

**Overview**

This document illustrates the return on investment (ROI) argument for investment in smart cards in the enterprise. It focuses on the ROI benefits of smart cards for both logical access (authenticating users to IT networks and systems) and physical access (controlling access to facilities), with a further assessment of converged solutions that combine the two. Datamonitor's analysis is grounded in a survey of over 200 IT decision makers, conducted in Q4 2007, as well as an outline of ROI in three identifiable areas where smart cards may be operated. The survey has been spread across all enterprise sizes.

The document examines the case for consolidating different types of employee identification, identifies enterprises' approach to passwords and outlines the perceived benefits of smart cards. In addition, a basic ROI is calculated with Datamonitor's findings from the primary research.

**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 any transaction. Simply put, authentication solutions within the enterprise 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.

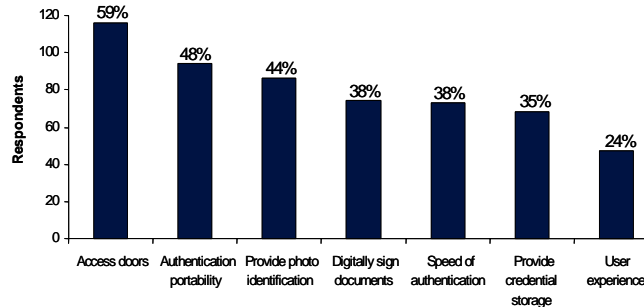
**Smart cards' value in the enterprise**

Smart cards are the ideal identifier for consolidating credentials

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 can hold 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.

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, Datamonitor considers smart cards to be the preferred authentication mechanism for a converged logical and physical access solution.

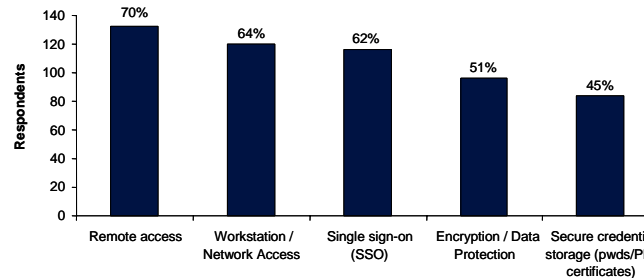
**Which smart card benefits could be relevant for your organization?**



Additional benefits of smart cards include:

- Smart card authentication is a far quicker process in comparison to one-time password tokens.
- Removing a smart card can lock a PC or workstation, enforcing security policy. Users are comfortable with this as authentication on returning is fast. Since one-time password token authentication takes longer, users are more likely to leave desktops unlocked when away from their desks.
- Since smart cards can store user credentials, users are able to travel with these credentials using different PCs/workstations. The smart card protects the credentials, which stay safe even if the card is lost.
- Smart cards can host multiple applications, enabling consolidation of services on one card, promoting cost savings and efficiency.
- Smart cards also have clear advantages as part of a public key infrastructure (PKI) solution. Storing the private key on a smart card is far more secure than on a PC desktop.

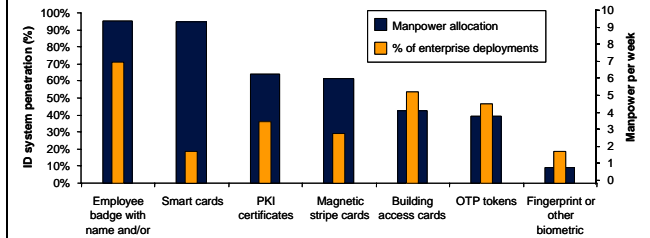
**Which smart card security apps have relevance to your organization?**



Smart cards' portability is clearly recognized, with around 70% listing remote access as being relevant. Dealing with home workers has become a reality in today's IT department: in a separate question, the survey found that very few enterprises (6%) have no home workers at all, while 44% have over 10% of their staff working at home at least once a week. With this in mind, it is clear that IT decision makers are looking for a strong authentication mechanism for remote access and that smart cards very often fit this bill.

**Man hour savings through smart cards**

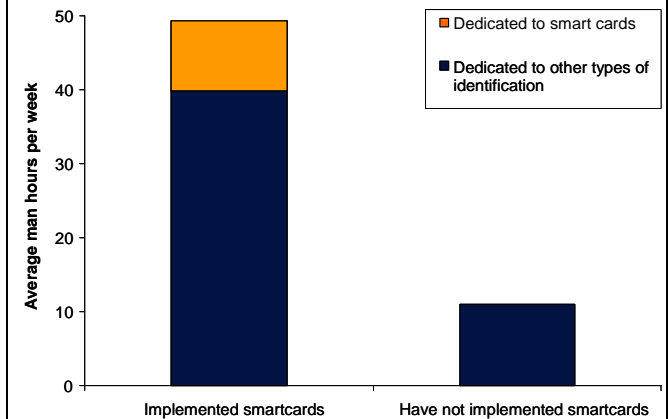
**Employee identification systems vary in terms of required manpower**



Datamonitor's survey reveals differing degrees of adoption of various types of employee identification systems. Deployment penetration ranges from 72% of enterprises operating employee badges to 15% using fingerprint or biometric technology. Smart cards are operated by a moderate 19% of the surveyed respondents, though this in large part reflects the fact that they are less relevant among smaller enterprises.

Of perhaps more interest is the manpower that is allocated to each of these employee identification systems. Enterprises reported that employee badges and smart cards are the most time consuming types of identification to manage, with both taking over a full working day of an individual's time. Although this may seem high in the case of smart cards, without a card management system, this identification type will invariably take some time to manage. Although the penetration of card management systems is currently low, as reflected by the survey, this is likely to change going forwards, with solutions like Identity Lifecycle Manager (ILM) 2007.

**Credential consolidation on a smart card saves man hours**



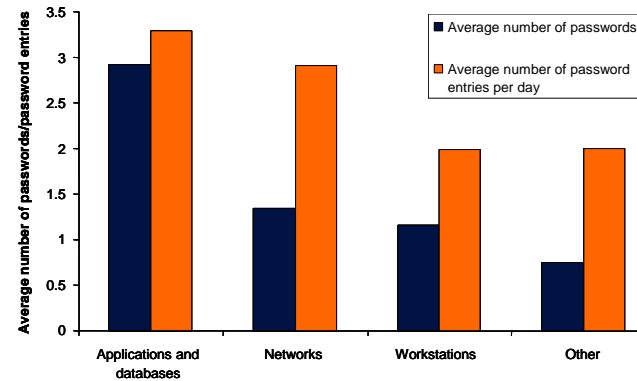
Further analysis of the time taken to manage smart cards reveals that, although enterprises may allocate an average of 9.5 man hours per week to this task, those enterprises that have deployed smart cards spend an even greater amount of time managing other identification types (such as passwords, tokens and proximity-only physical access badges).

A total of 39.79 hours is spent managing an average of 3 additional identification types, representing 13.26 hours per identification type on average. Smart cards may take a longer period of time on average to manage than other employee identification types but this has much to do with the fact that they are deployed by the type of enterprise that allocates more time to employee identification management.

Using a card management system like ILM 2007 to converge credentials, 39.8 man hours per week can be saved, representing the equivalent of one IT department staff member's annual salary.

### The problem with passwords

How many passwords do your users have in each of these areas? How many times do users enter passwords per day in these areas?

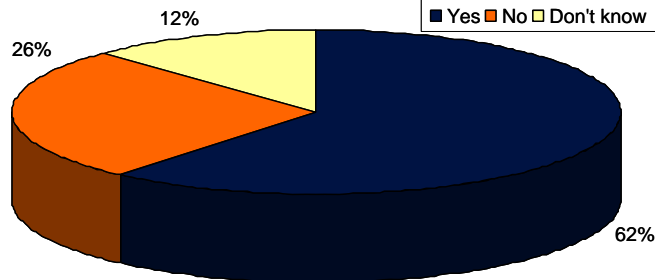


As well as their security weaknesses (they are often borrowed, lost or stolen), passwords are also an inefficient way for employees to identify themselves. Enterprises generally operate with different password systems (see above), with users entering passwords at various times in various systems. For those users accessing applications/databases & workstations as part of their role, the survey suggests that passwords must be entered 6 times a day on average. The survey is focused predominantly on mid-size enterprises, and this figure is likely to be closer to 15 passwords per user for organizations with 10,000+ employees.

### Passwords changes are a drain on the enterprise IT department

The survey also found that most enterprises' security policies dictate that users change their passwords at regular intervals, most typically either once a month (38.76%) or once a quarter (42.69%). This requirement represents a time-consuming administrative overhead for IT departments. Operating with a 2-factor authentication solution based around a PIN number, such as a smart card, could reduce the burden of password management.

### Have you experienced problems from passwords being shared, borrowed or stolen within your organization?



Most enterprises (62%) have experienced problems relating to passwords being shared, borrowed or stolen and the likelihood is that many of these problems would not have occurred with stronger forms of authentication.

### Identifying a return on investment argument

IT decision makers will invariably measure their investments against the financial criteria of profits, costs and ROI – hence they will want to understand the potential financial returns from smart card solutions. There are a number of hard dollar (tangible) and soft dollar (intangible) cost savings that stem from the deployment of logical, physical and converged access smart card solutions. Please note that the hard and soft dollar benefits for logical and physical access also apply to converged solutions.

#### Logical access: hard and soft dollar savings

Hard dollars	Soft dollars
<ul style="list-style-type: none"> <li>Reduction in password-related help desk queries.</li> <li>General improvements to IT administration processes.</li> <li>Reduction in ongoing operational costs through card management systems.</li> <li>Less expensive than other 2 factor solutions.</li> </ul>	<ul style="list-style-type: none"> <li>Cost of security breaches (data loss &amp; theft).</li> <li>Cost of security breaches (application downtime impacting revenue generation).</li> <li>Increased employee productivity from flexible working and ease of use.</li> <li>Reduction in the threat of fines through meeting regulatory compliance.</li> <li>Reduction in fraud.</li> <li>Improved security for 2 factor PKI and biometrics.</li> <li>Supports multiple applications and federated IDs.</li> <li>Supports mobile PKI for authentication and digital signature.</li> <li>Scalability of card management systems allowing more cost effective future solutions.</li> <li>Enhanced perception among customers/partners.</li> </ul>

#### Physical access: hard and soft dollar savings

Hard dollars	Soft dollars
<ul style="list-style-type: none"> <li>Ease of management versus alternative solutions.</li> <li>Reduction in staff costs – reduced requirement for staff members to manage access to facilities.</li> <li>Ease of use in enabling temporary access to building facilities.</li> <li>Reduction in insurance premiums through enhanced physical access.</li> <li>Reduction in costs relating to lost keys (smart cards cheaper to replace/reissue).</li> </ul>	<ul style="list-style-type: none"> <li>Enhanced employee satisfaction and improved security.</li> <li>Costs associated with unwanted individuals gaining access and conducting industrial espionage.</li> <li>Costs relating to the replacement of stolen equipment after unwanted individuals have gained access to facilities.</li> <li>Costs relating to lost time/production following equipment theft.</li> <li>Introduction of card-based solution reduces the potential risks relating to the authenticator being counterfeited.</li> </ul>

#### Converged access: hard and soft dollar savings

Hard dollars	Soft dollars
<ul style="list-style-type: none"> <li>Cost reductions from converged infrastructure (e.g use of one card versus many, one system versus disparate systems).</li> <li>Reduction in operational / provisioning costs.</li> <li>Additional staff cost reductions relating to the convergence of logical and physical access (e.g. merger of facilities and IT departments).</li> <li>Reduction in physical assets (e.g. reducing the number of readers and badging offices) may benefit an enterprise's balance sheet.</li> <li>Deployment of multi-application smart card solutions encourages purchase of items (e.g. by increasing vending machine throughput) and generates enterprise revenues.</li> </ul>	<ul style="list-style-type: none"> <li>Multi-application benefits e.g. canteen, encourages users to log off thereby enhancing security functionality.</li> <li>Ease of interoperability with additional security systems e.g. event correlation, identity management.</li> <li>Improved user experience increases employee satisfaction.</li> <li>Support mergers and acquisitions via standard and flexible interfaces.</li> <li>Enables the deployment of new security applications.</li> <li>Quicker reporting of lost physical badges.</li> <li>Leverages current physical badging office.</li> <li>Improved ability to perform investigations and remediation in case of misconduct.</li> </ul>

## Calculating a return on investment

Datamonitor provides basic ROI calculations for a physical, logical and converged access deployment. The examples below are based on an organization with 2,000 employees that is considering deploying smart cards instead of using one-time password (OTP) tokens.

### Physical access

A 2004 Datamonitor survey found that enterprises believe they could save an average of 34 seconds per employee through quicker access to their buildings and facilities. An enhanced physical access mechanism, such as a smart card, could therefore save on costs.

Net savings:

34 seconds x 2000 = 1,133 minutes = 18.88 hours per day

Savings per year (assuming \$70 / hour for all staff)

$$= (18.88 * 70 * 250 \text{ working days})$$

= \$330,400 savings per year

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

### Logical Access

The same 2004 Datamonitor survey found that enterprises believe that their employees could save an average of 1 minute and 13 seconds through an enhanced mechanism for user sign on such as a smart card.

Net savings:

73 seconds x 2000 = 2,433 minutes = 40.55 hours per day

Savings per year (assuming \$70 / hour for all staff)

$$= (40.55 * 70 * 250 \text{ working days})$$

= \$709,722 savings per year

### Converging credentials

Any system which reduces the number of times passwords are entered will have value from an efficiency point of view and resonate with the IT department which spends valuable time dealing with password-related queries and resets.

Where enterprises are operating a smart card, they may be dedicating time to manage other types of employee identification. The survey suggests that this is 39.8 man hours on average. Converging these credentials on to a smart card would clearly therefore lead to considerable net savings.

Net savings:

39.8 hours x 52 weeks = 2069.6 man hours/year

Administration Savings over 1 year (assuming \$75 / hour for IT staff)

$$= (2069.6 \text{ man hours}) * \$75 / \text{hour}$$

= \$155,220 savings per year

## Cost comparison with one-time password token

In order to focus on the difference between smart cards and tokens for remote access, a comparison will be drawn in terms of the cost of acquisition. Although hardware tokens vary in price, the majority of the market uses tokens that expire over a fixed period of time, and require a repurchase. The Manufacturer Suggested Retail Price for these tokens starts at \$56/token for 3 years for a basic model, meaning that two tokens must be purchased over the course of 3 years of service.

A smart card has neither an expiry date nor a battery which requires service, meaning that over the course of a 3 year period (and beyond), users can continue to use the same smart card. A smart card for remote access requires a reader, either connected to a computer or a standalone hand held reader. Without any volume discounts, a smart card costs an average of around \$19/card, with readers costing \$20/reader on average.

For simplicity, volume discounts will not be factored in. In Datamonitor's experience, customers will receive significant volume discounts at the 2,000 user level and above.

### Cost of token infrastructure / 3 years

Tokens (based on a 3 year token being replaced once over the course of 3 years)

$$(\$56 / \text{three year token}) \times (2 \text{ token} / \text{user}) \times (2,000 \text{ users})$$

Total 3 year cost of acquisition = \$224,000

### Cost of smart card infrastructure / 3 years

$$(\$19 / \text{smart card}) \times (1 \text{ smart card} / \text{user}) \times (2,000 \text{ users}) = \$38,000$$

$$(\$20 / \text{smart card reader}) \times (1 \text{ reader} / \text{user}) \times (2,000 \text{ users}) = \$40,000$$

Total 3 year cost of acquisition = \$78,000

Savings over 3 years = \$224,000 - \$78,000 = \$146,000

= \$48,666 average savings per year

## Summary

Datamonitor's survey of over 200 enterprises in EMEA coupled with its analysis of the market for secure access smart card solutions has revealed the following key findings:

- There are a number of hard (tangible) and soft dollar (intangible) savings that stem from a secure access smart card solution.
- Close to 40 man hours per week would be saved by enterprises in the survey were their ID credentials to be replaced by a smart card.
- Enterprises are generally operating different password systems for applications and databases, networks and workstations, representing an inefficient means of employee identification.
- 62% of enterprises have experienced problems relating to passwords being shared, borrowed or stolen from within their organizations.
- 80% of respondents recognize that smart cards would provide benefits to their organizations.

## Identity Lifecycle Manager 2007

Microsoft Identity Lifecycle Manager (ILM) 2007 provides an integrated and comprehensive solution for managing the entire lifecycle of user identities and their associated credentials. Its key capabilities include:

- A single administration point for digital certificates and smart cards
- The ability to support user self-service capabilities
- Configurable policy-based workflows for common tasks
- Detailed auditing and reporting capabilities
- Extensibility to support additional strong authentication technologies including OTP devices, physical access cards and biometrics
- Support for centralized, de-centralized and self-service scenarios
- Tight integration with Microsoft Certificate Services and Active Directory environments

The key business benefits of using an ILM 2007 based solutions approach include:

- Enhancing IT security through the use of strong authentication technologies
- Reducing the cost and complexity of deploying certificates and smart cards
- Facilitating stronger identity assurance and compliance enforcement
- Improving operational efficiency for user provisioning and credential management
- Reducing the help desk burden associated with user access and entitlement changes
- Leveraging your existing Microsoft IT infrastructure assets