both on-site and off-site requirements and involve controlling employee access to personal computers (PCs), fixed and wireless local and wide

area networks, virtual private networks (VPNs) and databases, as well as other logical information assets. Two-factor security solutions (something you have and something you know) are increasingly chosen for stronger authentication and often involve the integration of digital certificates.

- **Physical access** – Authentication mechanisms can also be used as a means of restricting access to buildings and facilities. A prominent example would be the use of smart cards to control access to transit systems, though typically most smart card solutions are deployed on enterprise premises. Card-based physical access solutions have been deployed in a great number of enterprises, particularly large corporations.

Increasingly, enterprises are looking to deploy a **converged** solution, whereby the authentication mechanism is used for both logical and physical access.

### *Smart cards are the preferred identifier for many enterprises*

Enterprise IT departments have a variety of options in terms of the authentication solutions they can deploy to secure logical access. Among others, passwords, tokens, USB tokens, smart cards, digital certificates and biometrics can all be used either independently or in combination. When choosing an authentication solution, enterprise IT managers must weigh the various merits of each mechanism along a number of lines including the degree of relative security, total cost of ownership, convenience, ability to scale and cost.

The function of the smart card as a secure and reliable means of electronic identification means that it is the preferred identifier for many enterprises deploying secure access solutions. The microchip within the smart card can be used to store, protect and modify information, thereby offering flexibility and options for information sharing and transfer. Essentially, smart cards offer a number of credentials that can be used to identify an individual, including static and dynamic passwords, digital certificates and private keys, biometrics and pictures.

### *The benefits of smart cards*

Although the latter point may seem trivial, one of the inherent advantages of smart cards over tokens is that they are large enough to contain pictures of individuals. Indeed, of the various authentication mechanisms for logical access, smart cards are the only technology that offers a cost-effective solution for physical access in addition

to logical access. In short, smart cards are the preferred authentication mechanism for a converged logical and physical access solution.

As well as their inherent security capabilities, smart cards can be used to host multiple applications, enabling consolidation of services on one card, which promotes cost savings and efficiency.

Finally, smart cards also have clear advantages as a public key infrastructure (PKI) solution. Storing the private key on a smart card makes it far less vulnerable than on a PC desktop, and a card is more portable for users. In addition, smart card solutions typically involve less systems integration than a full public key infrastructure (PKI).

# THE VALUE OF DEPLOYING SECURE ACCESS SOLUTIONS

## The drivers for smart card-based solutions

Datamonitor identifies a number of factors that are driving the investment of secure access smart card solutions in the enterprise. These are:

- **The need for strong security.** The benefits of smart cards in providing strong two-factor authentication are well documented and it is this functionality that serves to generate interest in secure access solutions. Enterprises are spending increasing proportions of their IT budgets on security, in large part due to high volumes of sensitive and high-value information and the need to restrict access to it. The combination of something a user has (the smart card) and knows (a PIN or password), coupled potentially with the user's physical make-up (e.g. a fingerprint) is serving to ease enterprises' concerns in this area.

- **Improvements to the user experience.** Datamonitor believes that the user experience with regard to accessing networks, applications and, increasingly, devices can be significantly improved through the use of smart cards as a single sign-on tool. Smart cards provide an ease of use and convenience that may be lacking in other authentication mechanisms. In larger organizations, which have multiple buildings and a dispersed IT infrastructure, there is a great deal of value to be derived from deploying a common ID platform – offering one seamless means of user identification. The multi-application benefits of smart cards can also simplify corporate life.

- **Expanding access to corporate data.** There can be very little argument about the trend towards the expansion of access to information through the ever-increasing number of mobile workers and telecommuters, as well as the extension of corporate data to customers, suppliers and partners. With this comes the need to increase portable authentication credentials, especially given the increasing size and complexity of enterprise networks. Smart cards clearly fit this requirement.

- **Regulatory compliance.** Generally speaking, enterprises choose to deploy secure access solutions of their own accord, though regulatory compliance influences them to a limited extent. For example, the requirements relating to the security of patient data following the Health Insurance Portability and Accountability Act (HIPAA) has influenced uptake in the healthcare industry. Perhaps the greatest influence from government has been the deployment at the US Department of Defense, which provides a high-profile reference site.

- **Development of standards** A positive development for converged secure access solutions has come with the formation of the Open Security Exchange (OSE) in 2003. The initiative, which includes Siemens Communication, Inc., Siemens Building Technologies, Computer Associates, HID Corporation, Gemplus, Fargo, Sony and CoreStreet, aims to reduce the complexities relating to converged logical and physical access systems through standards development. Datamonitor considers developments in standards to be an important market driver, providing a common framework for secure access solution design.

- **The potential return on investment.** The introduction of secure access solutions has a number of cost implications. For example, smart card deployments can solve the problem of passwords, which can become unmanageable for users and administrators. Enterprises can also clearly reduce overhead costs through the improvement in efficiency gained from combining physical and logical access systems. It is the ROI advantages of secure access solutions that are discussed in more detail in turn.

## The importance of return on investment

The reality of the current economic environment is that decision factors for IT investments will be measured against the financial criteria of profits, costs and ROI. It is therefore important for enterprises to understand the potential financial returns that secure access solutions can generate. Datamonitor's analysis has identified a

number of hard dollar (tangible) and soft dollar (intangible) cost savings that may stem from the deployment of a secure access smart card solution.

## Identifying the return on investment argument

**Figure 1: ROI metrics for smart card-based secure access solutions**

| | Hard dollars | Soft dollars |
|---|---|---|
| Physical | • Ease of management versus alternative solutions.<br>• Reduction in staff costs – reduced requirement for staff members to manage access to facilities.<br>• Time savings and productivity benefits relating to quicker building entry.<br>• Ease of use in enabling temporary access to building facilities.<br>• Reduction in insurance premiums through enhanced physical access.<br>• Reduction in costs relating to lost keys (smart cards cheaper to replace/reissue). | • Costs associated with unwanted individuals gaining access and conducting industrial espionage.<br>• Costs relating to the replacement of stolen equipment after unwanted individuals have gained access to facilities.<br>• Increases in insurance premiums following equipment theft.<br>• Costs relating to lost time/production following equipment theft.<br>• Introduction of card-based solution reduces the potential risks relating to the authenticator being counterfeited.<br>• Enhanced employee satisfaction and improved security. |
| Logical | • Reduction in password-related help desk queries.<br>• General improvements to IT administration processes.<br>• Reduction in cyber risk insurance premiums for enterprises.<br>• Reduction in ongoing operational costs through card management systems.<br>• Time savings relating to the speeding up of authentication processes through simple sign-on.<br>• Adoption of additional card-based security e.g. PKI enables eBusiness processes and generates revenues (expanding business opportunities).<br>• Less expensive than other 2 factor solutions.<br>• Easier and less expensive maintenance of PKI certificates. | • Cost of security breaches (loss of data).<br>• Cost of security breaches (application downtime impacting revenue generation).<br>• Increased employee productivity from flexible (home) working and ease of use.<br>• Reduction in the threat of fines through meeting regulatory compliance.<br>• Reduction in fraud.<br>• Improved security for 2 factor PKI and biometrics.<br>• Supports multiple applications and federated IDs.<br>• Supports mobile PKI for authentication and digital signature.<br>• Scalability of card management systems allowing more cost effective future solutions.<br>• Enhanced perception among customers/partners. |
| Converged* | • Cost reductions from converged infrastructure (e.g use of one card versus many, one system versus disparate systems).<br>• Reduction in operational / provisioning costs.<br>• Additional staff cost reductions relating to the convergence of logical and physical access (e.g. merger of facilities and IT departments).<br>• Reduction in physical assets through convergence may benefit an enterprise's balance sheet.<br>• Deployment of multi-application smart card solutions encourages purchase of items and generates enterprise revenues. | • Multi-application benefits e.g. canteen, encourages users to log off thereby enhancing security functionality.<br>• Ease of interoperability with additional security systems e.g. event correlation, identity management.<br>• Improved user experience increases employee satisfaction.<br>• Support mergers and acquisitions via standard and flexible interfaces.<br>• Enables the deployment of new security applications.<br>• Quicker reporting of lost physical badges.<br>• Leverages current physical badging office.<br>• Speedier payments in the canteen.<br>• Reduced maintenance involved in handling cash within the enterprise. |

* Hard and soft dollar benefits for logical and physical access also apply to converged solutions

Source: Datamonitor DATAMONITOR

Figure 1 illustrates Datamonitor's perspective on the various ROI criteria that apply to the deployment of secure access solutions. Hard and soft dollar savings have been identified for logical, physical and converged access. Datamonitor notes that the hard and soft dollar benefits for logical and physical access also apply to converged solutions. More detail on each of these criteria is provided in turn.

*Physical access – hard dollar savings*

- **Ease of management versus alternative solutions** – The roll-out of physical access smart card solutions is typically coupled with the implementation of card management systems that involve card issuance, personalization, access rights, management and post-issuance. Such solutions simplify management processes, making them more cost-effective.

- **Reduction in staff costs** – By deploying a smart card-based authentication mechanism, there is a reduced requirement for staff members to manage and control access to facilities. This positively impacts an enterprise's costs associated with staff overheads.

- **Time savings and productivity benefits relating to quicker building entry** – An effective smart card-based physical access mechanism is likely to ensure that employees can save time during the course of a day. By ensuring quicker entry to facilities, enterprises will ultimately enhance employee productivity.

- **Ease of use in enabling temporary access to building facilities** – Any mechanism for temporary access that is inefficient and time consuming, may influence outsiders' perceptions of an enterprise. Effective card management systems will ease the process of issuance and are likely to impress visitors and contractors.

- **Reduction in insurance premiums through enhanced physical access** – By demonstrating a considerably reduced risk in terms of intruders gaining access to their facilities, enterprises can make marked savings on their annual insurance premiums.

- **Reduction in costs relating to lost keys** – Effective systems for smart card issuance ensure that cards can be simply replaced should they be lost or stolen. This is likely to come at a cheaper cost than alternative authenticators for physical access such as door keys.

*Physical access – soft dollar savings*

- **Costs associated with unwanted individuals gaining access and conducting industrial espionage** – Weak systems for physical access could ultimately lead to unwanted individuals gaining access to facilities and acquiring information that could impact the competitive performance of the enterprise.

- **Costs relating to the replacement of stolen equipment after unwanted individuals have gained access to facilities** – Enterprises require systems that minimize the prospect of equipment theft. Such occurrences could prove costly both in terms of the dollar value of replacing the equipment and the loss of data and information (e.g. stored on laptops).

- **Increases in insurance premiums following equipment theft** – Insurers are highly likely to raise their premiums in light of a major breach of security. Enterprises may therefore feel the effects of any security breach over a longer period.

- **Costs relating to lost time/production following equipment theft** – The effect of equipment theft is also highly likely to impact staff productivity in the short term, due to a lack of equipment and potentially any ensuing stress.

- **Introduction of smart card-based solution reduces the potential risks relating to the authenticator being counterfeited** – In comparison to door keys or magnetic stripe cards, the inherent security of smart cards, given their embedded microchips, ensures that they are far harder to counterfeit. It is not possible to put a figure on the potential damage that an enterprise could suffer following counterfeiting.

- **Enhanced employee satisfaction and improved security** – By issuing their staff with strong authentication mechanisms, enterprises are effectively investing in their employees' well being and demonstrating that they take security seriously. This may improve employee satisfaction and ultimately their productivity.

*Logical access – hard dollar savings*

- **Reduction in password-related help desk queries** – The deployment of smart cards can solve the problem associated with passwords. As well as providing relatively weak security, passwords can easily become unmanageable for users and administrators. An authentication mechanism viewed as 'free' can prove to be surprisingly costly in terms of ongoing management and support costs.

- **General improvements to IT administration processes** – The introduction of smart cards for logical access, coupled with a wider identity management solution, ensures that it is far easier to conduct employee provisioning and allocate roles. Card management systems also ease the process of logical access.

- **Reduction in cyber risk insurance premiums for enterprises** – By demonstrating a considerably reduced risk in terms of IT security breaches, enterprises will be able to reduce their spending on cyber risk insurance.

- **Reduction in ongoing operational costs through card management systems** – Card management systems can be used for card issuance, personalization, access rights, management and post-issuance. They are an important tool for managing applications throughout their lifecycle and serve to make smart cards more efficient operationally.

- **Time savings relating to the speeding up of authentication processes through simple sign-on** – Smart cards are an efficient and quick means of authentication in comparison to alternative mechanisms. Time wasted in this process is effectively dead time which ultimately translates into lost employee productivity.

- **Adoption of additional card-based security e.g. PKI enables eBusiness processes and generates revenues (expanding business opportunities)** – One of the many advantages of smart cards is that they can be used to store additional security applications. Enhanced security during communication with partners, suppliers and customers ultimately encourages online transactions and increased revenue generation.

- **Less expensive than other 2 factor solutions** – Smart cards can be acquired at an equivalent cost to USB tokens and digital signatures, and are cheaper than biometrical authentication solutions. The fact that they have multi-application benefits and can be used for physical access effectively further reduces their cost of acquisition.

- **Easier and less expensive maintenance of PKI certificates** – Smart card-based PKI solutions typically involve less systems integration than a full public key infrastructure (PKI) and, with the correct processes in place, are an easier means for administrators to update certificates.

*Logical access – soft dollar savings*

- **Cost of security breaches (loss of data)** – An enhanced authentication mechanism will protect enterprises from the potentially damaging consequences of lost or stolen data.

- **Cost of security breaches (application downtime impacting revenue generation)** – Equally, by deploying smart cards enterprises can ensure that the potential for enterprise applications to be disabled is reduced. Any security breach that impacts operational performance could potentially be disastrous.

- **Increased employee productivity from flexible (home) working and ease of use** – Enterprises increasingly recognize that they must give their employees the tools to work away from the office. VPNs are typically the preferred solution for remote access connectivity and they should always be coupled with strong authentication mechanisms.

- **Reduction in the threat of fines through meeting regulatory compliance** – In a corporate world increasingly dominated by compliance, enterprises are wise to deploy security solutions that protect them against the prospect of damaging financial penalties. An effective identity management solution, is likely to ensure that adequate auditing processes are put in place.

- **Reduction in fraud** – Strong authentication establishes trust in any communication or transaction by proving the identity of participants.

- **Improved security for 2 factor PKI and biometrics** – One of the advantages of smart card-based PKI and biometrical solutions is that storing the private key on a smart card ensures that it is far less vulnerable than on a PC desktop.

- **Supports multiple applications and federated IDs** – As well as their use for physical access and supporting applications such as secure payments, smart cards can also be used as a basis for collaborative web services. Effectively they can ensure single sign on that translates across multiple enterprises.

- **Supports mobile PKI for authentication and digital signature** – A further advantage of a smart card-based PKI solution is that storing the private key on the card ensures that it is more portable for users.

- **Scalability of card management systems allowing more cost effective future solutions –** Card management systems can be used to ensure that new applications are loaded on to cards over the course of their lifecycle. The fact that

they can be used for issuance and post-issuance management ensures that they can adapt to future enterprise requirements.

- **Enhanced perception among customers/partners** – Any solution that provides stronger authentication for interaction with customers and partners is certain to enhance the perception of an enterprise as a trusted third party.

*Converged access – hard dollar savings*

- **Cost reductions from converged infrastructure (e.g use of one card versus many, one system versus disparate systems)** – By converging logical and physical access, enterprises can clearly reduce costs relating to the operation of different systems. The costs associated with issuing and managing a multitude of authentication solutions (e.g. various badges and cards) will also be reduced.

- **Reduction in operational / provisioning costs** – Deploying directory-enabled smart card solutions ensures that it is far easier to conduct employee provisioning in a single process, as well as to disable users and/or applications on the system.

- **Additional staff cost reductions relating to the convergence of logical and physical access** – With the facilities and IT departments typically managed as separate departments, the introduction of a converged solution may lead to a reduction in overheads by combining departments, ultimately employing fewer personnel and improving operational management processes.

- **Reduction in physical assets through convergence may benefit an enterprise's balance sheet** – There may be scope for enterprises to reduce their on site infrastructure following a converged smart card deployment, most notably by streamlining the number of readers and badging offices. This may make a difference to the health of an enterprise's balance sheet.

- **Deployment of multi-application smart card solutions encourages purchase of items and generates enterprise revenues** – Vending machine throughput can be significantly enhanced through cashless payment mechanisms and a converged smart card solution is likely to encourage employee spending.

*Converged access – soft dollar savings*

- **Multi-application benefits, encourages users to log off thereby enhancing security functionality** – Security solutions are often only as effective as the practices of the employees. Equipping employees with multi-application smart cards ensures that their mindset is to carry their card at all times. This will serve to lock computers when employees are away from their desks.

- **Ease of interoperability with additional security systems e.g. event correlation, identity management** – By deploying standards-based smart card solutions, enterprises will be able to tie their investment into back-end event correlation and identity management infrastructures. The latter will ensure that enterprises can create, update and remove user identities and relate them to access control solutions.

- **Improved user experience increases employee satisfaction** – As discussed, employees may value the investment that a converged access solution brings, both from the perspective of better security and enhanced experience at work. Satisfied employees are typically more productive employees.

- **Support mergers and acquisitions via standard and flexible interfaces** – Standards-based smart card solutions tied into an effective identity management solution also ensure that enterprises have the flexibility to adapt to any changes in their business, particularly in relation to an expansion in the number of employees.

- **Enables the deployment of new security applications** – The basic functionality of smart cards as identifiers for secure access can be further enhanced through additional security applications such as PKI, digital signatures, VPN authentication, single sign-on, file encryption, web access control and secure email.

- **Quicker reporting of lost physical badges** – Given the multiple uses of smart cards within the enterprise, lost cards are invariably reported quicker than lost keys.

- **Leverages current physical badging office** – Effective converged smart card solutions should also be able to leverage existing investments and business processes, such as the approach to issuing and reissuing badges for physical access.

- **Speedier payments in the canteen** – By using a card-based mechanism for handling cash, employees may spend less time purchasing products, which may translate itself into more time working.
- **Reduced maintenance involved in handling cash within the enterprise** – Equally, canteen staff will be far more efficient without the requirement of cash handling at vending machines throughout the enterprise.

# DATAMONITOR SURVEY FINDINGS

## Background to the survey

In Fall 2004, Datamonitor conducted a survey of 53 enterprises in North America concerning a number of issues relating to logical and physical access. Interviews were conducted with IT and facilities managers within these organizations. Some of the most significant findings from the survey are illustrated in turn.

*Survey sample*

**Table 1: How many staff does your organization employ?**

| Number of staff employed | Count |
|---|---|
| 0 to 100 | 8 |
| 101 to 500 | 12 |
| 501 to 1,000 | 6 |
| 1001 to 5,000 | 14 |
| 5,000+ | 12 |
| Don't know | 1 |
| **Total** | **53** |

Source: Datamonitor DATAMONITOR

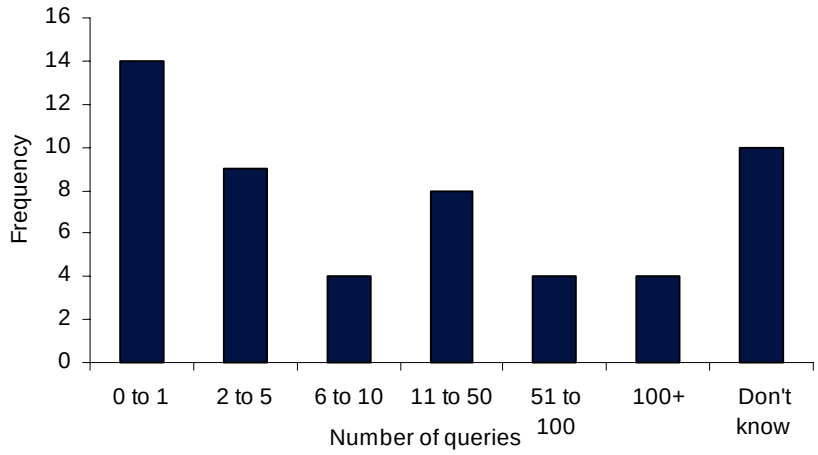
Datamonitor's sample was predominantly made up of medium and large organizations. The mean size of the organizations surveyed was 2,000 employees.

## Demonstrating return on investment

The survey investigated the return on investment arguments for investment in smart card-based secure access solutions for both physical and logical access. By questioning enterprises on issues relating to several of the aforementioned ROI criteria, Datamonitor's survey identifies real cost savings in a number of areas.

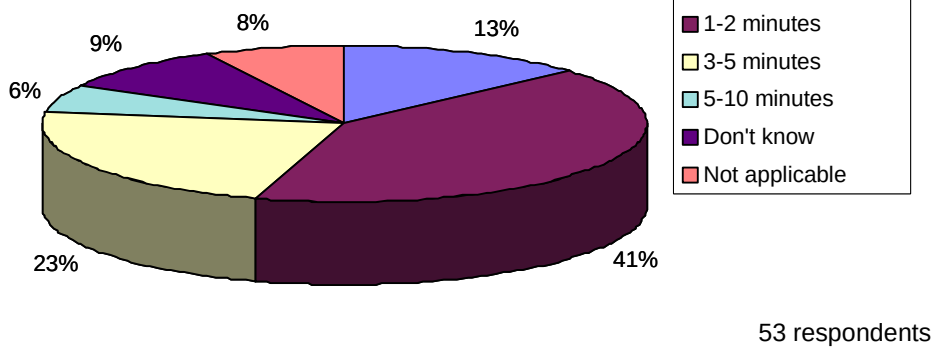
*The password problem*

**Figure 2: On average, how many password related helpdesk queries do your IT staff fulfill per day?**




Source: Datamonitor DATAMONITOR

**Figure 3: Typically how much time in minutes does a password-related help desk query take for one of your IT staff to fulfill per day?**




53 respondents

Source: Datamonitor DATAMONITOR

Figures 2 and 3 illustrate the password problem faced by many enterprises today. Datamonitor's survey indicates the volume and impact of password-related queries on IT staff's time.

The findings from the survey can be used to calculate the cost of password-related queries to an enterprise. Datamonitor's calculations and assumptions are as follows:

- By using the midpoint of the frequency ranges, an average of **23.5** password-related helpdesk queries are fulfilled by IT departments per day.
- By using the midpoint of the frequency ranges, password-related help desk queries take an average of **2 minutes and 26 seconds** to fulfill.
- For an enterprise with an average of 2,000 employees, therefore, the survey findings indicate that password related helpdesk queries take up **57 minutes and 11 seconds** of the IT department's time per day.
- If Datamonitor assumes an IT staff cost of $70 per hour, then the cost of password-related queries amounts to **$67** per day, **$335** per week and **$17,420** per year.

Datamonitor believes that focusing purely on labor costs, however, downplays the impact of passwords on an IT department. These figures do not take into the account the disruption caused by queries to an IT staff member's fulfillment of additional tasks,

neither the time required to undertake general maintenance of a password-based system.

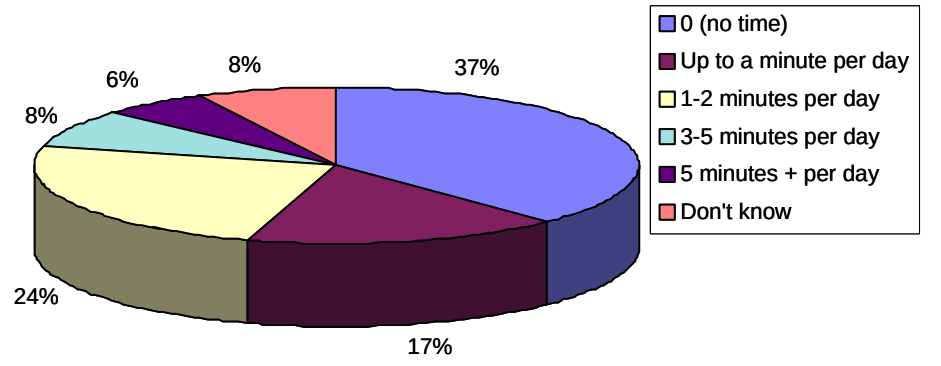
- Opinions differ regarding the cost to an enterprise per password query. Datamonitor estimates a typical password related call can cost an enterprise anywhere between **$10 and $40**, though notes that some large organizations are billing password resets internally at a cost of **$50** per reset.

- Assuming an average of **$25 per call**, therefore, the cost of password-related queries for an enterprise with 2,000 employees amounts to **$587** per day, **$2,935** per week and **$152,620** per year.

With a greater number of employees and hence password-related helpdesk queries, password management is clearly costing large enterprises hundreds of thousands of dollars per year in labor costs, not including lost employee productivity. A security solution that appears to be free is costing enterprises a material portion of their IT budget. In the context of increased scrutiny over IT budgets, enterprise IT managers should carefully consider the alternatives to a weak authentication mechanism that is taking up valuable IT department time.

*Improving employee productivity*

**Figure 4: How much time do you believe could be saved per person by introducing an enhanced mechanism for user sign on?**




53 respondents

Source: Datamonitor

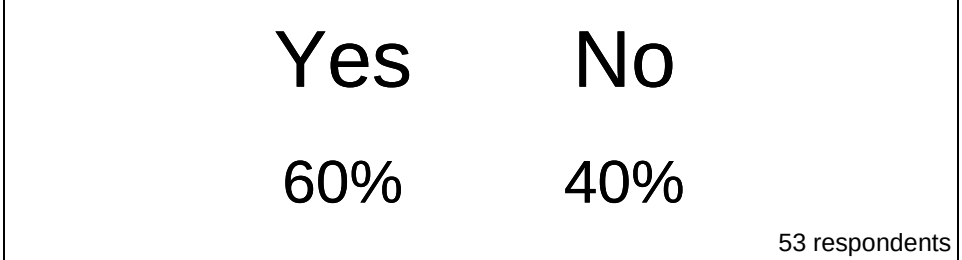
DATAMONITOR

Datamonitor's survey also addressed the extent to which an enhanced mechanism for user sign on could save an employee time. As figure 4 illustrates, over 50% of respondents believe that this would be the case. The findings from the survey can be used to calculate the associated potential cost savings from such a solution. Datamonitor's calculations and assumptions are as follows:

- By taking the midpoint of the frequency ranges, enterprises believe that they could save an average of **1 minute and 13 seconds** through an enhanced mechanism for user sign on.
- Assuming that each employee costs an enterprise $70 per hour, then this potential saving amounts to **$1.42** per employee per day.
- By taking the average number of employees (2,000) for the enterprises in the survey, this equates to a cost of **$2,833** per day, **$14,167** per week and **$736,667** per year.

It is clear that any technology that frees up even a relatively small amount of time could generate cost savings running into thousands of dollars.

**Figure 5: Would flexible home working increase the productivity of your employees?**




Source: Datamonitor

DATAMONITOR

In addition, Datamonitor has assessed the extent to which enterprises believe that home working would increase the productivity of their employees. 60% of the enterprises from the sample of 53 believe that this is the case. The survey, therefore, reaffirms that a high proportion of enterprises see the soft dollar benefits of home working. The smart card as an authentication mechanism is one potential means of enabling this process.

*Managing PKI certificates*

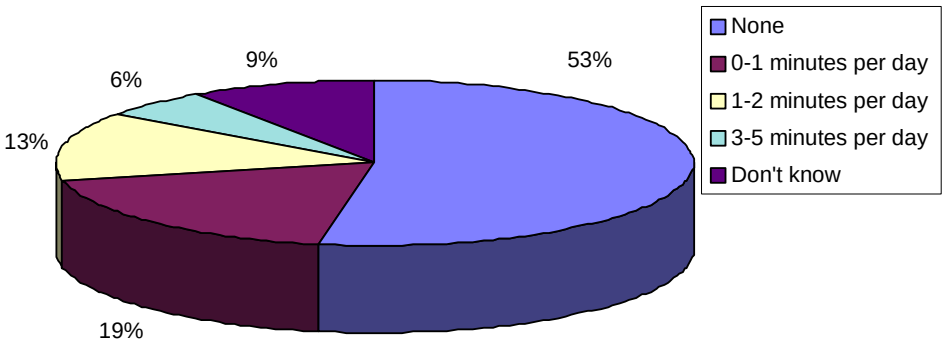
Datamonitor's survey highlighted some interesting anecdotal evidence concerning the benefits of managing PKI certificates through a smart card deployment. One prominent government department, which has implemented PKI as an authentication mechanism within its organization, estimates that between $101 and $500 per user per year is saved by managing PKI certificates through smart cards. With 800 employees in the department, and assuming a midpoint of $300 per user per year, this equates to an annual cost saving of $240,000. Scaling this figure up in line with Datamonitor's average enterprise of 2,000 employees and this equates to an annual cost saving of **$600,000**.

*Cost of IT security breaches*

A handful of enterprises in the Datamonitor survey admitted to having their IT security defences breached and data stolen due to unauthorized user access, such as a password breach. One enterprise, with 2,000 employees, estimated that this cost its organization **$100,000**, in large part due to application downtime.

*Quicker facilities access*

**Figure 6: How much time per person per day could be saved through quicker access to your buildings and facilities?**




53 respondents

Source: Datamonitor

DATAMONITOR

In terms of accessing buildings and facilities, figure 6 illustrates Datamonitor's survey findings relating to whether improvements to this process would lead to employee time savings. While 53% of respondents do not believe that there are potential time savings through quicker access to buildings and facilities, 38% do.

The combined survey results demonstrate, therefore, that there is a cost saving associated with an enhanced physical access mechanism. Datamonitor's calculations and assumptions are as follows:

- By taking the midpoint of the frequency ranges, enterprises believe that they could save an average of **34 seconds** per employee through quicker access to their buildings and facilities.
- Assuming that each employee costs an enterprise $70 per hour, then this potential saving amounts to **67 cents** per employee per day.
- By taking the average number of employees (2,000) for the enterprises in the survey, this equates to a cost of **$1,337** per day, **$6,684** per week and **$347,569** per year.

Once again, a small improvement in process can generate significant cost savings for medium and large organizations.

### *Other facilities benefits*

In addition, a number of the enterprises (23%) in the survey identified that staff costs would be reduced through the automation of access to buildings and facilities. These enterprises generally stated that they spend up to 25% of their facilities budget on staff costs. With the facilities budget of one organization with 2,000 employees amounting to $500,000 per annum, then a reduction of 25% would amount to a **$125,000** saving.

85% of the enterprises surveyed identified an annual cost relating to the replacement of lost keys / mechanisms for physical access. Although invariably a relatively small amount, 3 of the enterprises surveyed stated that this cost is over **$5,000** per annum. In addition, one government organization noted that its insurance premiums had fallen between 6% and 10% following the deployment of a smart card based physical access mechanism.

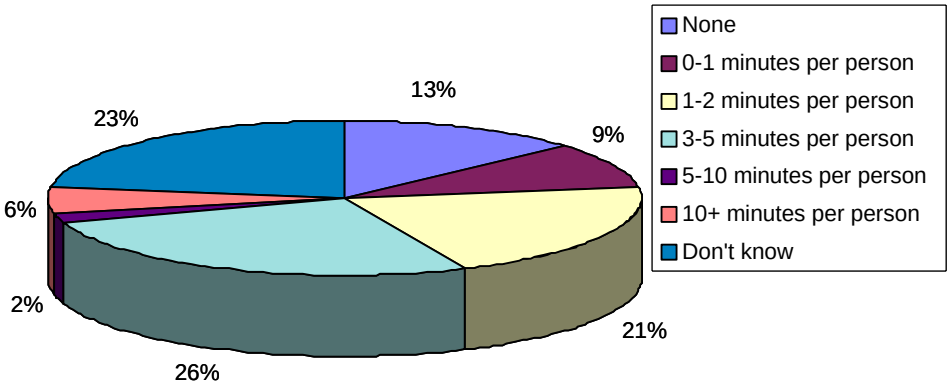
*Temporary access*

| Table 2: | On average how many people per day (whether visitors or contract staff) require temporary access mechanisms for physical access to your buildings and facilities? |
|---|---|

| Number of people | Count |
|---|---|
| 0 to 10 | 19 |
| 11 to 50 | 13 |
| 51 to 100 | 6 |
| 101 to 500 | 5 |
| 500+ | 3 |
| Don't know | 7 |
| **Total** | **53** |

Source: Datamonitor DATAMONITOR

**Figure 7: How much time does it take to issue a temporary access mechanism per person?**




53 respondents

Source: Datamonitor DATAMONITOR

Table 2 and figure 7 indicate the survey results for another important element of facilities management, the issuance of temporary access mechanisms to visitors and

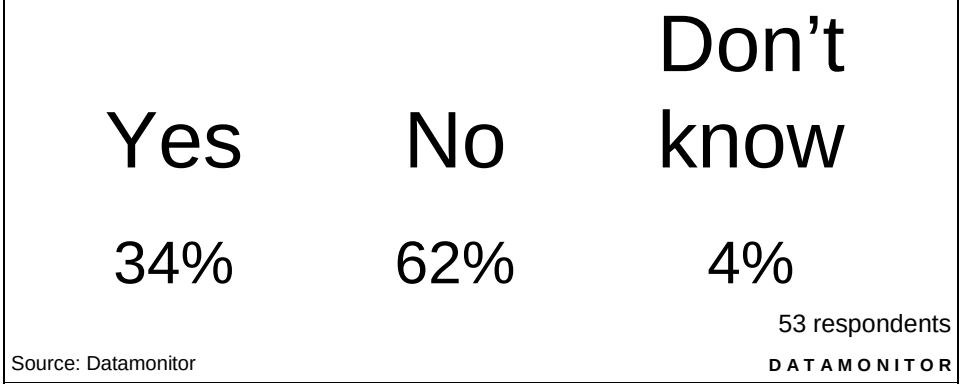
contract staff. Datamonitor's survey has quantified the regularity and impact of this process within enterprises. The results combined with Datamonitor's assumptions reveal the following:

- By taking the midpoint of the frequency ranges, an average of **86** people per day require temporary access mechanisms for an enterprise's buildings and facilities.
- By taking the midpoint of the frequency ranges, it takes enterprises **2 minutes and 45 seconds** to issue a temporary access mechanism per person.
- Combining these two results suggests that enterprises spend **3 hours 54 minutes and 43 seconds** issuing temporary access mechanisms every day.
- Assuming that the employee costs of those issuing the temporary access mechanisms are $70 per hour, then this equates to a cost of **$274** per day, **$1,370** per week and **$71,240** per year.

Although there will be time associated with issuing any mechanism for temporary access, one of the benefits of smart cards combined with card management systems is that this time can be reduced. For example, if Datamonitor assumes that it takes one minute to issue a smart card for temporary access, then this will save a 2,000-employee enterprise **$45,335** per annum.

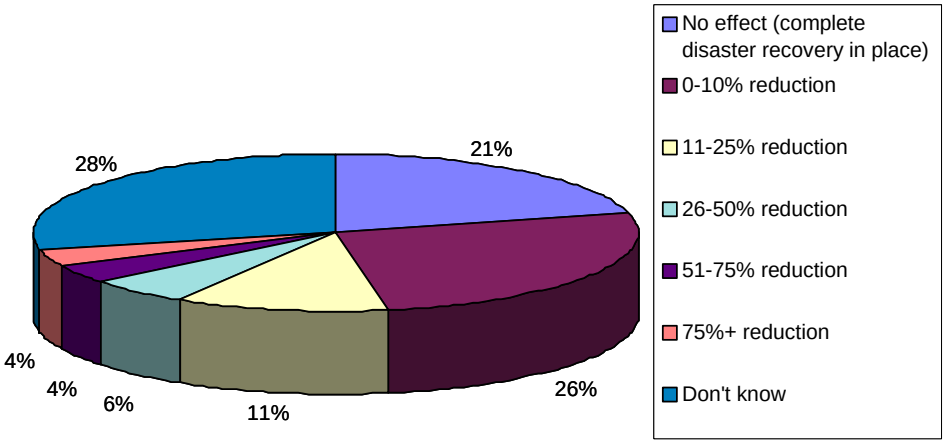
*Potential revenue loss*

**Figure 8: Is there potential to be fined for failure to meet industry regulations due to weaknesses in your processes for user access?**




Source: Datamonitor

**Figure 9: To what extent do you estimate your day-to-day revenues would suffer should your facilities be inaccessible / destroyed?**




53 respondents

Source: Datamonitor

DATAMONITOR

The Datamonitor survey also highlights some of the potential costs that could be associated with security weaknesses given certain scenarios. 34% of the enterprises surveyed believe that they could potentially be fined for failure to meet industry regulations due to weaknesses in their user access processes. It is hard to quantify how damaging this could be, though what it is clear is that many enterprises recognize this threat.

Enterprises have provided more tangible data relating to the impact of their facilities being inaccessible or destroyed. This could stem directly from weaknesses in both systems for logical and physical access. The survey results and Datamonitor's assumptions indicate the following:

- By taking the midpoint of the frequency ranges, enterprises estimate that their day-to-day revenues would decrease by an average of **15%** should their facilities be inaccessible or destroyed.

- The average annual turnover of those enterprises surveyed is $665 million (23 respondents). Assuming 52 working weeks and 5 working days per week this equates to daily revenues of $2.56 million.

- Should the average enterprise from the Datamonitor survey lose 15% of its daily revenues, therefore, this would equal **$384,000**. Over the course of a week, this would amount to **$1.92 million**.

Although this situation may prove to be very much a worst-case scenario, the point is very clear; enterprises could lose significant revenues should their security systems be breached. The ROI from introducing an effective security system to avert such a scenario would essentially be immediate.

### *Other benefits of convergence*

36% of the enterprises surveyed note a cost associated with provisioning both physical and logical access rights in terms of staff and infrastructure (such as user directories and user information stores). The majority of these enterprises recognise that these costs would be reduced should user-provisioning functions for logical and physical access be converged.

In addition, 25% of the sample commented that the introduction of a multi-application smart card would encourage increased spending on their premises, in some cases by up to $50 per user per week.

## Financial summary

Datamonitor's survey illustrates a number of potential cost savings associated with the deployment of smart cards for both logical and physical access. A summary of the various survey findings for an enterprise with 2,000 employees is provided below.

| | |
|---|---|
| **Annual cost savings** | |
| Cost of password-related queries for IT department | $152,620 |
| Time savings from enhanced mechanism for user sign on | $736,667 |
| Cost savings by managing PKI certificates through smart cards | $600,000* |
| Time savings through quicker access to buildings and facilities | $347,569 |
| Reduction in staff costs through automation of physical access | $125,000* |
| Costs relating to the replacement of lost keys | $5,000* |
| Cost savings from issuing smart cards for temporary access | $45,335 |
| Total | **$2,012,191** |
| **Additional potential costs** | |
| Cost of an IT security breach | $100,000* |
| Cost of facilities being inaccessible or destroyed for one day | $384,000 |
| Grand total | **$2,496,191** |

* Denotes gathered through anecdotal evidence.

Datamonitor notes that these savings will scale for enterprises with greater numbers of employees. An enterprise with 10,000 employees, for example, could generate annual cost savings of over $10 million. Although these savings do not factor in the cost of deployment and operation, the information gathered clearly illustrates that enterprises will generate significant cost savings over time by deploying a secure access smart card solution.

# WHAT SHOULD ENTERPRISES LOOK FOR FROM A SECURE ACCESS SOLUTIONS VENDOR?

Secure access smart card solutions will provide a range of potential benefits to an enterprise and the prospect of generating returns from any investment. Given some of the complexities of deployment, enterprises require technology partners with proven experience both in integration and business process change. Datamonitor's analysis identifies a number of characteristics that enterprises should look for from a secure access solution technology partner.

### *Broad range of solution offerings and capabilities*

No two secure access solutions will be the same. Enterprises have different legacy physical access mechanisms, different security needs in terms of the relative strength of security and different requirements for the multi-function capabilities of smart cards. Consequently, enterprises require vendors that can offer a comprehensive range of products and demonstrate flexibility in terms of their solution offerings. While packaged solutions are valuable, ultimately it is those vendors that can provide bespoke solutions that will add the most value.

### *Provide a migration strategy*

It is extremely important that vendors ensure that their solutions fit into a wider standards-based identity management solution. In this way, enterprises will be able to support biometrics or alternative technologies as they become available or are practical to integrate. Enterprises should also ensure that they do not invest in technologies that will become obsolete such as magnetic stripe and proximity technology. Given that solutions will often evolve, enterprises should work with a vendor that can demonstrate its longevity and state of health.

### *Scalable solutions*

Enterprises' requirement for an evolutionary outlook also involves a need for solutions to scale to a greater number of users, if required. Selecting vendors that can build or revise an internal identity management infrastructure coupled with card management systems will help enterprises in this regard. Solutions should be always be designed so that additional applications can be added over time.

*Expertise in integration*

Systems integration for secure access solutions may prove complex. Integrating card readers can be a challenge, especially since they must interface with legacy systems and applications. The need to make changes in the back-end, relating to the mainframe or network configuration for example, may also be necessary. If enterprises operate a combination of Windows 2000, NT, 98 and 95, this suggests a high degree of complexity in bringing logical network access under the same umbrella. In short, secure access solutions are not 'plug and play'. Rather the quality of the systems integration will often dictate the success of a project.

*Business process expertise*

Enterprises are now increasingly familiar with smart card technology, though knowledge of areas such as standards and an understanding of how smart cards can improve business processes is often lacking. Datamonitor notes that enterprises need advice and guidance on managing smart cards through their life-cycle, including knowledge of how to make post-issuance cost-effective. Enterprises should therefore turn to vendors that offer tailored education programs, can demonstrate process expertise, and illustrate how secure access solutions can solve business problems.

*Demonstration of ROI*

As this paper has illustrated, with over $2 million of potential cost savings for a 2,000-employee enterprise, one of the benefits of a converged physical and logical access solution is that it is possible to make a clear case for ROI. It should be a fundamental expectation for enterprises to expect a tailored and thorough walk through of the potential returns that can be generated from secure access smart card solutions.

## More than simply strong security

Ultimately, Datamonitor believes that enterprises should consider smart card-based secure access solutions as offering more than simply strong security. Enterprises should pay attention to those vendors that are able to promote the wider benefits of smart cards within the enterprise, highlighting potential cost savings and process improvements. Enterprises should also expect their considerations relating to management, users and budgets to be met. In short, the value of secure access smart card-based solutions is that they can protect business, enable business and provide a clear and tangible ROI.

## ABOUT SIEMENS

Siemens AG (NYSE:SI) is one of the world's largest global electronics and engineering companies with reported worldwide sales of $80.5 billion in fiscal 2003. Founded more than 150 years ago, the company is a leader in the areas of Information and Communications, Automation and Control, Power, Transportation, Medical, and Lighting. With its U.S. corporate headquarters in New York City, Siemens in the USA has sales of $16.6 billion and employs 65,000 people throughout all 50 states and Puerto Rico. Ten of Siemens' worldwide businesses are based in the United States. With its global headquarters in Munich, Siemens AG and its subsidiaries employ 417,000 people in 192 countries. For more information on Siemens in the United States: www.usa.siemens.com.

## ABOUT SIEMENS BUILDING TECHNOLOGIES

Headquartered in Buffalo Grove, Ill., Siemens Building Technologies, Inc., is one of 14 Siemens operating companies in the United States and is a leading single-source provider of cost-effective facility performance solutions for the comfort, life safety and security of some of the most technically advanced buildings in the world. In North America, Siemens Building Technologies employs 8,500 people and provides service from more than 100 locations.

## ABOUT SIEMENS INFORMATION AND COMMUNICATION NETWORKS GROUP

Siemens Information and Communication Networks Group is a leading provider of network and applications technology for enterprises, carriers and service providers. ICN's product strategy is focused on next-generation switching, next-generation access and next-generation optics. ICN's flagship brands are HiPath for enterprises, SURPASS® for carriers, and SpeedStream® voice, data and video broadband solutions for business and residential customers.

# ABOUT DATAMONITOR

Datamonitor plc is a premium business information company specializing in industry analysis.

We help our clients, 5000 of the world's leading companies, to address complex strategic issues.

Through our proprietary databases and wealth of expertise, we provide clients with unbiased expert analysis and in-depth forecasts for six industry sectors: Automotive, Consumer Markets, Energy, Financial Services, Healthcare, Technology.

Datamonitor maintains its headquarters in London and has regional offices in New York, Frankfurt and Hong Kong.