

Smart Card Alliance

Logical Access Security: The Role of Smart Cards in Strong Authentication

A Smart Card Alliance Report

Publication Date: October 2004

Publication Number: ID-04002

Smart Card Alliance
191 Clarksville Rd.
Princeton Junction, NJ 08550
www.smartcardalliance.org
Telephone: 1-800-556-6828

About the Smart Card Alliance

The Smart Card Alliance is the leading not-for-profit, multi-industry association of member firms working to accelerate the widespread acceptance of multiple applications for smart card technology. The Alliance membership includes leading companies in banking, financial services, computer, telecommunications, technology, health care, retail and entertainment industries, as well as a number of government agencies. Through specific projects such as education programs, market research, advocacy, industry relations and open forums, the Alliance keeps its members connected to industry leaders and innovative thought. The Alliance is the single industry voice for smart cards, leading industry discussion on the impact and value of smart cards in the U.S. For more information, visit www.smartcardalliance.org.

Copyright © 2004 Smart Card Alliance, Inc. All rights reserved. Reproduction or distribution of this publication in any form is forbidden without prior permission from the Smart Card Alliance. The Smart Card Alliance has used best efforts to ensure, but cannot guarantee, that the information described in this report is accurate as of the publication date. The Smart Card Alliance disclaims all warranties as to the accuracy, completeness or adequacy of information in this report.

Smart Card Alliance Members: Members can access all Smart Card Alliance reports at no charge. Please consult the member login section of the Smart Card Alliance web site for information on member reproduction and distribution rights.

Government Agencies: Government employees may request free copies of this report by contacting info@smartcardalliance.org or by joining the Smart Card Alliance as a Government Member.

Table of Contents

EXECUTIVE SUMMARY	5
INTRODUCTION	7
OVERVIEW OF LOGICAL ACCESS	9
CURRENT METHODS FOR ACCESSING COMPUTER NETWORKS	9
DRIVERS FOR STRONGER LOGICAL ACCESS METHODS	10
<i>Administrative Costs</i>	10
<i>Security Risks</i>	10
<i>Risks of Legal and Regulatory Noncompliance</i>	10
<i>Privacy and Identity Theft</i>	11
<i>Technology Evolution and Migration</i>	11
THE ROLE OF SMART CARDS	12
OVERVIEW OF AUTHENTICATION TECHNOLOGIES	13
PASSWORDS	13
<i>Cleartext Passwords</i>	14
<i>Password Conversions</i>	14
<i>One-time Passwords</i>	16
BIOMETRIC FACTORS.....	17
PUBLIC KEY CRYPTOGRAPHY.....	18
SOFT TOKENS.....	18
SMART CARD TECHNOLOGY.....	19
SUMMARY	20
KEY CONSIDERATIONS FOR IMPLEMENTING STRONGER LOGICAL ACCESS AUTHENTICATION	21
BUSINESS ENVIRONMENT	21
BUSINESS TRANSFORMATION AND PROCESS RE-ENGINEERING	22
COST REDUCTION AND RETURN ON INVESTMENT	22
SECURITY AND PRIVACY	23
MANAGEMENT, USABILITY AND TRAINING.....	24
BENEFITS OF SMART CARD TECHNOLOGY FOR LOGICAL ACCESS	25
STRONG AUTHENTICATION.....	25
BUILT-IN SECURITY	26
ENHANCED SECURITY AND CONVENIENCE FOR USERS	26
ENHANCED PROTECTION AGAINST IDENTITY FRAUD	27
STANDARDS-BASED APPLICATION COVERAGE	28
EASE OF INTEGRATION	29
EASE OF DEPLOYMENT	30
MULTI-PURPOSE FUNCTIONALITY.....	30
SMART CARDS AS SMART ID BADGES: AN EXAMPLE SCENARIO.....	32
ADVANTAGES OVER OTHER LOGICAL ACCESS ALTERNATIVES	33
SMART CARDS AND THE IT INFRASTRUCTURE	35
MICROSOFT WINDOWS	35
<i>Smart Card and Reader Communications</i>	35
<i>User Authentication</i>	37
<i>Web and E-mail Services</i>	37
<i>File System Encryption</i>	37
<i>Support Offered by Different Windows Versions</i>	38
LINUX	38
<i>Smart Card and Reader Communications</i>	38

<i>User Authentication</i>	39
<i>Web and E-mail Services</i>	40
<i>File Encryption</i>	40
<i>Support Offered by Different Varieties of Unix</i>	40
USING SMART CARDS FOR MULTIPLE APPLICATIONS	41
MULTI-APPLICATION USAGE	41
<i>Physical Access Control</i>	41
<i>Payment</i>	42
<i>Secure Data Storage and Management</i>	43
<i>Wireless Network Access</i>	43
APPLICATION INSTALLATION	43
MULTIPLE APPLICATION EXAMPLES	44
THE BUSINESS CASE FOR SMART CARDS AND LOGICAL ACCESS	45
INTANGIBLE BENEFITS	45
<i>Regulatory Compliance</i>	45
<i>Strategic Positioning</i>	45
TANGIBLE BENEFITS	46
<i>Simplified User Management</i>	46
<i>Elimination of OTP Tokens</i>	46
<i>Reduction of Overall Infrastructure</i>	46
<i>Increased Productivity</i>	47
INVESTMENT	47
CONCLUSIONS	49
REFERENCE AND RESOURCES	50
PUBLICATION ACKNOWLEDGEMENTS	52
APPENDIX A: SMART CARD USER PROFILES	54
BOEING'	54
MICROSOFT	55
RABOBANK	56
SHELL GROUP	57
SUN MICROSYSTEMS JAVABADGE	58
U.S. DEPARTMENT OF DEFENSE	60
U.S. DEPARTMENT OF STATE	61
APPENDIX B: INDUSTRY INITIATIVE PROFILES	63
ELECTRONIC AUTHENTICATION PARTNERSHIP	63
LIBERTY ALLIANCE PROJECT	63
INITIATIVE FOR OPEN AUTHENTICATION	64
OPEN SECURITY EXCHANGE	64
OPENCARD CONSORTIUM	65
APPENDIX C: DEFINITION OF TERMS AND ACRONYMS	66

Executive Summary

Passwords Provide Insufficient Security for Logical Access to Networked Resources

Organizations of all sizes and in all industries are anxious to improve the process used to identify users to their networked systems. With the growing use of wired and wireless networks to access information resources and the increasing occurrence of identity theft and attacks on corporate networks, password-based user authentication is increasingly acknowledged to be a significant security risk. Passwords are typically controlled by the password owner, who can use easily guessed passwords, share passwords with others, write passwords down, or use the same password to access multiple systems. In addition, storing password data on corporate networks introduces additional vulnerability to attackers who gain network access.

Password management is a significant cost to organizations. Industry statistics show that 30% to 50% of information technology (IT) help desk resources are consumed by managing and resetting passwords.

Both enterprises and government agencies are moving to replace simple passwords with stronger, multi-factor authentication systems that strengthen information security, respond to market and regulatory conditions, and lower support costs.

A Variety of Technologies Can Authenticate Users for Logical Access

Technologies used to authenticate individuals for logical access include passwords (with a number of variations – cleartext, encrypted, one-time), symmetric keys, asymmetric public/private keys, and biometric data. Individuals typically prove their identity using a single authentication factor. However, strong identity authentication requires the use of two or three factors, such as something you have (a physical item or token in your possession), something you know (information only you know), or something you are (a unique physical quality or behavior that differentiates you from all other people).

Smart cards support all of the authentication technologies, storing password files, public key infrastructure certificates, one-time password seed files, and biometric image templates, as well as generating asymmetric key pairs. A smart card used in combination with one or more authentication technologies provides stronger multi-factor authentication and significantly strengthens logical access security. Smart card technology also provides the flexibility for including all authentication factors in a single smart card, improving the security and privacy of the overall authentication process.

Smart Card Technology Provides Significant Advantages for Implementing Stronger Authentication

Smart card technology significantly strengthens security, protecting both the electronic credential used to authenticate an individual for logical access and the physical device. Since the credential is permanently stored on the card, it is never available in software or on the network for an unauthorized user to steal. Smart cards build protection into the physical device by supporting tamper-resistant features and active security techniques for encrypting communications.

Smart cards are becoming the preferred method for logical access, not only for their increased security, but also for their ease of use, broad application coverage, ease of integration with the IT infrastructure, and multi-purpose functionality. Both Microsoft® Windows® and Unix® operating systems offer a significant level of smart-card-related support and functionality, through either built-in (out-of-the-box) support or commercial add-on software packages. Smart-card-based logical access allows organizations to issue a single ID card that supports logical access, physical access, and secure data storage, along with other applications. By combining multiple applications on a single ID card, organizations can reduce cost, increase end-user convenience, and provide enhanced security for different applications.

Smart card technology provides organizations with cost-effective logical access. Smart cards deliver a positive business case for implementing any authentication technology. Improved user productivity, reduced password administration costs, decreased exposure to risk, and streamlined business processes all contribute to a significant positive return on investment.

About This Report

This report was developed by the Smart Card Alliance to provide a primer on the authentication technologies used for logical access and to describe how smart cards strengthen authentication processes.

Designed as an educational overview for decision-makers, the report provides answers to commonly asked questions about the use of smart cards for logical access, such as:

- Why are organizations looking for strong authentication solutions for logical access to networked resources?
- What authentication technologies are available and how do they compare to each other?
- How are smart cards used for authentication and what benefits do they bring to an organization?
- How are smart cards integrated into the IT infrastructure?
- What is the business case for using smart cards for logical access?
- What other applications can be supported using smart card technology, and how does a multi-function card benefit the organization?

The report includes profiles of organizations currently using smart ID cards for logical access, including Boeing, Microsoft, Rabobank, Shell, Sun Microsystems, U.S. Department of Defense, and U.S. Department of State.

Introduction

In today's workplace, secure logical access is a critical concern. The Internet has enabled effective electronic collaboration among partners, customers, and suppliers. New technologies allow mobile workers to communicate outside of traditional security perimeters, using wireless technology or working remotely over a virtual private network (VPN). Increasing operational efficiencies motivate increasing numbers of enterprises and service organizations (such as banking, health, and insurance companies) to migrate to an enterprise network composed of corporate portals, application servers, and protected Web resources. The rising incidence of identity theft and advent of new regulations and legislation, such as the Health Insurance Portability and Accountability Act (HIPAA), Sarbanes-Oxley Act, and Gramm-Leach-Bliley Act, also contribute to an environment in which secure logical access is extremely important. For all of these reasons, organizations who manage user identities, authentication policies, and user privileges are challenged to prevent intruder access to proprietary information.

The current password-based logical access infrastructure fails to address these new threats, new business models, and the growing complexity of networked resource access. Passwords are costly to manage (an estimated 30% to 50% of help desk costs are attributable to resetting passwords) and can be cracked using widely available tools. The security concerns raised by password-based systems and the added convenience that smart cards provide may be two major reasons why organizations are moving to smart-card-based logical access systems. According to a Frost & Sullivan survey,¹ 39% of Fortune 500 companies plan to use smart cards within 3 years and 63% of Fortune 500 companies either have investigated or are investigating smart cards for network security implementations.

Smart card technology is available in multiple form factors – as a plastic card, a Universal Serial Bus (USB) token, or a Subscriber Identification Module (SIM) in a mobile phone. Each has a semiconductor chip that can carry a microcontroller, crypto-coprocessor, memory, operating system, and application software. A smart card's computing capability rivals that of the first personal computer (PC); smart cards have all of the features of a PC except a keyboard and monitor. Microcontroller-based smart cards are also designed to resist attack using a variety of countermeasures built into the chip by the manufacturer, making it unlikely that data stored on the smart card will be exposed, stolen, modified, or destroyed. The unique ability of smart cards to provide secure data storage and support sophisticated cryptographic functions make them the best choice for authenticating individuals requesting logical access.

Smart card technology has advanced over the last 20 years to include improved storage and processing capacities, enhanced security, mature smart card management software, contactless technologies, and integration of multiple applications in a single smart ID badge. Smart cards can support a variety of applications used by organizations, including Windows logon, password management, one-time passwords (OTP), VPN authentication, e-mail and data encryption, electronic signatures, enterprise single sign-on, secure wireless network logon, biometric authentication, cafeteria payments, personal data storage, role-based access, secure physical access, and

¹ "Fortune 500 Companies' Preference for Corporate Security Applications," Frost & Sullivan, Feb. 17, 2003

customer loyalty. Today, smart cards are essential to the security backbone of an organization's identity management system, supporting the strong authentication required to validate individuals accessing networked resources and providing a critical first step in blocking intruders.

The standardization work accomplished by Global Platform and the Government Smart Card Interoperability Specification (GSC-IS) enables card issuers to combine solutions from multiple sources, thus ensuring large-scale interoperability and reducing the costs of ownership by providing an open market. Because significant investment is still required to integrate new authentication systems into a legacy infrastructure, ongoing commitment by top executives and dedicated project management are required to make new identity management system deployments successful. Organizations who adopt smart cards for logical access see a strong return on investment and significant benefits, including improvements in convenience and security, greater accountability and better security decisions, regulatory compliance, operational efficiencies, and new business opportunities.

This report explains the concepts necessary to understand what authentication technologies are used for logical access and how smart cards can be used to make logical access more secure. Many organizations have successfully deployed smart cards in their logical access systems, and profiles of seven of them – Boeing, Microsoft, Rabobank, Shell, Sun Microsystems, U.S. Department of Defense, and U.S. Department of State – are included in the appendix of this report.

Overview of Logical Access

Logical access is the process by which individuals are permitted to use computer systems (which can include other digital devices such as PDAs and mobile phones) and the networks to which these systems are attached (such as corporate local and wide area networks, telecommunications networks, intranets/extranets, and wireless networks). The objective of secure logical access is to ensure that these devices and networks, and the services they provide, are available only to those individuals who are entitled to use them. Entitlement is typically based on some sort of predetermined relationship between the network or system owner and the user, as a paying subscriber, an employee, a customer, or some other type of binding relationship.

The system that supports delivery of such networked services represents a significant investment; in fact, this system may represent the single largest asset that the owning organization has. These assets require protection from unauthorized use by individuals or entities who may diminish or destroy their value. Therefore, controlling access to these assets is of paramount importance to virtually all organizations that rely on information technology (IT) systems to accomplish their objectives.

Current Methods for Accessing Computer Networks

The most widely implemented method for controlling logical access is the user ID–password combination. Users provide the user ID (usually the user's name) and a secret that only the user knows (usually a password). A simple database lookup determines that the password is attached to the user ID, authenticates the user's identity, and grants access. Each system or application typically assigns a unique user ID and password combination to each user and then determines access controls for that user based on the unique ID.

Over time, however, this type of authentication has proven to be weak and inefficient. User IDs and passwords can be compromised relatively easily through a variety of well-known techniques. When such information is obtained by criminal elements, it can be used to achieve unauthorized and illegal entry into a network. The results of compromised access controls can be disastrous for the network owner and for the user whose network or system identity is stolen. In addition, user identities are typically managed application by application, creating operational inefficiencies as the number of systems and applications in an organization grows and introducing security vulnerabilities as it becomes increasingly difficult to control policies governing the use of those identities.

Fortunately, new technologies are available that can strengthen the authentication process supporting access control and provide a higher level of assurance that users are who they claim to be and that the identity credentials presented are valid. These technologies, which are described in the following sections, generally employ encryption techniques, biometric data of some sort, and/or the possession of a physical token or credential to improve the effectiveness of access control systems. Unlike the use of a single factor (i.e., user ID–password combination), strong authentication requires the use of two or three factors to validate identity. Factors would include some combination of something you know (a password or personal identification number that only you know), something you have (a physical item or token in your possession) and something you are (a unique physical quality or behavior that differentiates you from all other individuals).

Using stronger authentication technologies and multiple authentication factors mitigates potential loss due to unauthorized access to network assets.

Drivers for Stronger Logical Access Methods

Compromised security is not the only reason for seeking improved logical access control techniques. Other drawbacks of the user ID–password combination include high administrative costs, inadequate ability to manage different risks, and inability to leverage the additional security that is now being built into computer systems and applications.

Administrative Costs

As users access increasing numbers of network services, each requiring a separate user ID and password, the user's ability to manage and remember required access information breaks down. As a result, users either write the information down, which makes it vulnerable, or call their network administrators. Administrators must regularly deal with service calls from users who have forgotten their user ID–password combination.

Such service calls are expensive and are becoming more so, as the services provided through a multitude of expanding networks increase. Several sources estimate that a single call to an administrator to reset a forgotten password costs approximately \$40. The costs associated with supporting this method of authentication and access control are driving network administrators to look for solutions that are more efficient, as well as more secure.

Security Risks

Recently, reports of unauthorized individuals breaking into computer networks to steal information for financial or political purposes have multiplied.

In the private sector, the impact of such security breaches is measured in terms of both financial loss and loss of customer confidence. In government circles, the risk is magnified by the potential effect on national security and the impact on the public's trust and confidence in critical government institutions.

As more intrusions take place, the ability to quantify their negative impact is improving. Institutions in both the public and private sector are better able to analyze the costs and benefits of investing in new technologies to improve network security, including technologies to improve access control, and are able to justify doing so based on solid return on investment.

Risks of Legal and Regulatory Noncompliance

In the aftermath of the September 11 terrorist attacks, a significant amount of new legislation was passed, primarily aimed at improving the security of computer networks owned and managed by the Federal Government. Additional legislation promotes the adoption of systems that deliver government services electronically. One critical part of these initiatives is support for the logical authentication of individuals trying to access such services.

As a result, network security and the mechanisms by which users are granted access to government-controlled assets have moved to the top of the government agenda. Policy and implementation guidelines define the various levels of authentication that are needed based on the sensitivity of

the information being accessed, and a variety of candidate technology options have been identified, ranging from user IDs and passwords to public key infrastructure (PKI), biometrics, and smart cards. Many U.S. government agencies have already put in place programs to issue smart ID cards that support stronger authentication techniques for both physical and logical access.

The government already requires contractors to meet government-specified standards for security technologies, policies, and practices. The trend is for the private sector to adopt technologies and practices put in place by the government, not only as an example of best practices, but also as a means of mitigating any legal risk that may be incurred by nonconformance. Businesses are also subject to a number of new requirements for access control and audit, as a result of new laws or regulations such as the Gramm-Leach-Bliley Act, HIPAA, the Sarbanes-Oxley Act, and the USA Patriot Act.

Privacy and Identity Theft

According to the Federal Trade Commission,² in the last 5 years 27.3 million Americans were victims of identity theft, with businesses and financial institutions losing nearly \$48 billion to identity theft and consumer victims reporting \$5 billion in out-of-pocket expenses. Attacks on consumers' computers, through "phishing" and other virus and "spyware" attacks, constitute new ways to steal usernames and passwords. Gartner reports that more than 1.4 million U.S. adults have suffered from identity theft fraud due to phishing attacks, costing banks and card issuers \$1.2 billion in direct losses in the past year.³

As privacy and identity theft become larger issues (and are addressed by legislation at the state and national level), the private sector will have to move toward stricter controls on customer databases and the personal information that companies are entrusted to protect. Companies will need to control access to sensitive information and ensure that such information is only accessible to those with the proper authorization.

Technology Evolution and Migration.

Because of the increasing demand by IT users for improved access control mechanisms, IT solution providers are building more security into their products to provide native support for modern authentication solutions. For example, support for PKI logon and encrypted and digitally signed e-mail is now native to Windows. More and more products from a wide variety of vendors enable the use of PKI, biometric, and smart card technologies to support strong authentication methods using multiple factors.

As computer systems are refreshed and upgraded over time, support for strong authentication through multiple technological approaches will be more readily available. The result should be increasingly widespread use of strong authentication techniques, higher levels of security assurance, and greater user convenience.

² "FTC Releases Survey of Identity Theft in U.S. 27.3 Million Victims in Past 5 Years, Billions in Losses for Businesses and Consumers," Federal Trade Commission press release, Sept. 3, 2003, <http://www.ftc.gov/opa/2003/09/idtheft.htm>

³ "Phishing Victims Likely Will Suffer Identity Theft Fraud," Gartner press release, May 14, 2004, http://www3.gartner.com/5_about/press_releases/asset_71087_11.jsp

The Role of Smart Cards

Smart card technology can play a pivotal role in solutions that provide strong authentication, improve network security, and protect the identities and privacy of individuals. As a cryptographic device, the microcontroller at the heart of the smart card can support a number of security applications and technologies. Smart cards offer secure data storage and support the strong authentication approaches required to access that data, including the following:

- Support for PKI and asymmetric key applications (e.g., digital signatures, e-mail message encryption), on-card key generation, and protection for the privacy of the user's private key
- Secure storage for biometric templates
- Secure storage for user IDs and passwords
- Support for one-time password generation
- Secure storage for symmetric keys
- Support for other applications, such as physical access control or financial transactions

In the card form factor, smart card technology can also be used in a multi-function smart ID badge, providing a visual ID card as well as enabling automated, authenticated physical and logical access.

Overview of Authentication Technologies

In the story *Ali Baba and the Forty Thieves*, a treasure stolen by 40 thieves is hidden in a cave protected by a magic stone. The only way to enter the cave is to speak the secret password, "Open Sesame." It doesn't matter who the speaker is. Those words, said in that exact form, cause something magical to happen, moving the stone and allowing the speaker to enter.

That same magic happens every time someone logs on to a computer network. The importance of authentication cannot be overstated. Once a person is authenticated to the network, the person's privileges and access rights are based on that authentication. The purpose of authentication is therefore to permit network access to everyone who is authorized while keeping all others out. Stopping imposters without hindering valid users is the goal of every authentication technique.

Various approaches address this vital task. All rely on the incorporation of one or more of the three factors critical to authentication:

- Some knowledge the person has, such as a password. This factor is commonly referred to as "something you know."
- Some physical characteristic, such as a fingerprint. This factor is commonly referred to as "something you are."
- Some item the person possesses, such as a key, a token, or a smart card. This factor is commonly referred to as "something you have."

Each individual approach is uniquely designed to authenticate a user as completely as possible without imposing too much inconvenience. Each also has unique potential weaknesses. Used in combination, the strength of authentication security is magnified, reducing the potential for impostor entry.

Passwords

The password is undoubtedly the most commonly used access control technique. The user simply provides a username and password, submits the information, and is granted or denied access. Within the computer system, this authentication method compares the username and password combination to stored information. An electronic response grants or denies access based on the results of this comparison. Protecting usernames, passwords, and the relationships between them is therefore critical to controlling logical access with passwords.

There are many ways for unauthorized individuals to gain access to passwords. Several of the most common methods follow.

- **Social engineering** is probably the best known of all ways to gain access to a system. For example, unauthorized individuals use flattery or logical reasons to obtain another person's password. This risk is most easily mitigated by educating users on the need for strong and effective security.
- **Password cracking programs** use either brute force or dictionary look-up methods to attempt to decrypt protected passwords.
- **Sniffer programs** monitor packets traveling over a network. If an unencrypted password passes by, the sniffer captures and uses it, compromising the integrity of the system. However, the effectiveness of sniffing tools has decreased with widespread adoption of network switches and routers, greatly reducing the usefulness of sniffing utilities.

- **Personal knowledge** about legitimate users is used to try to guess their passwords.
- **Access to employees' desks.** A person can sit at an employee's desk when nobody is around and look for passwords that have been written down.
- **Look and see.** By far the easiest way to get a password is to watch someone type it!

In order to safeguard password integrity, security policies require users to change passwords regularly to deter access to their accounts through such methods as finding written passwords, watching the person enter information, using keyboard sniffing programs, or guessing. Such password security policies are effective but can become quite complicated. These policies usually direct users not to reuse passwords, forcing them to create new and equally "guess resistant" passwords that they can remember. The protection of stored information is also critical to a strong password security policy.

Passwords can be implemented in a variety of ways. In all cases, implementation of a password security policy is highly recommended. The policy may be as simple as requiring a minimum number of letters and may require the inclusion of upper- or lowercase letters, numbers, and special characters.

Cleartext Passwords

The most elementary approach to passwords is to store cleartext (i.e., unencrypted) passwords and usernames in a flat file stored on a network. Such a file might look like this:

USERNAME	PASSWORD
AliceZ	myDOGsparkY
BobY	Home4holidays
CarolW	getthejobdone

This approach is easy to implement. The challenge is to protect the information from inappropriate access or manipulation while retaining instant accessibility for the logon process. While this approach is appropriate for certain situations, it is extremely vulnerable to attack. Once attackers find out how the logon function works and determine that passwords are maintained in the clear, access is greatly simplified. Once inside the system, the attacker simply reads the file and obtains network privileges and access based on existing user accounts.

Password Conversions

In order to mitigate the vulnerability of storing cleartext passwords, three approaches rely on techniques that convert the password entered by the user from cleartext to some other form of data:

- Hashing
- Message authentication codes
- Cryptography

All three approaches potentially suffer from the same vulnerability: they all rely on the ability of people to choose passwords that are easy to remember (without writing them down) but complicated enough to withstand attack. Converting a password protects the stored form of the password, thereby eliminating the value of gaining access to the password database. However, the password itself is still potentially vulnerable to guessing or sniffed replay (in which an attacker intercepts data containing the password and extracts it from the data).

Hashing. Hashing, sometimes referred to as a message digest, uses a one-way mathematical algorithm that creates a fixed length result from a message of any length. Hashing essentially creates a digital fingerprint of a message and, in this case, is used to protect passwords. Hashing changes a password into binary format and divides it into code blocks of a predetermined size. Each block is then processed through the hash algorithm and combined with the next unprocessed block to be processed again until all blocks have been processed. The result is then reconverted to ASCII text. Hashing is a reliable method for converting passwords because the result of feeding the same password into the same algorithm is always the same. However, virtually no mathematical or logical approach can obtain the original password from the result.

The two most popular hashing algorithms are MD5, which produces a 128-bit hash from any input, and the Secure Hash Algorithm (SHA), designed for use with the Digital Signature Standard by the National Institute of Standards and Technology (NIST) and the National Security Agency (NSA). SHA-1 produces a 160-bit hash.

A SHA-1 hashed password file looks like this:

USERNAME	PASSWORD
AliceZ	c0f1ce0662f4a2f8d86613cf2e7ddc311fbcf3bd
BobY	6dc04707c1204dac18b73e5b388365deac43f70c
CarolW	2a70467b07eb3acfb90944c90e0261a5cb44649d

Message Authentication Codes. Protecting passwords using a message authentication code (MAC) depends on a process that first hashes the password and then adds a symmetric cryptographic key. Security is enhanced by the fact that the hashed password is encrypted. The verifying location compares the password to a stored value.

The password is typically prepared for transport within the computer used to log on. Like hashing, MACs protect passwords only after they are submitted.

Cryptography. Passwords can also be protected using cryptography. A cryptographic algorithm, generally residing on the logon computer, encrypts the password and sends it to the location where the password data resides. The password is then compared to the stored data and the result is sent back to the logon computer.

Symmetric cryptographic algorithms are typically used, since they are fast and robust. Unlike hashing and MACs, the resulting length varies in relation to the length of the password.

A file of encrypted passwords might look like this:

USERNAME	PASSWORD
AliceZ	60135d5b849c2700dc60ffc2606fb947
BobY	0c0dd92d4bd8d8ca864441d23e066d8b
CarolW	7b94228224366ce3b2a049acaa0bd3c2

One-time Passwords

One-time passwords (OTPs) were developed to counter the potential problems of user-determined, static passwords and password security policy management. OTPs use a time-based algorithm with a random number generator that is unique for each individual user.

Each time the user authenticates to the system, a different password is used, after which that password is no longer valid. The password is computed either by software on the logon computer or OTP hardware tokens in the user's possession that are coordinated through a trusted system.

Software-based OTPs. Software-based OTP programs reside completely on the network and the host machine. One of the most common software-based OTPs is S/KEY[®], which is freely available on the Internet and is used as an example in the following discussion.

S/KEY uses a combination of a permanent S/KEY password that is never sent over the network and a one-time key. When the user connects to the remote machine, a dialog box displays a one-time key and prompts for a password. The one-time key and the user's permanent S/KEY password are entered into a local S/KEY client machine, which then generates a password that allows logon. Every time the user connects to the remote machine, the one-time key changes; however, the user's permanent S/KEY password remains the same.

One of the advantages claimed for this approach is that no secrets are stored on the host server. However, the server does need to store the OTP most recently used for authentication. For this reason, software-based OTPs are vulnerable to intruders who obtain root privileges on a server.

OTP Tokens. Hardware-based OTPs are generated by a physical token or other device that users carry with them. Password generation is based on either time-based or challenge-response algorithms.

The most popular time-based algorithm is incorporated in the RSA SecurID[®] product. In this implementation, the user carries a special token that generates and displays a six-digit number that changes every 60 seconds. To log onto a system, the user enters a username and uses the six-digit number as the password. A server hosts software that uses a clock to coordinate with the hardware token and maintains a database with the correct passwords and challenge response. If the number is what the server expects, the password is accepted. In a challenge-response system, a challenge is issued by the host system, which is then used by the user to compute the appropriate response. The response can be computed by the token, an automatic program, or user software.

Alternative OTP techniques are available, including approaches that use a smart card or smart-card-based USB token as the physical OTP device.

Single Sign-on. Single sign-on is an authentication mechanism that requires computer users to sign on to a system (i.e., present a password) once. The single sign-on then provides them with access to all applications

and systems that they are authorized to access. Single sign-on solutions are typically being implemented to reduce human error and user frustration. The acceptance of single sign-on solutions has not been universal, since they often only reduce the number of passwords required or they are too complex to integrate with applications. Since single sign-on solutions rely on passwords, they also suffer from the weaknesses inherent to all password-based authentication unless other authentication factors are also implemented.

Biometric Factors

Approaches that rely on biometric factors comprise a group of proven technologies and computerized methods that identify and verify individuals based on personal characteristics. These approaches match a characteristic in real time against a record of the characteristic that was created at enrollment. The main biometric technologies include fingerprint, face, hand geometry, iris, palm, signature, voice, and skin.

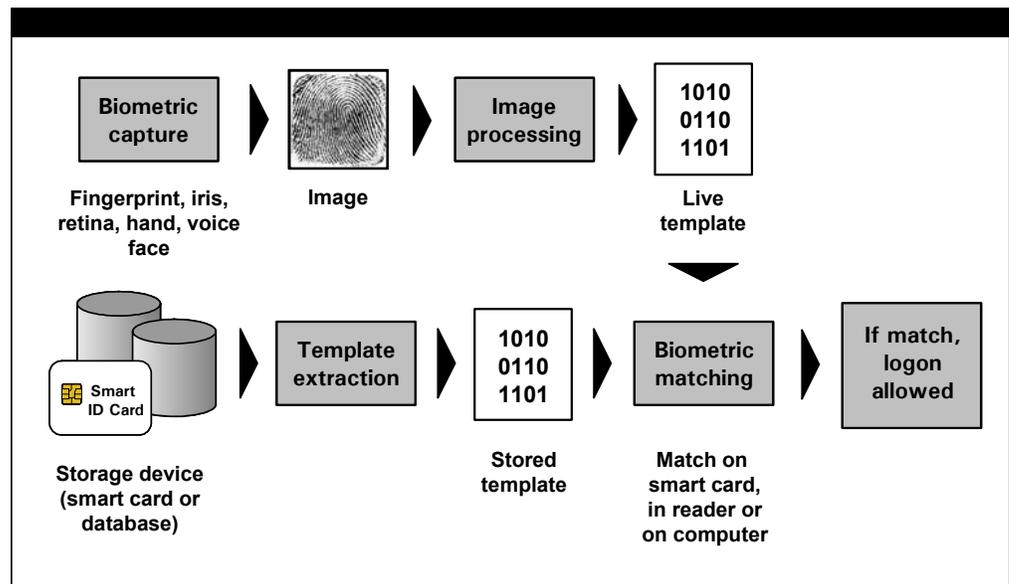
The matching process is carried out in three steps:

1. An image of the biometric data (e.g., a fingerprint) is captured.
2. The image is converted into a unique template.
3. Complex algorithms compare the template with a stored record.

Biometric technologies are being used more often as a primary or secondary control for logical access. In a typical scenario, users enter a username and place a finger on a reader (instead of or in addition to providing a password). A server compares the biometric template created by the reader with a record stored on the server. As an alternative, users may insert a smart card in a card reader and use a fingerprint to authenticate that they are the valid cardholders. The biometric captured by the reader is compared to biometric data on the smart card. If the captured biometric matches the biometric stored on the card, the smart card then releases the secret information required to log the user onto the network. In this case, the biometric comparison may be done in the reader or on the card (called match-on-card).

Figure 1 illustrates the identity verification process using biometrics.

Figure 1: Identity Verification Process with Biometrics



The value of using biometrics for logical access will increase as the technology becomes easier and faster to use. Personal traits are an attractive, convenient, and reliable authentication mechanism. Security concerns, however, center on the biometric data matching process, which typically either requires sending unprotected data over the network or storing the data on the logon computer. Such data is vulnerable to replay (resulting in illegal access) or replacement (resulting in denial of access). This concern can be mitigated by protecting biometric data in transit or by capturing and comparing the biometric data locally (e.g., within a reader or on a smart card).

Public Key Cryptography

Public key cryptography (also known as asymmetric key cryptography) encrypts information using mathematically related pairs of cryptographic keys. One key in the pair is used to encrypt information; the information can then only be decrypted using the other key. Users obtain the key pairs through a trusted authority and use them to exchange data securely and privately.

Each key pair comprises a public key and a private key. The public key is used to encrypt confidential information. The private key authenticates the key holder and decrypts information that has been encrypted using the public key. The private key must be kept secret. The person using the private key can therefore be certain that information the key is able to decrypt was intended for them, and the person sending the information can be certain that only the holder of the private key can decrypt it.

Information describing the public key is recorded in a certificate that is signed digitally by a certificate authority. A user can provide the public key to a sender, or the key can be retrieved from a directory in which it is published.

The use of asymmetric keys is supported by PKI. PKI is a combination of standards, protocols, and software composed of at least the following components:

- A certificate authority (CA), which issues and verifies digital certificates
- A registration authority (RA), which verifies the identity of the requestor before a digital certificate is generated and issued
- One or more directories where certificates (with their public keys) and the certificate revocation list (CRL) are stored

Public key cryptography offers an additional level of security, since there are no shared secrets. Generally, the PKI certificate is stored on a logon computer or hardware token (for example, a smart card) and is used to encrypt the password before it is sent to be authenticated.

Soft Tokens⁴

Soft tokens (also known as virtual cards) are software files that contain cryptographic keys used for authentication. Users authenticate themselves to a network by proving possession and control of this cryptographic key (typically stored on disk or some other media). The media used to store cryptographic keys is itself password-encrypted, with the password known only to the user. Each instance of an activation requires the entry of the

⁴ *Electronic Authentication Guideline*, NIST Special Publication 800-63, Version 1.0, June 2004

password to decrypt the contents of the soft token. The unencrypted copy of the authentication key is erased after every authentication.

Soft tokens are generally seen as inexpensive, easily managed, and disposable. However, this authentication method is not typically portable; users must be at a client machine to authenticate themselves. Some soft-token offerings support user mobility, either by allowing keys to be stored on servers and downloaded to the user's system as needed, or by employing key components generated from passwords combined with key components stored on servers.

Soft tokens rely on a trusted client and a trusted server. In addition, the user must have another key to access the soft token; otherwise, anyone with access to the client machine can be authenticated.

Smart Card Technology

When used for logical access, smart card technology typically comes in two form factors: a credit-card-sized plastic card or a USB device, each with an embedded computer chip. By far the most popular form factor is the plastic card, due to its ability to include a picture and visible corporate information and to host other security mechanisms such as a magnetic stripe or bar code.

Regardless of form factor, smart cards can be used to implement any of the authentication techniques described above. Smart cards have the ability to:

- Securely store password files
- Generate asymmetric key pairs and securely store PKI certificates
- Securely store symmetric keys
- Securely store OTP token seed files
- Securely store biometric image templates

Using a smart card to store password files is the simplest use of smart cards for logical access. The benefits of this type of system are:

- Users do not have to remember their passwords.
- Stored passwords can be very large and almost unbreakable using a dictionary attack.
- The card can be activated by a personal identification number (PIN) or biometric if required, adding an authentication factor.
- This implementation is usually the lowest entry-cost system.

Smart cards can also be used to support stronger authentication schemes. For example, in a system that uses symmetric keys, the card can securely store a shared secret injected at the point of manufacture. This key can then be used during the authentication process with a secure server as part of an algorithmic challenge and response session. Smart cards are also widely acknowledged as the ideal carrier of PKI credentials; smart cards can store public key certificates securely, support on-card key generation, and protect the user's private key.

The use of a smart card with one or more of these approaches can provide a more secure means of logical access, even if the combination does not necessarily meet the criteria of two- or three-factor authentication. For example, a smart card alone cannot authenticate a user to a network, but a smart card can store information that provides a logon mechanism. A smart card that stores a user's PKI logon certificate can authenticate that user to the network but only satisfies the requirement for something you have.

However, combining a smart card with a PIN or biometric protection achieves two-factor authentication. A smart card used with both a PIN and biometric data provides three-factor authentication.

Table 1 summarizes the use of smart cards with authentication factors.

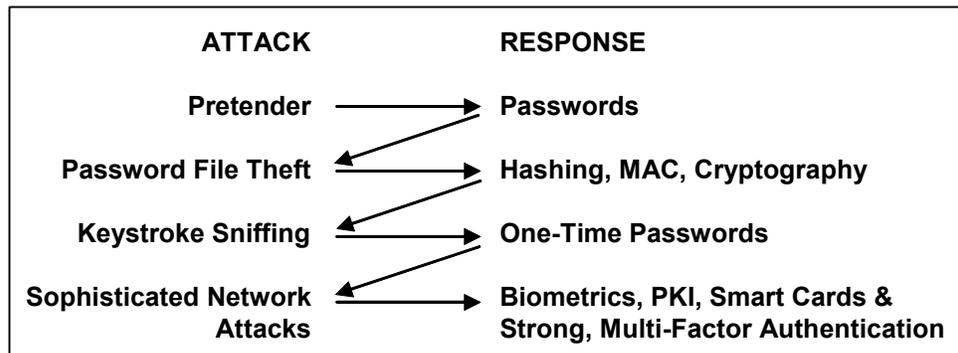
Table 1: Single and Multiple Factor Authentication Approaches

Approach to Authentication	Factor		
	Something You Have	Something You Know	Something You Are
Passwords		✓	
OTP token seed file	✓		
Biometric image template in database			✓
Smart card	✓		
Smart card with PIN	✓	✓	
Smart card with PKI smart card logon certificate	✓		
Biometric image template stored on smart card	✓		✓
Smart card with PIN and password (or certificate) stored on card	✓	✓	
Smart card with PIN, password (or certificate) and biometric on card	✓	✓	✓

Summary

As shown in Figure 2, authentication technologies have evolved in complexity in response to new attacks on systems and networks. The purpose of an authentication technology is simply to stop individuals from gaining unauthorized access to information and applications, regardless of their purpose. As information becomes increasingly vital, it is critical that authorized individuals have the privileges that allow them to access information and applications that are appropriate and essential to their roles and tasks. Attacks on systems have created the need for technological responses that can be used to thwart intrusions.

Figure 2: Attacks and Authentication Technology Responses



Key Considerations for Implementing Stronger Logical Access Authentication

Businesses and organizations are discovering that the current approach to logical access authentication is obsolete and inadequate. A number of important factors are leading companies and government agencies to reevaluate their logical access strategies and plans, resulting in a move towards the use of stronger authentication for logical access. This section reviews some of the key considerations and business requirements driving this trend and discusses how stronger authentication methods can help address these important requirements.

Business Environment

Changes in the business environment can be strong drivers for re-engineering IT processes and implementing stronger authentication for logical and physical access.

- **Is your business trying to comply with new or changing regulatory mandates, such as HIPAA, Sarbanes-Oxley, Gramm-Leach-Bliley, Visa Waiver Program, or International Civil Aviation Organization (ICAO) Machine-Readable Travel Documents (MRTD)?** Many of these mandates affect policymakers as well as the IT department. Stronger authentication methods can help address the access and audit-trail requirements that are integral to many of these mandates. For example, enforcing strong authentication by using smart cards and fingerprint biometrics can help address some of the privacy requirements for HIPAA compliance.
- **Has your organization or a business partner recently suffered a security breach, or has an audit uncovered vulnerabilities?** While such events can be unpleasant to deal with, they can also provide extra motivation (and funding) to justify implementing stronger security measures. Analyze these events for weaknesses in current authentication procedures and apply stronger authentication methods to current logical access systems where appropriate.
- **Is your organization currently contemplating, planning, or implementing a new or enhanced physical access system? Are you considering integrating your physical and logical access systems?** Consider upgrading your logical access procedures at the same time. Taking a holistic view of access requirements can offer a stronger, more integrated and user-friendly security system. Integrating physical and logical access approaches can also provide significant cost savings by eliminating or reducing the number of required badges or ID cards, averting reader replacement or upgrade costs, and streamlining identity provisioning procedures.
- **Was your organization recently involved in an acquisition or merger? Are you integrating or migrating multiple IT systems?** Many companies face the challenge of dealing with disparate logical access systems as they integrate different IT environments. Many groups freeze new initiatives until these different IT systems have been integrated. But this approach can be risky and costly when it comes to logical access. Instead, consider using strong authentication as a migration aid through the integration process. For example, strong authentication implemented with a single smart card credential could

replace multiple user IDs and passwords while adding security to IT systems.

Business Transformation and Process Re-engineering

Many organizations consider stronger authentication as a key component of projects to reengineer company-wide IT processes.

- **Does your organization have or is it considering integrated identity management? Are you thinking about sharing identity credentials with business partners, suppliers, or government agencies?** If so, such plans can help you determine what types of authentication practices to implement and convey to stakeholders how these practices will strengthen identity management overall. Strong authentication will also be an integral component of any federated identity management systems in which you decide to participate. Requiring the proper use of strong authentication in a federated identity management system protects you not only from potential weaknesses within your own organization but also from potential weaknesses in other parts of the federation.
- **Is a portal or Web services strategy or deployment underway? Is it employee-facing, customer-facing, or both?** Migration to a Web-centric infrastructure for both internal- and external-facing applications represents an excellent opportunity to centralize, integrate, and strengthen logical access policies and practices.
- **Is your organization hoping to replace multiple user IDs and passwords with a single credential?** Usability issues, password management costs, and security concerns (with reused or easy-to-remember passwords) have spurred single (or reduced) sign-on initiatives in many organizations. A single sign-on credential dictates the use of stronger authentication methods when this "super" credential is used.

Cost Reduction and Return on Investment

The implementation of strong authentication can help to reduce overall IT costs and deliver a compelling return on investment. Key questions to consider include the following.

- **What is the total cost of managing user IDs and passwords across your organization, including intangible costs such as customer satisfaction and employee productivity?** In addition to the security risks inherent in user IDs and passwords, other costs include system administration, help desk support, and lost productivity. Strong authentication methods can save money while enhancing security. Understanding the total cost of current logical access procedures can help quantify the benefits of moving to stronger authentication methods.
- **How many applications, systems, and networks does your organization operate, manage, or own? How many users access these applications, systems, and networks?** The more systems you have and the larger the user population, the more savings can be achieved by moving to strong authentication methods. While the biggest cost savings come from enhanced security, administrative cost savings and productivity improvements can also be significant contributors to the business case.

-
- **What is the makeup of your user population? Can business partners access your systems? Do users access your systems from external networks?** The more varied the user population, the greater is the return on investment from moving to strong authentication methods. Such a move offers the flexibility to choose and enforce the most effective authentication procedures for each different user population. For example, two-factor authentication (such as a smart card and a biometric) can be required for remote access to an intranet, while only a single factor (such as a smart card or a biometric) can be required for on-campus network access.

Security and Privacy

Improving the security of IT system access and protecting the privacy of individuals are primary drivers for most organizations implementing new logical access systems that use stronger authentication techniques. Key considerations include the following questions.

- **Does your organization have a privacy policy that protects user information from unauthorized access?** For example, system administrators should not be able to browse users' personal information at will. Strong authentication procedures can allow administrators to fulfill their jobs while preventing them from accessing private user information.
- **Do your existing authentication methods provide enough security and privacy? Is your logical access security dependent on passwords only?** Access control can be strengthened by using multiple factors of authentication (something you have, something you know, and something you are). The highest levels of security and privacy are achieved when authentication methods use factors from several categories in combination or multiple factors from one or more categories (for example, multiple biometrics). A properly implemented strong authentication system can enforce a variety of authentication policies and procedures, based on the needs of particular applications and user populations.
- **Does your organization use ID badges or cards? How are these cards produced and distributed?** Strong authentication procedures can leverage and enhance an existing ID card issuance infrastructure and may be implemented using central or distributed card production. Central production and distribution provide added security and reduce costs for equipment and maintenance. Distributed, point-of-enrollment production provides faster turnaround, increases customer satisfaction, and represents an additional opportunity to train users.
- **Is biometric technology ready to use? What biometric is right for your application or system?** Biometric technology providers continue to make advances in accuracy, performance, and cost. Today's biometric systems offer usable and acceptable matching capabilities, while providing predictable and reliable performance for system users. It is important to select the biometric technology that is appropriate for an application and authentication requirement. Whether fingerprint, iris, voice, face, some other biometric factor, or multiple biometrics are used, biometric technology can help enforce higher levels of security and privacy in a logical access system, while also providing usability benefits.

Management, Usability and Training

Strong authentication solutions can simplify management and improve the usability of authentication processes. Consider the following questions when implementing new access control solutions.

- **How does your organization detect and deactivate lost or stolen credentials? How do you know when a password has been compromised?** These are serious problems for logical access applications, especially if the applications are protected only by static passwords. Strong authentication minimizes these risks. For example, requiring the use of a smart card and a password minimizes the risk that a password will be shared or compromised. Using biometric data with a smart card effectively renders the card useless if it is lost or stolen.
- **How does your organization train users on security?** Security training is a key element to any organization's overall security plan. Strong authentication provides a constant reminder to users that security is important. It also offers an additional opportunity to train users on security. For example, during ID card issuance, users can be instructed in the proper use of their strong authentication credentials. This instruction can include a demonstration of how to present a high quality fingerprint and describe how biometric data is protected and stored and who has access to it. Strong authentication credentials are also a reminder to employees that network activities are monitored and that network and computer security are extremely important.
- **Does your organization have common work areas or multi-shift operations that require workstations to be used by multiple users?** A common security problem in these types of environments is the lack of user access controls or sharing of user credentials. Users typically find ways to circumvent cumbersome access controls that slow down the workflow. Strong authentication can help provide better security for IT administrators and enhanced usability for users, addressing the needs of both groups. For example, using a fingerprint to sign a transaction provides administrators with accountability and an audit trail to an individual user, while also being faster and easier for the user than logging on and off with a username and password.
- **How many identities do users need to manage today? How many user IDs and passwords must they remember?** In just about every job and every industry, users must interact with a number of applications. This is often compounded by the trend to electronic delivery of employee benefits, communications, and training. So not only do users need to manage identities for workflow and process applications, but they often must also remember user IDs and passwords for human resources, health care, and financial applications as well. Strong authentication can help simplify identity management for both users and administrators while providing higher levels of security.

Benefits of Smart Card Technology for Logical Access

For most organizations today, computer and network resources are accessed by using a user ID and password. Each system or application typically assigns a user ID and password to each user and then determines access controls for that user based on the unique ID. User identities are managed on a per-application basis. However, as the number of systems and applications in an organization grows, administering and using those identities create significant operational inefficiencies. Increasing numbers of applications also introduce security vulnerabilities, as it becomes more difficult to control policies around the use of those identities.

Strong Authentication

More and more organizations today are looking for stronger authentication solutions – beyond usernames and passwords – to validate that the users accessing systems are who they say they are. Organizations that have deployed strong authentication (typically in the form of dynamic password tokens) traditionally provide such solutions to remote employees only. This practice is based on the assumption that individuals physically located within a building can be trusted. However, the 2004 E-Crime Watch Survey (conducted by CSO Magazine in cooperation with the U.S. Secret Service and CERT Coordination Center) revealed that 36% of the 350 respondents experienced “unauthorized access by an insider” as one of the electronic crimes committed against their organizations in 2003.⁵ This type of crime was the fourth most common attack, behind viruses, denial of service, and spam. IDC estimates that more than 60% of all serious threats are internal, coming from employees, contractors, consultants, systems integrators, partners, distributors, and others with privileged access.⁶

The boundaries of information systems and data continue to expand. The Internet and wireless technologies provide increasing numbers of convenient access points for employees but create a nightmare for IT. To shore up security throughout an organization, a method is needed to provide strong, consistent authentication for access to all networked resources. Smart card technology is the best platform for securing all access points in an organization.

Smart cards significantly increase the security of a user’s digital credentials, regardless of the nature of the credentials. The credentials are permanently stored on the card, which is in the possession of the end user, and never available in software or on the network for an unauthorized user to steal. Smart cards are typically used to enable two-factor authentication, incorporating something that you have (the smart card) and something that you know (typically a PIN that activates the card’s cryptographic functions). Taking control of a user’s digital identity requires stealing the smart card and guessing the PIN. Users know very quickly when a card is stolen and can

⁵ “2004 E-Crime Watch™ Survey Shows Significant Increase in Electronic Crimes,” CSO Magazine survey conducted in cooperation with the United States Secret Service and Carnegie Mellon University Software Engineering Institute’s CERT® Coordination Center, May 25, 2004 (www.csoonline.com/releases/052004129_release.html)

⁶ “Endpoint Security Management: Maximizing Best of Breed,” IDC report, March 4, 2004

contact the network administrator to revoke the stolen credentials. In addition, too many incorrect password guesses can lock the card.

Smart card technology also supports the addition of biometric technologies (something you are) to enable three-factor authentication. As an alternative, the biometric can simply replace the PIN, which strengthens security while increasing user convenience. Adding biometric authentication to the access control solution is easy, because the smart card can store the user's biometric data and perform the processing required to determine a match. No back-end database of biometric data is required. Having the credentials for accessing an application securely stored on the smart card and protected by the user's biometric data provides an organization with biometric security without having to touch back-end applications.

Built-In Security

A smart card is typically a plastic credit-card-sized device with an embedded computer chip. The chip can contain both a microcontroller and internal memory or memory alone. Smart chips can also be embedded in other devices, including tokens that plug directly into a computer's USB port and SIM chips that plug into GSM mobile phones.

Microcontroller-based chips are the most practical choice for secure logical access applications, because such chips can store large amounts of data and have the ability to process data and perform a variety of functions. This unique ability supports the addition of active security methods to the smart card, depending on an application's requirements. Most of the smart card solutions currently available for logical access are already loaded with the most widely used encryption algorithms, such as DES, 3DES, and RSA⁷.

In addition, most microcontroller-based smart chips are designed to resist attack. Smart chip manufacturers build in a variety of countermeasures that detect and react to a number of possible attacks, including voltage, frequency, light or temperature manipulation, and differential or statistical power attacks. The typical reaction to most attacks is to lock the chip down, making it inoperable.

Sophisticated attacks on smart cards are time-consuming and expensive, and the attacker must have physical possession of the card. If a user's smart card is missing, it is likely that the user will report it, and the card can be disabled before any attack can succeed. When credentials are stored in software on a user's computer, however, the user may never know that they have been stolen.

Enhanced Security and Convenience for Users

Users in most organizations face the challenge of managing multiple passwords for multiple systems and applications. This requirement has implications for security and user productivity. Some IT departments choose the path of least resistance, allowing users to use the same password for every application. This practice represents the greatest security risk, since all applications are compromised if a single password is guessed or stolen. Other IT departments may establish a stronger policy, requiring a different password for each application and a more complex password, containing a mix of character types (alphanumeric, uppercase, lowercase, symbols). In

⁷ The RSA encryption algorithm has become the international standard for secure transmissions.

addition, a secure password policy may require that passwords be changed on a regular basis. Establishing stronger password policies is an important step when access relies on a static password alone, but enforcing these policies can be challenging. Most users have difficulty remembering multiple complex passwords, so they write them down or store them in plain text on their computers, where they can easily be stolen.

IT departments also face the challenge of administering passwords for multiple users and multiple applications without sacrificing productivity and without creating unhappy users. Industry statistics show that 30% to 50% of IT help desk resources are consumed by managing and resetting passwords. End-user productivity is also affected, since users cannot access applications until a new password is assigned.

Various “identity management” solutions are currently available that address these productivity issues. Consolidating users’ identities in central directories and implementing provisioning tools to manage those identities minimize the productivity losses attributable to managing different identities for different accounts. Such solutions also address the security vulnerabilities posed by accounts that remain on a system long after the owner’s access is no longer valid. Similar solutions are available for Web-based content and applications. However, such solutions cannot be implemented overnight. In addition, they require a gradual change in an organization’s back-end infrastructure. And users still need to juggle multiple passwords for their applications. Other identity management solutions simplify the end-user experience by using password synchronization, self-service password management, or single sign-on, but these also typically require modifications to the IT infrastructure and do not address the security concerns raised by using passwords.

Organizations that use smart card technology for logical access do not have to wait for back-end identity management system implementation to realize operational efficiencies and return on investment. User identities and credentials can be consolidated onto a smart card immediately, providing users with a single, consistent approach to logical access, regardless of whether the user is logging onto a workstation or a network or accessing the network remotely using a VPN. The user experience remains consistent when the organization updates its identity management infrastructure: insert a smart card and enter a PIN.

A smart card is a user’s personal key to all of the user’s data and applications. In addition, because the key is portable, users are not tied to a single workstation on which their credentials are located. They can travel from machine to machine, a critical advantage for users who work at multiple locations.

Enhanced Protection against Identity Fraud

Smart cards can help defend against ever-more-cunning attempts at phishing. Phishing uses e-mail messages or the Internet to attempt to fool individuals into divulging information about their accounts. For example, a phishing attempt might use e-mail to send a potential victim what appears to be a genuine request from a trusted party (e.g., a bank or an Internet service provider). The individual would then respond to the request by providing account numbers, PINs or passwords to a rogue Web site posing as the legitimate entity. Phishing attacks exploit the lack of authentication between the e-mail sender and recipient and between the rogue Web site and the individual.

Smart cards can be used to combat phishing attacks by applying two-way mutual authentication for secure access to Web site services. When account issuers offer a Web service (e.g., for account management), they can issue smart cards to account holders that allow access to the legitimate Web site. The smart card credential can both authenticate the user to the Web site and authenticate the Web site as legitimate.

By providing strong, multi-factor authentication and by enabling mutual authentication, smart cards can help defeat phishing attacks. Individuals can be assured that they are communicating with a legitimate site and that their identity credentials are protected from unauthorized access.

Standards-Based Application Coverage

Smart card technology is becoming a preferred approach for logical access, not only for the smart card's increased security, but also for its ease of use, broad application coverage, ease of integration, and multi-purpose functionality. Smart cards provide organizations with a cost-effective solution that can be deployed easily and is widely accepted by the end user.

Different applications impose different requirements on users before granting access. Some applications support only one method of granting access; others support multiple methods. Few applications allow credentials to be shared.

Some of the most common application access methods are the username and password combination, password only, shared secret, OTP, biometrics, and PKI or digital certificate. The username and password combination, while the least secure approach, is currently the primary method used for access control. More secure methods, such as OTPs or PKI certificates, can increase security only for applications that support these methods and require additional infrastructure to manage. As the methods required to access different applications multiply, user acceptance decreases, often leading to decreased security.

Smart cards, unlike other solutions, can provide the user with all of these access methods built into a single card, while requiring only the entry of the user's PIN. Additional functionality enables smart cards to generate OTPs that replace single-use tokens and use biometrics to replace the PIN. Commercial products are available that leverage the security and portability of smart cards to store usernames and passwords for all applications. In addition, smart cards are more flexible than traditional token technology, because they are cryptographic devices that can support a wide range of functionality. They are not dependant on the presence of a server, and they can be erased and reprogrammed for continued use within an organization.

Smart cards can now provide a user with a single interface for access to all applications, regardless of the credential required by the application. This capability increases user acceptance and convenience, while implementing and enforcing the organization's security policies.

Over the last several years, standards have evolved that provide the interoperability needed to allow a smart card to access multiple organization resources. For example, cryptographic standards such as PKCS #11 and Microsoft Crypto API (CAPI) allow applications to use a digital certificate stored on a smart card to authorize end-user access. The private key is stored on the smart card chip and can only be accessed by a user who provides the correct PIN when the application opens.

The adoption of the Personal Computer/Smart Card (PC/SC) standard and the proliferation of readers and reader drivers have also contributed to a wider acceptance of smart cards for logical access. The price of readers has decreased, and their quality and availability has increased to the point that many of the major computer manufacturers now build a reader into a computer keyboard or laptop for little additional charge.

Ease of Integration

Smart cards include built-in functionality that simplifies their integration into an organization's IT infrastructure. Most applications requiring credentials other than a username adhere to one of the standards listed above. For this reason, enabling smart card access is typically simple, requiring installation of a small middleware application on the computer. Smart cards can then be used for logon, VPN access, signing and encrypting e-mail, SSL-based Web access, and biometric-based logon.

Most of the leading CAs have adopted smart cards as the preferred platform for storing and using digital certificates. A CA can use either the PKCS #11 or Microsoft CAPI interface to generate keys, load certificates, and perform required cryptographic functions. Configuring a CA to use a smart card is straightforward and typically consists only of selecting the correct interface.

Smart card readers are now easily integrated with applications and desktop operating systems through two standards: the PC/SC standard and the CCID, or Chip Card Interface Device, specification.

The PC/SC standard allows smart card readers to be integrated easily with middleware or other applications, regardless of manufacturer or command set. Although this standard was developed for use in a Microsoft environment, it is now considered the de facto standard for many other platforms as well.

The CCID specification was developed for USB smart card readers. It was designed to support easy integration of smart card readers with desktop operating systems, thereby removing the need to install additional reader driver software onto the user's desktop. The specification was defined by the USB Implementer's Forum (USB-IF)⁸ in conjunction with the smart card industry. CCID defines a command set and transport protocol over the USB so that a host system can communicate with a smart card reader. A specific USB class is now defined for smart card readers.

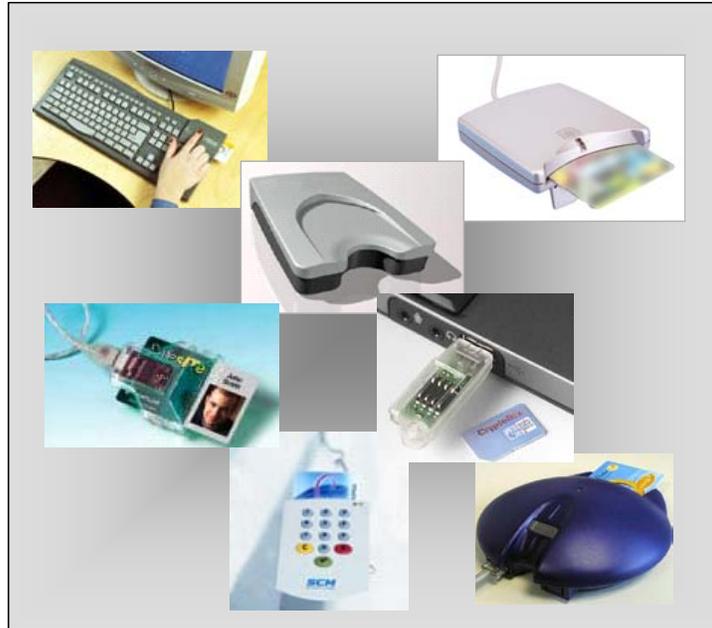
The adoption of the CCID specification enables smart card reader manufacturers to build devices that are compliant with this specification. Operating system vendors can write one driver that adheres to this specification and supports all CCID-compliant readers. Microsoft has released a CCID-compliant driver on Windows Update for Windows 2000 and Windows XP. The driver will be included in service packs and all future operating system releases. Porting to Windows CE is also being considered. Other major operating system vendors (e.g., Apple and Sun) are also including native CCID drivers in their operating systems.

Use of a CCID-compliant smart card reader provides true plug-and-play support, removing any need for additional software to be installed. This greatly enhances the user experience.

⁸ Additional information about CCID can be found at the USB Implementer's Forum web site, <http://www.usb.org>.

Figure 3 shows a variety of solutions for connecting a smart card to a computer, including contact and contactless smart card readers, USB smart card devices and a smart card reader with integrated biometric reader.

Figure 3: Examples of Smart Card Readers⁹



Ease of Deployment

Management tools and deployment methods are available that facilitate large deployments of smart cards. Card management systems integrated into an organization's directory or procurement system provide the functionality needed to deploy and manage smart cards and their credentials. Reader drivers and smart card middleware are mature and easily deployed throughout an organization as well.

Both top management and dedicated project management support are still critical to successful implementation. Deploying a new, organization-wide identity management system that includes smart cards can be a complex project that extends across multiple organizations and affects core business processes.

Multi-Purpose Functionality

Plastic cards are a common fixture within many organizations and have many uses, such as identification, physical access, and time and attendance. Smart cards allow organizations to realize the benefits of combining all such applications on one card. The user can then carry a single card for physical access, logical access, identification, and other business functions. Other technologies often associated with a plastic card, such as magnetic stripes, bar codes, radio frequency (RF) technology, and security laminates can be used in conjunction with the smart card. In addition, as smart chip

⁹ Photos provided by Atmel, Axalto, Datakey, Gemplus, Honeywell, and SCM Microsystems. Additional information about smart card readers can be found in the Smart Card Alliance smart card reader catalog at www.smartcardalliance.org.

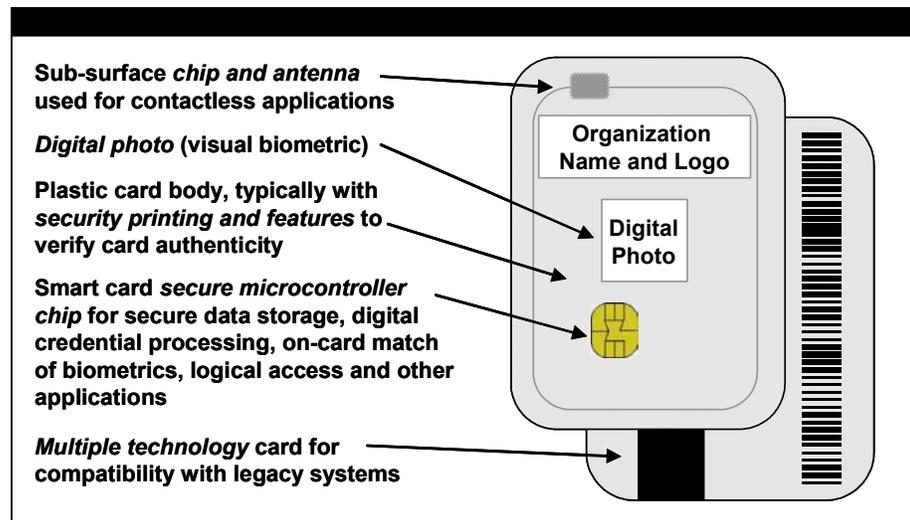
technology continues to make advances in contactless capability¹⁰, smart cards can host applications that require contactless identification, such as physical access to buildings and transportation services.

Smart cards supporting contactless identification are often described as either hybrid or dual-interface chip smart cards. A hybrid card contains two chips, one supporting a contact interface and one supporting a contactless interface. The chips are generally not connected. A dual-interface chip card contains a single chip that supports both contact and contactless interfaces. Dual-interface cards provide both contact and contactless functionality with a single chip in a single card, with current designs allowing the same information to be accessed using either contact or contactless readers.

Most organizations that currently use smart cards for both physical and logical access have deployed hybrid smart cards, using the contactless interface for physical access and the contact interface to a standard PC/SC smart card reader at the user's computer for logical access. This is because, until recently, contactless smart card technology could not support highly secure, encryption-based applications, and the infrastructure required to support contactless implementations for logical access (applications and readers) was not available. Today, smart chip manufacturers are beginning to deliver dual-interface chips with the performance and processing capabilities required to support more sophisticated logical access applications. Dual-interface cards are now available that have achieved FIPS140-2, Level 3 certification (as a finished card) or cc. EAL 5+ (as an integrated circuit). These security levels are as high as are available from contact-only smart cards. Application vendors are also developing logical access applications that use these chips in either contact or contactless mode. In addition, major smart card reader vendors are beginning to deliver standards-based PC readers that communicate in either mode.

Figure 4 illustrates components on a typical smart ID card.

Figure 4: Smart ID Card Example



¹⁰ A contactless smart chip communicates with the reader using RF and does not require physical contact with the reader.

Smart Cards as Smart ID Badges: An Example Scenario

To illustrate what happens when organizations provide employees with a smart ID badge that is used for both logical and physical access, consider a typical day in the life of Kay Smith, the fictitious customer service manager for a fictitious company, Enterprise Systems. Enterprise Systems implemented a smart ID badge system for its employees 2 years ago to integrate security across the organization and comply with corporate-wide security policies.

Before Enterprise Systems adopted the single smart ID card/badge solution, the company parking lot was accessed by using a magnetic stripe card. The new smart IDs include magnetic stripes so that Enterprise Systems can continue to use their existing parking access application. At the start of her day, Kay Smith accesses the parking lot in the same way she always has, by swiping her badge through a reader.

Once inside the building, Kay must present her smart ID badge to the guard to verify that the badge is indeed her badge. The guard checks the photo on the badge and waves her through. Next, Kay waves her badge close to the RF-based door reader so she can leave the lobby and enter the main office area. Enterprise Systems was able to maintain its existing RF access readers and incorporate the physical access capability into the smart ID badge. The new smart ID cards were delivered with integrated RF antennae that are interoperable with the readers. The only change for employees is that they now use the same card to get into both the company parking lot and the main office area.

Now that Kay is at her desk, she turns on her computer and inserts her badge in the attached smart card reader. The standard Windows logon process recognizes the smart card reader, and Kay is prompted to enter the PIN for her badge, which only Kay knows. Kay is now logged onto her computer and can get to work. As she accesses her various applications (e.g., e-mail, customer database, support database) she is prompted for a password or other credential. The smart ID card automatically provides the required information to access those applications, providing Kay with single sign-on (using the PIN in the initial authentication to the card). Before Kay was given her new badge, she had to remember 12 different passwords for different corporate applications, which frustrated her. She often wrote her passwords down on notepads next to her computer. Kay loves her new badge, because the process is now the same for her no matter what application she accesses. The smart ID card is also configurable so that Enterprise Systems can require different authentication processes or credentials for each application if needed (for example, requiring smart card PIN entry for each application).

Kay is required to adhere to certain company e-mail policies. Sensitive e-mail messages regarding new product information or human resource issues must be signed and encrypted. Enterprise Systems uses digital certificates for e-mail. To secure an e-mail message, Kay accesses the security options for the message and clicks on "sign and encrypt." The system automatically accesses the digital signature information on Kay's smart ID badge. Only the valid recipient can now open and read Kay's message.

It is also a policy at Enterprise Systems that employees must carry their smart ID badges with them at all times. Kay heads for a meeting, grabbing her badge as she goes. As soon as the card is removed from the desktop reader, the Windows desktop is inaccessible until Kay returns, reinserts her badge, and reenters her PIN.

Home at the end of day, Kay decides to access her e-mail and also confirm a customer order. Enterprise Systems uses digital certificates for VPN access. Kay uses her smart card in conjunction with a VPN client on her home computer to connect to the Enterprise Systems intranet. The only information she needs to provide is her smart card PIN, and she's connected.

During the course of her working day, Kay has used a single smart-card-based ID badge to replace multiple cards granting physical access to her employer's facilities. The same badge has facilitated and secured access to her employer's information resources, both on site and remotely, and allowed her to use these resources more efficiently. As this scenario illustrates, smart cards are an effective approach to combining robust security with ease of use.

Advantages Over Other Logical Access Alternatives

Table 2 summarizes the advantages that smart cards can provide for logical access when used with different authentication mechanisms.

Smart card technology represents a flexible and cost-effective means of implementing any authentication technique. The technology offers advantages to both the card issuer and the cardholder, improving the experience of both while strengthening authentication and security for logical access.

Table 2: Enhancing Authentication with Smart Cards

Authentication Mechanism	Issue	Value Added by Smart Cards
Single-Factor Authentication		
Static passwords	<ul style="list-style-type: none"> • Easy to guess, sniff, or steal • Difficult to enforce strong password policies • User frustration and resistance to changing and memorizing passwords • Cost to manage 	A smart card system provides a secure container for passwords and automates the user's logon, relieving the user of the requirement to manage passwords. Strong password policies are easy to enforce.
Passive or active token without a PIN	<ul style="list-style-type: none"> • Token loss or theft 	A smart card system provides security for the token seed and also adds PIN-based access to the card, implementing two-factor strong authentication.
Biometric reader	<ul style="list-style-type: none"> • Replay attack • Masquerade attack • Biometric credential and matching security 	A smart card system provides secure storage for the biometric template, performs the biometric match on the card, and adds PIN-based access to the card, implementing three-factor authentication.
Two-Factor Authentication		
One-time password token with PIN	<ul style="list-style-type: none"> • Complex infrastructure • Man-in-the-middle attack • Single function product • OTP seed protection • Token life-cycle cost 	<p>A smart card system replaces a single-function token with multi-function capability (securing application and network access) and reduces overall complexity and life-cycle cost.</p> <p>Smart card investment can be leveraged by using the card as a smart ID badge for secure access to buildings.</p> <p>Smart cards are programmable. Cards can be reused easily, supporting a more cost-effective approach to issuing temporary access cards. New smart card functions can be added after issuance, supporting upgrades to systems or new applications</p>
Biometric reader and password	<ul style="list-style-type: none"> • Complex back-end infrastructure • Credential security 	A smart card system provides secure storage for the biometric template and performs the biometric match on the card.
Three-Factor Authentication		
Token, biometric, PIN	<ul style="list-style-type: none"> • Credential security, whether on the server or workstation • Complex infrastructure 	A smart card system provides the least complex mechanism for three-factor authentication when integrated with biometric match-on-card capability

Smart Cards and the IT Infrastructure

Modern desktop operating systems offer a significant level of smart-card-related functionality, through either built-in (out-of-the-box) support or commercial add-on software packages. This section describes the capabilities built into the Microsoft® Windows® operating systems and the freely available Linux operating systems. More sophisticated capabilities are also available from third-party vendors.

Microsoft Windows

The Microsoft Windows family of operating systems has included smart card functionality since the release of Windows 98 and Windows NT® 4.0. This functionality supports three types of operations:

- Smart card and reader communications
- Access control
- Web and e-mail services

Smart Card and Reader Communications

PC/SC

The basic technology for communication between personal computers and smart cards is PC/SC, defined by the PC/SC Workgroup¹¹. PC/SC defines an application program interface (API) that provides software developers with a standard set of tools for managing smart card readers and communicating with readers and cards. The PC/SC interface defines standard interfaces for a variety of smart card related-operations. The most common are:

- Enumerating and describing attached smart card readers
- Requesting information about card and reader states
- Exchanging commands with cards

Microsoft has implemented the PC/SC API as part of the Win32® API, which is the fundamental toolset for building Windows applications. Microsoft is also a member of the PC/SC Workgroup.

Support for Microsoft's PC/SC implementation is handled as part of Windows operating system support as a whole. Microsoft support contracts are available, as is fee-per-incident support.

Installation of Reader Drivers

Microsoft takes the same approach to installing smart card reader drivers as it does to installing other hardware drivers in the Windows operating system. Reader manufacturers provide device drivers that are installed by the user. After the driver is installed, the reader is visible through the PC/SC API. In addition, a handful of recommended readers are pre-installed with Windows 2000, Windows XP, and Windows 2003.

The complexity of the installation process depends on the hardware connection. Installing and configuring a smart card reader attached to the USB port is straightforward. The user connects the reader to the port, inserts a driver disk (if necessary), and follows the prompts. Readers that connect to the serial port are somewhat more difficult to install, since the operating system cannot automatically recognize the type of attached device.

¹¹ See www.pcscworkgroup.com for additional information on the PC/SC specification.

However, the basic process is the same: attach the reader and install the driver.

Microsoft has a Windows logo program for smart card readers, which certifies that the readers have been tested by Microsoft to verify their compliance with Microsoft's implementation of the PC/SC standards. Microsoft recommends that only tested and approved smart card readers be used with Microsoft operating systems. However, most of the manufacturers of non-approved card readers have put considerable effort into ensuring that their hardware is compatible with Microsoft's operating systems, and compatibility problems are rare.

CCID

The Chip Card Interface Device (CCID) specification is an approach to smart card reader communication that is gaining in popularity. The specification defines a standard communication protocol for smart card readers that connect to a computer via USB, allowing the same host-side driver to communicate with any CCID-compliant smart card reader. Microsoft provides a CCID driver through the Windows Update system. All new smart card reader deployments should seriously consider using CCID-compliant readers, both to reduce driver installation issues and to ensure that, in the future, the installed smart card readers can be easily and transparently replaced with any other CCID-compliant reader.

Contactless Smart Card Readers

Through PC/SC and now CCID specifications, contact readers have become very well-standardized and easy to integrate. With the finalization of Revision 2.0 of the PC/SC specification, which is expected to be released shortly, similar support has been introduced for contactless smart card readers. It is recommended that organizations interested in deploying contactless smart card readers use PC/SC-compliant readers.

Communication with Applications

After a smart card reader is installed and configured, an application programmer can use the PC/SC API to exchange commands with a smart card in the reader. PC/SC makes an attempt to hide the complexities of different card-reader communications protocols but does not currently provide a higher level abstraction of different card types.¹² The API provides a communications channel for smart card commands. The structure of these commands is defined by ISO standards, but the meaning of specific commands is largely defined by the manufacturer of the individual smart card. Communicating with smart cards at the application level requires programming skill.

Because command semantics are defined by each unique smart card implementation, applications that wish to operate with different types of cards must determine what type of card is present and adapt to the card's command set. For some applications, like payment using the EMV specification, the command set is standardized, and interoperability is assured by the card vendors. Other applications can accomplish the same effect by using programmable card operating systems, such as Java Card™ or MULTOS, so that cards from different vendors can be configured to respond to the same set of application commands.

¹² Version 2.0 of the PC/SC specification is in progress and will provide some higher-level abstractions.

Application Selection

PC/SC provides automatic application selection. Applications can register with PC/SC, requesting notification when a particular type of smart card is inserted in the reader. The insertion of a card triggers the loading of an application that knows how to use that card.

User Authentication

Windows 2000 and Windows XP provide full support for smart-card-based logon and authentication, both to a local machine and to a Windows domain server. The Windows authentication system is built around PKI, using a central certificate authority to issue per-card certificates that are associated with the cardholder's machine or domain username. Microsoft's Internet Explorer and Outlook® applications can also use the certificates on smart cards.

Web and E-mail Services

Many of the Web browsers that run under Windows (such as Internet Explorer and the popular Netscape® and Mozilla families of browsers) can use the smart card as a PKCS#11 token. A PKCS#11 token holds certificates and performs private key operations. The certificate on the smart card can perform client-side certificate-based authentication to a Web server, using the SSL/TLS protocols. In addition, the certificate can digitally "sign" Web forms. Not only does a digital signature provide integrity and authenticate the origin of the form's contents, in some places it can also be a legally-binding signature.

Many of the e-mail clients that run on the Windows platform, such as Microsoft Outlook and the e-mail clients integrated into the Netscape and Mozilla Web browsers, can also use smart-card-based certificates to sign and encrypt e-mail messages. Digitally signing an e-mail message ensures that the recipient can trust the identity of the sender – especially important since an e-mail message "from" address can be easily forged. E-mail encryption ensures that only the intended recipient can read a message and any attachments. Since e-mail messages routinely traverse many servers and routers, often over public networks, encryption is necessary when private communications are desired.

Microsoft Outlook supports the S/MIME standard technology for digitally signing and encrypting e-mail messages. S/MIME uses public/private key pairs, embodied in certificates, to perform signing, encryption, and decryption operations. The PKCS#11 standard enables Outlook to use a private key stored on a smart card to perform digital signing and decryption operations. Encryption is performed using public keys stored by Outlook on the user's PC.

File System Encryption

The NTFS file system provided by Windows NT, Windows 2000, and Windows XP offers per-file and per-directory encryption to protect file contents (but not file names). The file encryption keys are encrypted with one or more public keys and stored with the encrypted files. The private key used to retrieve the file encryption key is also usually stored on the local file system but can be stored on a smart card for greater security.

To the user of the system, the encryption and decryption are transparent. Once the system is configured, the user can select files that should be secured. Those files will open only when the smart card is inserted and be inaccessible when the smart card is removed. Accessing and writing to

encrypted files is often noticeably slower than the same operations on unencrypted files.

Support Offered by Different Windows Versions

Different versions of the Windows operating system offer different levels of support for smart cards. The newest version, Windows XP, has the best support. It provides all of the features described above and comes with built-in drivers for a good selection of smart card readers. Nearly all other smart card reader manufacturers provide drivers for use with Windows XP.

Windows 2000 also has extensive support for smart cards. The only significant difference between Windows 2000 and Windows XP is in the selection of smart card reader drivers provided out-of-the-box. But again, other reader manufacturers provide drivers that function with this operating system.

Windows NT, Windows ME, and Windows 98 all provide some level of support for smart cards. They provide most of the capabilities described above but do not provide a wide selection of reader drivers. In addition, minor difficulties frequently occur, particularly during the installation process. Windows ME and Windows 98 do not use the NTFS file system and do not provide file system encryption features, nor do they provide smart-card-based logon.

Windows 95 and Windows 95SE provide no built-in support for smart cards. Microsoft has created a module that can be installed to implement smart card support, but the module is notoriously difficult to get working. Currently, Microsoft has formally dropped support for Windows 95, and it is not clear how much longer Microsoft will continue to distribute the smart card support module.

Linux

Smart card capabilities have been available for several years for systems running the Linux operating system. There is no smart card support available within the Linux kernel, but user space tools provide a powerful environment for smart card technology. Most of the smart card work for Linux and other Unix[®] operating systems is performed by the MUSCLE project (for more information, see www.musclicard.com).

One key difference between the smart card support provided by Linux or by a variety of Unix and the Windows operating system is the options. The options available from Microsoft are few but complementary. The open source world provides greater choice, but many of the tools, particularly for implementing high-level functionality, are somewhat duplicative. Users of smart card security functions in the open source world must do more research to understand what options are available, but this effort is generally rewarded with a more appropriate and more flexible solution, often with no required license fees.

Smart Card and Reader Communications

The central component of the Linux smart card infrastructure is a tool called PCSC Lite. PCSC Lite implements the PC/SC API defined by the PC/SC Workgroup. This implementation provides the same basic tools as the PC/SC implementation in Microsoft's Win32 API.

PCSC Lite

PCSC Lite is open source software, licensed under a BSD[®]-style license, which essentially gives everyone permission to do anything they like, as long

as they pass the license along (see the copyright notice in the PCSC Lite source files for details). PCSC Lite has been ported to many different platforms, including Linux, Solaris™, FreeBSD, NetBSD, OpenBSD, Mac OS® X, HP-UX, and Microsoft Windows. Porting it to other operating systems is fairly easy.

PCSC Lite is stable, fast, and easy to use. In fact, some Windows deployments of smart cards have opted to use PCSC Lite, rather than the native Windows PC/SC implementation, because of the transparency and flexibility of PCS Lite.

Free support for PCSC Lite is available through the project's mailing list, which is also where design and development discussions occur. Questions are often answered within an hour and nearly always within a day or two, often by the PCSC Lite developers themselves. Most installation and development questions can be answered by searching the list archives. Paid support is available from some of the developers of PCSC Lite and can also be obtained from companies who specialize in supporting open source software, such as Red Hat.

Most Linux distributions provide easy-to-install binary packages that automatically install and configure PCSC Lite.

Reader Driver Availability

Many smart card manufacturers provide PCSC Lite reader drivers. When manufacturer-provided device drivers are not available, independently developed drivers often are.

Drivers for a large selection of smart card readers are available at www.musclecard.com/drivers.html. In addition, many smart card readers use compatible chip sets, so readers that are not listed explicitly often function with an appropriate driver. The best approach is to select a reader that is known to have good manufacturer support for PCSC Lite. However, drivers for other readers can often be located through the reader manufacturer or the PCSC Lite mailing list. If necessary, an experienced programmer with the right skills and the appropriate manufacturer documentation should be able to produce a solid driver in 1 to 2 weeks. Many of the PCSC Lite developers offer driver development services.

Most Linux distributions provide prepackaged and often preinstalled drivers for the most common smart card readers.

CCID

There is a CCID driver for PCSC Lite, so all CCID-compliant smart card readers should work on all platforms supported by PCSC Lite.

User Authentication

The MUSCLE project provides the tools required to implement smart-card-based logon and other authentication for any operating system that uses the Pluggable Authentication Modules (PAM) system for authentication. These systems include Linux and most Unix operating systems. MUSCLE provides the PAM module, a Java Card applet (for the smart card), management tools, and complete instructions for installing and using the MuscleCard authentication system. Oberthur AuthentIC and Axalto Cryptoflex cards are supported out-of-the-box, as are all other PKCS#11-compliant smart cards.

The MuscleCard system has also been ported to Windows, as a Windows Cryptographic Service Provider Module, enabling the Windows smart card infrastructure to be used with MuscleCard cards.

Web and E-mail Services

The MuscleCard project provides PKCS#11 modules that enable Web authentication and form signing in all of the major Linux, Unix, and Macintosh® Web browsers. The project also provides S/MIME integration for nearly all of the e-mail clients that support S/MIME. Support is provided on any PKCS#11-compliant card or any Java Card through the MuscleCard applet.

In addition, some e-mail clients, like Kmail, provide PGP/MIME for digital signing, encryption, and decryption of e-mail messages.

File Encryption

Although Linux includes several tools for file encryption, none provide the convenience of NTFS file encryption. However, tools are available that allow smart cards to unlock any of the Linux-encrypted file systems.

One Linux 2.4 tool, Cryptoloop, transparently encrypts and decrypts an entire disk partition. Configured in one way, Cryptoloop can encrypt an entire system, so that the system will not even boot without presentation of an appropriate password or smart card. Configured another way, Cryptoloop can protect a block of storage within an otherwise unsecured partition. In any configuration, Cryptoloop has the advantage that file names and sizes, as well as file contents, are hidden from unauthorized users. Unfortunately, Cryptoloop's security has been questioned by experts.

With the introduction of Linux 2.6, dm_crypt became the recommended way to achieve transparent file encryption. Like Cryptoloop, dm_crypt works on complete disk partitions or on blocks of storage that act like partitions. dm_crypt has significantly better performance than Cryptoloop and, depending on the encryption cipher chosen, can operate almost as quickly as an unencrypted file system.

In addition to transparent file-system-level encryption tools, tools are available that provide encryption services for single files or file archives. Some of these tools protect file names and sizes as well as file contents, and many of them integrate with smart cards. The user must take steps to encrypt or decrypt each file for use. Although a thorough overview of these tools is beyond the scope of this document, one example, KGPG, provides drag-and-drop file encryption and decryption using the GNU Privacy Guard tool.

Support Offered by Different Varieties of Unix

Nearly all of the smart card functionality described here is available under any of the Unix operating systems, including NetBSD, FreeBSD, OpenBSD, Solaris, HP-UX, Mac OS X, IRIX®, and many others. The only exceptions are Cryptoloop and dm_crypt, which operate under Linux only.

For more information about smart-card-related tools and functions on non-Windows platforms, use any Internet search engine (such as Google) and the PCSC Lite mailing list.

Using Smart Cards for Multiple Applications

Organizations that select smart cards for logical access control can include additional applications on the card. Two recent developments have made it practical to use a single smart card for multiple applications. First, card memory capacities have increased. Second, multi-application operating systems are now available.

Supporting multiple applications on the same card offers a number of advantages:

- Reduced costs. The marginal increase in cost for adding applications to a card is significantly less than issuing additional cards.
- Cardholder convenience. It is more convenient to carry one card than many.
- Improved efficiency. In some cases, it may be possible to use the same digital credentials for a number of applications, further increasing the benefits of multi-application cards.
- Enhanced business case. By supporting multiple applications with a single smart ID badge, organizations can improve the return on investment for the ID technology and preserve flexibility for handling future organization needs.

Multi-Application Usage

Smart cards that implement logical access applications can support a variety of other applications, including the following:

- Physical access applications
- Payment applications
- Secure data storage
- Secure document signature applications
- Form completion applications
- Wireless network access

Physical Access Control

Smart cards are ideally suited for physical access control applications, thanks to their built-in multi-application capabilities. Contactless smart cards in particular constitute an ideal technology upgrade to the widely used 125-kHz proximity technology, offering the convenience and environmental- and vandal-resistant features of proximity technology while adding significant security capabilities, greater storage capacity, and multi-application support.

Physical access control applications can now be implemented using different mechanisms than in the past, when cards were equipped with less memory and fewer security features. In traditional access control systems, a card contains a unique number that points to an entry in a database recording the cardholder's name and access rights. When such a card is presented to a reader, the number is transmitted to a host, which grants or denies access based on the database entry for that number.

The traditional method can still be used by today's smart cards, but a new alternative is available. The alternative is to store all of the cardholder's credential data securely on the smart card itself. When the card is presented to the reader, the reader makes the access decision, allowing card readers to be standalone and not connected to a host system. Because today's smart cards have greater storage capabilities, the actual access transactions can be written to the card and collected later when the cardholder presents the card to an online reader.

Another way in which physical access applications can take advantage of increased card storage capacity is by using biometric data as an authentication factor. The smart card can securely store the cardholder's biometric data. When the card is presented to a biometric reader, the biometric information is retrieved from the card and compared to the actual cardholder biometric captured at the access point to validate the cardholder's identity. If the application uses one of the more powerful smart cards with an embedded microcontroller, the biometric data can be compared and matched on the card. A "match on card" assures the greatest degree of privacy. The biometric data never leaves the card, and the card can be destroyed when the cardholder leaves an organization.

Growing numbers of organizations in both the public and private sectors are adopting smart cards to support physical and logical access using a single card. For example, the new Microsoft employee badge not only opens doors using a contactless interface, it also supports secure network logon using an application that resides on the contact chip embedded in the card.

A combined physical and logical access smart card allows fast identity verification for physical access to buildings, delivers robust user and ID card authentication (by using digital signatures, biometric data, and password/PIN technologies), allows for non-repudiation of transactions, and encrypts e-mail. If an organization seeks such benefits as part of an overall network security plan, the benefits can be quantified and incorporated into the overall business case for adoption of smart card technology.

Currently, one major obstacle to the development of the market for ID cards supporting both physical and logical access is the historical separation of physical security and network security. These two functions are generally handled by two distinctly different parts of an organization, each with a separate mission, budget, and technical infrastructure. However, as smart card technology has become more widely available in a variety of forms (e.g., contact, contactless, USB), more organizations are developing a business case that integrates these two security functions to achieve cost savings and improve organization-wide security.

Payment

Smart cards support payment transactions through both contact and contactless interfaces. For example, the Washington Metropolitan Area Transit Authority (WMATA) issues passengers a contactless smart card called the SmarTrip[®] card. Passengers load a fare amount onto a card, then use the card to access the subway through the entry turnstiles, which simultaneously deduct the fare amount from the amount stored on the card.

Using contactless smart card technology for payment was pioneered in the transit sector, where the combination of secure payment and fast physical access is a critical requirement. Contactless-card-supported payments are also beginning to surface in the general retail sector. American Express, MasterCard and Visa all have programs that use contactless technology to implement secure credit-card payment transactions.

Payment applications can also be supported by a contact chip embedded in the same card body as a contactless chip used for physical access. Currently, contact chips support a wide variety of payment applications, ranging from electronic purses, which store monetary value, to conventional credit and debit transactions. The global EMV specification allows smart cards to support chip-based credit and debit transactions just as magnetic stripe cards do today.

A smart card that is intended initially to support logical access control can include an application that supports a wide variety of payment functions. The combination of these functions can result in a more compelling business case for the adoption of smart card technology. For example, an enterprise's bank can provide a corporate smart card to employees that includes the bank's payment application and a contactless chip used for physical access to facilities. The enterprise benefits from not having to run two separate card programs, and the bank can underwrite some of the cost of managing the physical access program.

Another scenario (and one that has already been implemented in a number of organizations) is the so-called "campus card." The campus card is a multi-application smart card that can be used as an ID card (including a picture) and can also be used to pay for food and items in vending machines, open dormitory doors, check out books from the library, and pay for telephone calls. Generally, these cards employ a variety of technologies, such as magnetic stripe, bar code, and a smart card chip, to support a wide range of applications. Most implementations support physical access control in combination with payment and a variety of additional applications, all of which add value to the card.

Secure Data Storage and Management

Smart cards are being used in a number of innovative ways to support functions that require secure, portable storage of sensitive and not-so-sensitive information. For example, medical records can be stored on a smart card so that only the cardholder or the cardholder's doctor can access the records. Access to such records is typically protected by a PIN.

Similarly, the Department of Defense has issued over 5.4 million Common Access Cards (CAC) to active duty military personnel, selected reserve personnel, civilian employees, and eligible contractor personnel that includes secure storage applications. The CAC can store information related to medical history or other data relevant to cardholder's mission.

Contactless cards used for physical access systems can securely store information that tracks card usage. For example, a contactless card can be used to record data describing access to a particular building (i.e., door location, time, date) for retrieval and auditing. This function can be managed by the card or at a central server.

Wireless Network Access

Smart cards allow organizations to control access to wireless networks. Smart cards can provide strong, multi-factor authentication, support cryptographic protection of content, and facilitate session key management. Additionally, smart cards allow worker mobility within organizations, supporting both seamless reauthentication and configuration management. With a smart card, a PIN, and the appropriate access credentials, wireless users with widely varying information requirements (employees, customers, partners) can uniquely identify themselves to networks or applications.

Application Installation

When a smart card is used to carry multiple applications, the applications can be loaded either before or after the card is issued. Until recently, application installation procedures were proprietary. In the last 2 years, however, Global Platform has created standards for personalizing cards and loading applications. The Global Platform standards allow card issuers to combine solutions from multiple sources with confidence.

Post-issuance installation requires a little more effort than pre-issuance installation. Information about the issued cards must be available, including the amount of memory available on the card, what keys or certificates are needed to access the card, and what keys or certificates are needed to install new applications. Such information is typically available through a card life-cycle management system. Post-issuance installation also requires that the card be able to connect to the host providing the new application. Lastly, installing applications after a card is issued relies on there being a relationship between the application issuer and the card issuer. The card issuer must allow or enable the third-party application to be loaded onto the card. Both parties need information about what is on the card.

Multiple Application Examples

Table 3 shows examples of how multi-application cards are currently being used in many implementations. Detailed information about each implementation can be found in Appendix A.

Table 3: Multi-Application Implementations

Organization	Smart Card Applications
Boeing	<ul style="list-style-type: none"> Employee ID badge Physical access Logical access Windows 2000 logon with PIN, PKI and biometric applets Web single sign-on Password wallet VPN authentication Other planned applications: Data/e-mail encryption, electronic signatures, cafeteria payments, personal data storage, role-based access
Microsoft	<ul style="list-style-type: none"> Employee ID badge Physical access Remote access and logon to corporate networks using PKI
Rabobank	<ul style="list-style-type: none"> Logical access to networks and applications using PKI Microsoft Windows logon Digital signatures
Shell Group	<ul style="list-style-type: none"> Physical access Desktop and network access using PKI Document and e-mail encryption and signing
Sun Microsystems JavaBadge	<ul style="list-style-type: none"> Employee ID badge Physical access Network and desktop logical access Remote network access Single sign-on E-mail, document, and transaction encryption and signing E-purse payment
U.S. Department of Defense Common Access Card	<ul style="list-style-type: none"> Employee ID badge Logical access to networks and desktops using PKI E-mail and document encryption and signing Other planned applications: physical access, biometric authentication
U.S. Department of State	<ul style="list-style-type: none"> Employee ID badge Physical access Logical access using PKI, including desktop security and encryption, secure e-mail, and VPN access Other planned applications: biometrics, secure data storage

The Business Case for Smart Cards and Logical Access

Many enterprises are currently considering the use of smart cards to support secure logical access. A recent study¹³ of U.S. Fortune 500 companies revealed the following:

- All of the companies surveyed (100%) are aware of smart card technology.
- More than 63% of the executives interviewed either have investigated or are investigating smart cards for network security.
- More than 39% of the companies surveyed plan to use smart cards to enhance and strengthen their corporate security systems within the next 3 years.
- A total of 30% of the companies are currently using or testing smart cards within their security systems.

For smart cards to be adopted, the technology investment must be supported by the appropriate business case, which requires consideration of both tangible and intangible benefits.

Intangible Benefits

Businesses invest in strong authentication technology for two main reasons:

- Regulatory compliance
- Strategic positioning

Regulatory Compliance

Businesses are increasingly required to enhance their authentication processes to comply with external requirements. Such external requirements include new legislation or regulations (for example, HIPAA, Sarbanes-Oxley) and other government or industry standards. In such cases, businesses typically are required to demonstrate that they meet certain prescribed standards. Failure to comply with these standards may result in significant financial penalties.

The requirement to upgrade information systems to offer stronger authentication is commonly seen by senior management as the cost of doing business in a given sector or market. In addition, privacy violations can result in significant penalties.

Strategic Positioning

Smart cards form part of the security backbone of an enterprise. In that respect, they are no different from directory servers, VPNs, intrusion detection systems, or firewalls. Businesses are starting to recognize that to maintain a competitive advantage, they need to ensure that their intellectual assets are well defended.

Certain businesses have established a Chief Security Officer (CSO) position to ensure that security concerns are addressed in a holistic manner. To be effective, the CSO position typically reports to the CEO. Smart cards are attractive within such an environment, since they act as a bridge between the physical and logical security domains.

¹³ "Fortune 500 Companies' Preference for Corporate Security Applications," Frost & Sullivan, Feb. 17, 2003.

Tangible Benefits

It is highly probable that an organization considering a smart card deployment will have a legacy infrastructure, typically including the following:

- Username–password-based local authentication
- OTP tokens for secure remote access to protected assets
- An employee ID badge infrastructure with a supporting physical access control system

Organizations often consider a combined physical-logical access system based on smart cards. These cards include a contactless interface to support building access and a contact interface to support logical access. Historically, these two components have been physically separate, but there is a growing trend for both functions to be supported on a dual-interface chip with significant processing and data storage capability.

The benefits of such a system include the following:

- Simplified user management
- Elimination of OTP tokens and associated infrastructure (e.g., servers)
- Increased user productivity

Simplified User Management

Significant expense is associated with the maintenance of traditional password-based authentication systems. For example, the Aberdeen Group has found that the cost of configuring and maintaining password systems for small companies averages \$100 to \$150 per user per year. Costs for a mid-tier company average \$200, and a large enterprise spends an average of \$300 to \$350 per user per year.¹⁴ In fact, it is not uncommon for IT departments to levy an internal charge for handling password maintenance. Smart card management systems offer “self-service” capabilities that can reduce the administrative overhead associated with password management. While secrets (such as PINs) still need to be managed, a smart card management system typically includes an unattended user management capability that can significantly decrease the expense associated with the maintenance of these secrets.

Elimination of OTP Tokens

OTP tokens are expensive to acquire and manage and have a significant failure rate. The typical cost for an OTP token can approach \$100 per year per user. Smart cards offer equivalent functionality but at a reduced total cost of ownership.

Reduction of Overall Infrastructure

Combining logical and physical access applications in a single token offers organizations an opportunity to eliminate redundant technology. Typically, smart-card-based systems can be positioned as an upgrade to, rather than a replacement for, current physical access systems.

¹⁴ “Ask the Analyst: Passwords Are Gobbling Up your Profits,” Jim Hurley, Aberdeen Group, May 1, 2003

Increased Productivity

The introduction of smart cards commonly coincides with other initiatives designed to simplify business workflow, thereby increasing employee productivity and efficiency. Stronger authentication generally increases the efficiency of various internal and external services, yielding a measurable improvement in profitability. Such improvements can be multiplied if trading partners also use the same or interoperable software.

Investment

Smart cards and smart-card-associated systems do represent an investment. The level of investment depends on a number of factors, including the organization's current infrastructure and the authentication technique that is being implemented. The expenditures described below are required to acquire and deploy a smart-card-based authentication system.

Smart Card Tokens. Smart cards themselves are more expensive than legacy ID cards. A premium of \$5 to \$10 per card is typical for smart cards.

Smart Card Readers. It is now not uncommon for computers to be delivered with built-in smart card readers. For legacy systems, a typical external smart card reader that attaches to a computer's USB port can be acquired for about \$15 (in volume). Smart-card-based USB tokens can plug directly into a computer's USB port, requiring no additional hardware investment.

Middleware. To enable the smart card authentication process, middleware must be installed on each user's workstation. Costs range from \$2 to \$10 per seat, depending on the authentication technique being implemented.

Smart Card Management System. A smart card management system supports the issuance and life-cycle management of smart cards and the credentials stored on them. Systems vary in capability and complexity depending on the authentication technique supported and can range from \$5 to \$50 per user.

Authentication Technique Infrastructure. When used for logical access, smart cards implement an organization's selected authentication technique or combination of techniques. Techniques can include passwords of various types, symmetric-key-based authentication, asymmetric-key-based authentication, and biometrics. The cost of the infrastructure to support the chosen authentication technique needs to be considered. Smart cards provide an advantage. Their ability to support multiple authentication techniques on a single ID card allows an organization to implement authentication of the strength required to meet the organization's security requirements. The ability to add applications to smart cards after initial issuance allows organizations to begin using smart cards for simple password storage and add stronger authentication techniques as desired, without reinvesting in cards and readers.

Other Project Costs. Deploying a new identity management system can be a large-scale IT project. Investment will be required in business process reengineering, user training, and support, as well as for initial system configuration and deployment and project management.

Table 4 summarizes key potential benefits, savings, and costs that should be considered when implementing a smart-card-based logical access solution.

Table 4: Smart Card Logical Access Systems – Savings and Costs

Key Benefits and Savings	Costs
<ul style="list-style-type: none"> • Simplified user password management <ul style="list-style-type: none"> - Lower support costs - Increased user convenience • Elimination of OTP token costs • Reduced infrastructure cost by combining multiple functions on a single smart ID badge • Legislative and regulatory compliance • Improved user productivity and reduced operating costs <ul style="list-style-type: none"> - Easier access to networked resources - Improvements to business processes (e.g., document signing) • Reduced risk of security breaches and their resulting costs (e.g., financial, productivity, sales, market position, legal exposure) • Ability to migrate to stronger or different authentication techniques without re-investing in cards and readers 	<ul style="list-style-type: none"> • Smart card token cost • Smart card reader cost (if used with card form factor) • Client middleware • Smart card management system • Infrastructure costs supporting the chosen authentication techniques (e.g., biometrics, PKI, symmetric key) • IT project costs: project management, user training, business process reengineering, system configuration and deployment

Conclusions

Virtually every day another news story highlights the importance of network security – corporate networks are breached, databases are accessed by unauthorized individuals, and identities are stolen and used to conduct fraudulent transactions. As a result, both businesses and governments are evaluating or implementing new identity management systems to provide more secure logical access.

Strong authentication for logical access requires the use of multiple authentication factors. Smart card technology – typically used in conjunction with a PIN to unlock the card – is increasingly being used to offer the critical second or third factor of authentication that makes logical access more secure.

Smart card technology is available in multiple form factors (plastic card, USB device, or mobile phone SIM chip) and supports any or all of the authentication techniques commonly used to secure logical access. Smart card devices are themselves secure, tamper-resistant, and easy to use. Smart cards can support multiple applications, allowing a single ID card to perform multiple functions. For example, the same smart ID card can allow an individual to enter a building securely, log onto the corporate network securely, sign documents securely, encrypt e-mail and transactions, and pay for lunch at the organization's cafeteria. This flexibility makes it easy for organizations to develop a strong business case for smart-card-based access control systems.

The Smart Card Alliance urges organizations who are evaluating new identity management and logical access control systems to implement strong authentication using smart card technology. Smart card technology provides the foundation for privacy, trust and security in logical access applications. The combination of smart card technology and multi-factor authentication improves security, enhances user convenience and delivers powerful business benefits.

For more information about smart cards and the role that they play in secure identification and other applications, please visit the Smart Card Alliance web site at www.smartcardalliance.org or contact the Smart Card Alliance directly at 1-800-556-6828.

Reference and Resources

"2004 E-Crime Watch™ Survey Shows Significant Increase in Electronic Crimes," CSO Magazine survey conducted in cooperation with the United States Secret Service and Carnegie Mellon University Software Engineering Institute's CERT® Coordination Center, May 25, 2004

(http://www.csoonline.com/releases/052004129_release.html)

"Ask the Analyst: Passwords Are Gobbling Up your Profits," Jim Hurley, Aberdeen Group, May 1, 2003

"The Boeing Company Chooses Siemens to Enhance Physical and Information Security with Identity Management System," Siemens and Boeing press release, Sept. 8, 2003,

http://www.siemens.com/index.jsp?sdc_p=cs4uo1093899pnflm

"Boeing SecureBadge Program," Sharon Lindley, SecureBadge Program Director, Boeing, Smart Card Alliance Annual Conference presentation, Oct. 16, 2003

Department of Defense Personal Identity Protection (PIP) Program, DoD Directive Number 1000.25, July 19, 2004

(<http://www.dtic.mil/whs/directives/corres/html2/d100025x.htm>)

Electronic Authentication Partnership (EAP), <http://www.eapartnership.org>

"Electronic Authentication Guideline: Recommendations of the National Institute of Standards and Technology," NIST Computer Security Division, NIST Special Publication 800-63, Version 1.0, June 2004

"Endpoint Security Management: Maximizing Best of Breed," IDC report, March 4, 2004

"Fortune 500 Companies' Preference for Corporate Security Applications," Frost & Sullivan, Feb. 17, 2003

"FTC Releases Survey of Identity Theft in U.S. 27.3 Million Victims in Past 5 Years, Billions in Losses for Businesses and Consumers," FTC press release, Sept. 3, 2003, <http://www.ftc.gov/opa/2003/09/idtheft.htm>

Global Platform (<http://www.globalplatform.org>). Industry association that is creating and advancing interoperable technical specifications for smart cards, acceptance devices and systems infrastructure.

"Government Smart Card Handbook," February 2004, available at

<http://www.smartcardalliance.org>

"HIPAA Compliance and Smart Cards: Solutions to Privacy and Security Requirements," Smart Card Alliance report, September 2003, available at

<http://www.smartcardalliance.org>

Initiative for Open Authentication (OATH), <http://www.openauthentication.org>

International Civil Aviation Organization (ICAO) Machine Readable Travel Documents (MRTD), <http://www.icao.int/mrtd/Home/Index.cfm>)

MUSCLE Project (<http://www.musclecard.com>). MUSCLE is a project to coordinate the development of smart cards and applications under Linux.

NIST Personal Identity Verification (PIV) Project (<http://csrc.nist.gov/piv-project/index.html>)

Liberty Alliance, <http://www.projectliberty.org>

“One Card Fits All,” Boardroom Minutes: Technology Intelligence for Business Executives, available at <http://www.sun.com/software/sunone/boardroom/newsletter/0603solutions.html>

OpenCard Consortium, <http://www.opencard.org>

Open Security Exchange (OSE), <http://www.opensecurityexchange.com>

PC/SC Workgroup (<http://www.pcscworkgroup.com>). Industry group who developed the PC/SC specification, which defines how to integrate smart card readers and smart cards with the computing environment and how to allow multiple applications to share smart card devices.

“Phishing Victims Likely Will Suffer Identity Theft Fraud,” Gartner press release, May 14, 2004, http://www3.gartner.com/5_about/press_releases/asset_71087_11.jsp

“Privacy and Secure Identification Systems: The Role of Smart Cards as a Privacy-Enabling Technology,” Smart Card Alliance white paper, February 2003, available at <http://www.smartcardalliance.org>

“Secure Identification Systems: Building a Chain of Trust,” Smart Card Alliance report, March 2004, available at <http://www.smartcardalliance.org>

“Securing the Enterprise,” Albert Leung, Group Marketing Manager, Java Card Technology, Sun Microsystems, Smart Card Alliance Annual Conference presentation, October 16, 2003

Smart Card Alliance Smart Card Reader Catalog, available at http://www.smartcardalliance.org/industry_info/catalog.cfm

“Smart Card Case Studies and Implementation Profiles,” Smart Card Alliance report, December 2003, available at <http://www.smartcardalliance.org>

“Smart Card Deployment at Microsoft,” Microsoft white paper, March 11, 2004, available at <http://www.microsoft.com/technet/itsolutions/msit/security/smartcrd.msp>

USB Implementer’s Forum, <http://www.usb.org>

“Using Smart Cards for Secure Physical Access,” Smart Card Alliance report, July 2003, available at <http://www.smartcardalliance.org>

Publication Acknowledgements

This report was developed by the Smart Card Alliance to discuss the issues with authenticating individuals for logical access and to define the benefits that smart card technology provides. Publication of this document by the Smart Card Alliance does not imply the endorsement of any of the member organizations of the Alliance.

The Smart Card Alliance wishes to thank the Secure Personal ID Task Force members for their contributions. Participants from 22 organizations were involved in the development of this report including: ActivCard, AOS-Hagenuk, Axalto, CardLogix, Datakey, Gemplus, Honeywell Access Systems (OmniTek), IBM, Identix, Litronic/SAFLink, Lockheed Martin, MartSoft Corporation, Northrop Grumman Information Technology, OTI America, SCM Microsystems, Smart Commerce, Inc., Sun Microsystems, U.S. Department of Defense, VeriFone, VeriSign, Visa USA, XTec, Incorporated.

Special thanks go to the individuals who wrote, reviewed and edited this report.

David Asay, IBM
David Berman, VeriSign
Kirk Brafford, Litronic/SAFLink
Yuh-Ning Chen, Ph.D., MartSoft Corporation
Michael Davis, Honeywell Access Systems (OmniTek)
Patrice Erickson, Identix
Nick Hislop, Gemplus
Mansour Karimzadeh, Smart Commerce, Inc.
Colleen Kulhanek, Datakey
Kevin Kozlowski, XTec Inc.
Albert Leung, Sun Microsystems

Mark McGovern, Lockheed Martin
John McKeon, IBM
Cathy Medich, Consultant & Task Force Chair
Yahya Mehdizadeh, Axalto
Bob Merkert, SCM Microsystems
Neville Pattinson, Axalto
Dwayne Pfeiffer, Northrop Grumman Information Technology
Bruce Ross, CardLogix
Nick Stoner, Lockheed Martin
Shawn Willden, IBM

Copyright Notice

Copyright 2004 Smart Card Alliance, Inc. All rights reserved.

Trademark Notices

All registered trademarks, trademarks, or service marks are the property of their respective owners.

Apple, Macintosh and Mac OS are trademarks of Apple Computer, Inc., registered in the U.S. and other countries.

BSD is a registered trademark of Berkeley Software Design, Inc.

CosmopolIC is a trademark of Oberthur.

Entelligence is a trademark of Entrust.

IRIX is a registered trademark of Silicon Graphics, Inc., in the U.S. and/or other countries.

Mediametric is a trademark of XTec, Incorporated.

Microsoft, Windows, Windows NT, Win32, Outlook are either registered trademarks or trademarks of Microsoft Corporation in the U.S. and/or other countries.

MIFARE is a trademark of Philips Semiconductors.

Netscape is a registered trademark of Netscape Communications.

OS/2 is a registered trademark of IBM Corporation.

SecurID is a registered trademark of RSA Security Inc. in the United States and/or other countries.

S/KEY is a registered trademark of Bell Communications Research.

SmarTrip is a registered trademark of WMATA.

Sun, Sun Microsystems, Sun Ray, Java, Java Card and Solaris are trademarks or registered trademarks of Sun Microsystems, Inc. in the United States and other countries.

Unix is a registered trademark of The Open Group.

Appendix A: Smart Card User Profiles

Many organizations are working on improving the security of logical access to their networks, data, applications, and services. This appendix includes profiles of the following organizations, all of which are implementing smart-card-based logical access systems:

- Boeing
- Microsoft
- Rabobank
- Shell Group
- Sun Microsystems
- U.S. Department of Defense
- U.S. Department of State

Boeing^{15,16}

Boeing is implementing a smart-card-based employee identification card, called SecureBadge. More than 200,000 Boeing employees, contractors, and partners are scheduled to receive the multi-function smart card over the next 5 years. The new SecureBadge supports Boeing's goal: to increase access security for both information systems and buildings.

A number of business issues drove Boeing to implement a smart-card-based employee ID card. Mergers and acquisitions had resulted in multiple identity management processes. After a new standard identity management process was defined, the Boeing employee badge needed to be updated to support the process. Boeing also wanted to deploy stronger authentication methods and replace the inherently weak password approach. While using extremely long passwords mitigates the risk of weak passwords, Boeing needed a way to store these keys that was controlled by the user.

The result was the definition of the Boeing SmartBadge program, which uses a standardized badge with a smart chip. The smart ID card integrates the current Boeing physical access control system, directory infrastructure, and Web-based single sign-on portal. The smart card contains PIN, PKI, and biometrics applications that support Windows 2000 logon, Web single sign-on, password wallet, and VPN authentication applications. Boeing plans to implement new applications in the future to support data and e-mail encryption, electronic signatures, cafeteria payments, personal data storage, and role-based access.

Boeing has found that the SmartBadge delivers multiple benefits to the organization. Two-factor authentication strengthens the security of desktop access, replacing the less secure user IDs and passwords. The single badge for access to both enterprise facilities and IT resources provides greater overall security for the organization. Interoperability among different entities using the SmartBadge is enhanced through the definition of trust relationships. Finally, Boeing expects to see savings in excess of what might

¹⁵ "The Boeing Company Chooses Siemens to Enhance Physical and Information Security with Identity Management System," Siemens and Boeing press release, Sept. 8, 2003, http://www.siemens.com/index.jsp?sdc_p=cs4uo1093899pnfilm

¹⁶ "Boeing SecureBadge Program," Sharon Lindley, SecureBadge Program Director, Boeing, Smart Card Alliance Annual Conference presentation, Oct. 16, 2003

have been achieved by using other two-factor remote authentication approaches.

Microsoft¹⁷

Microsoft has deployed a smart card employee identity system that manages both physical access and remote logical access to company networks. Microsoft completed worldwide deployment of the smart ID card at the end of 2002.

With industry-wide security threats to corporate network access increasing, Microsoft initiated the smart card project in late 2000 to implement a two-factor security solution for remote access to company networks. Due to Microsoft's size (more than 61,000 employees in over 400 locations worldwide), managing the security risks inherent in remote access was a critical problem.

Microsoft evaluated a number of technologies before deciding on smart cards, including biometrics, other hardware tokens (e.g., devices that automatically calculate new passwords at specified times and match passwords generated by a similar password-changing device on an authentication server), and USB token-reader devices similar to smart cards. Microsoft chose to deploy smart card technology due to the combination of reliability, performance, cost, features, mobility benefits, and integration with the Windows network environment.¹⁸

Microsoft has reported the following benefits of deploying employee smart cards:¹⁹

- Strengthened security. Two-factor authentication with smart cards (requiring both the smart card and PIN) provides stronger security than simply entering valid credentials.
- Increased flexibility. Smart cards carry security certificates and can be used for other projects. The ability of smart cards to support other applications (such as digital e-mail signatures, document signatures, personal data storage, and personal payment systems) was viewed as a key benefit.
- Ease of use. Users find smart cards simple to use, with no bulky device to break or cumbersome password generator to carry. Microsoft designed the smart card implementation to minimize the impact on users when using the smart card during the remote authentication experience. The smart ID card was also a familiar form factor, since employees already carried an RFID-style photo ID cardkey to access buildings. By implementing a smart ID card that combined the smart chip and RFID capability, Microsoft avoided requiring employees to carry (and possibly lose) an additional card.
- Leverage of existing infrastructure. Microsoft uses the PKI capabilities native to Windows 2000 Server and Windows 2003 Server to create security certificates and manages the process internally.

¹⁷ This profile extracts content from the Microsoft white paper, "Smart Card Deployment at Microsoft," March 11, 2004, available at www.microsoft.com/technet/itsolutions/msit/security/smartcrd.msp

¹⁸ "Smart Card Deployment at Microsoft," Microsoft white paper, March 11, 2004

¹⁹ Ibid.

Rabobank²⁰

Rabobank Group is the largest Dutch retail bank, operating nearly 1,500 offices and 380 local banks. A total of 33,000 of its 50,000 employees worldwide serve 9 million customers in the Netherlands. Rabobank Group's specialized banking businesses are the market leaders in virtually all financial services, from leasing and trade finance to insurance, venture capital, and private banking

Although revolutionary changes in banking practices and technologies over the past century have completely altered the culture of the industry, customer demands for trust and security remain constant. An increasing number of technology-savvy financial customers around the world expect to initiate secure transactions over the Internet or by phone at any time. As a result, large financial organizations like Rabobank Group have implemented both internal and external security strategies to keep pace with the technology requirements associated with electronic banking.

Rabobank Group has stayed several steps ahead of these increasingly complex technological challenges by consistently investing in a security infrastructure and strategy it calls Rabo Web Security (RWB), deployed enterprise-wide by its Zeist-based ICT Group.

"The bank's way of working today is quite different from the past and much more distributed," says Ad Bezemer, Project Manager of Infra Services at Rabobank ICT headquarters in Zeist. "Financial services have become much more complicated, as integrated products and several distribution channels are emerging. In the past, security meant shielding off hackers and intruders, but today, it means building the highest levels of trust right into our systems and communications."

To build the highest levels of trust into its systems as it moves closer to the future vision of "anytime, anywhere banking," Rabobank ICT has applied its forward-looking security strategy to several fronts, including its own internal communications and channels. Since 1997, Rabobank ICT has been moving all applications (which in the past had disparate security and required multiple passwords) to its intranet, to make them available on all distribution channels. "This move enables us to centralize the security around these applications," explains Ad Bezemer.

To control access to these centralized applications and ensure strong authentication of its internal employees, Rabobank is deploying 33,000 smart cards combined with PKI technology. The cards enable a new level of security and efficiency for internal employees.

The deployment of smart cards is eliminating the risks inherent in a "knowledge only" system based on multiple passwords. This is accomplished by using two-factor security that incorporates something that is owned (the smart card) and something that is known (the user's password). In e-business security language, the smart cards provide non-repudiation – two-factor security authenticates users unequivocally – and therefore guarantee integrity and security

²⁰ This profile is an updated extract from a case study that was developed by the Smart Card Alliance with the assistance of Datakey and published in August 2002. For additional information, the complete case study is available in the Smart Card Alliance report, "Smart Card Case Studies and Implementation Profiles," available at www.smartcardalliance.org.

Because Rabobank's cooperative banks decide independently on their local needs and requirements, some are also using the smart cards for physical access. To meet the specific requirements of those banks, the smart cards are delivered with custom formats that include magnetic stripes and proximity technology. All employees use the smart cards to access the network, log onto Microsoft Windows, and provide digital signatures.

Rabobank has given several hundred additional smart cards to large customers for special transactions. In international scenarios, for example, the smart card is used for dealing room currency transactions. The customer is able to do an immediate buy or sell in the exact dollar (or other currency) amount without incurring the risk of losing funds through currency fluctuations. "By ordering the currency transaction directly with the smart card, the customer is able to sidestep the process of calling the bank and arranging a transaction which may take a month or two to complete," says Ad Bezemer. "The usually 10-second confirmation makes the transaction almost real-time, versus the risky delays with the old process. The smart card offers our currency-trading international customers speed, cost-efficiency, and transactional security."

Shell Group²¹

In the winter of 1999, the Royal Dutch Shell Group (www.shell.com) looked at the high total cost of ownership (TCO) for managing their desktop/IT environment and decided it was time for a change.

Shell sought a new approach, one that would have a positive effect on the bottom line while also improving security. In addition, the new approach needed to be simple and user-friendly and offer a clear path to e-business capabilities in the future.

Faced with the ever-escalating costs of password management, Royal Dutch Shell embarked on a smart card project as an important component of their Group Infrastructure/Desktop (GID) initiative. The GID was tasked with, among other things, reducing the support costs for PCs. To reduce those costs, Shell focused on reducing password management costs, which industry estimated at \$100 per user per year. By adopting a variety of technologies, such as thin clients, smart cards, and PKI, Shell hoped to reduce their desktop TCO by 50%.

The Hague-based energy corporation asked Axalto to deliver a global IT solution using smart cards integrated into Windows 2000. The project solution eventually affected 85,000 Shell employees at 1,200 sites across 134 countries.

Shell's goal was a unified security offering integrating physical, thin client, and desktop access. Smart cards constituted the best solution, allowing all of these services to be offered on a single platform that also supported existing physical access systems. The Microsoft Windows 2000 platform provided smart card support as part of its native PKI capability and offered integrated single sign-on using Kerberos.

²¹ This profile is an updated extract from a case study that was developed by the Smart Card Alliance with the assistance of Martha Jones, Axalto, and Bryan Ichikawa and published in April 2002. The full case study is available in the Smart Card Alliance report, "Smart Card Case Studies and Implementation Profiles," published in December 2003 and available at www.smartcardalliance.org.

With the massive proliferation of networks, Internet, thin clients, and PCs, Shell faced a fundamental problem: how to know who was really on their network. In the past, authentication was managed with passwords, but because passwords are expensive and provide very little security, a different, more cost-effective solution was required. Smart cards provide strong authentication of end users. Shell uses smart cards to authenticate users, reduce support costs, and leverage the investment in network equipment and IT personnel. Using one card, Shell employees have physical access to their facilities, can log onto the network from any device, and can sign and encrypt documents and e-mail. A Web-based card management system makes the cards easy for Shell and Shell employees to manage.

Through careful and thorough planning and commitment to consistent technologies, Shell has succeeded in this technically and logistically complex undertaking. As of July 2004, 100,000 smart ID cards have been issued worldwide, implementing the PKI applications. Currently, Shell is evaluating adding health, safety, and environment information to the employee smart cards.

Sun Microsystems JavaBadge

"At Sun Microsystems™ we created a new smart card solution for network security and physical access control called JavaBadge," said Chris Saleh, marketing manager and program manager for JavaBadge. "We've rebadged every Sun™ employee worldwide, with over 31,000 JavaBadges issued. We are using Java Card™ technology manufactured by Axalto and readers from SCM Microsystems as well as our own embedded ones. The cards have a magnetic stripe and MIFARE™ contactless chip for access control, with most of Sun's entry doors converted to contactless smart card technology now. We chose Java Card technology because it offers the important advantage of being able to dynamically add applications in the field in real time."



Sun's implementation of JavaBadge had several objectives:²²

- Securely enable the virtual enterprise by rebadging employees with a multi-application Java™-powered digital ID card for authentication throughout the enterprise and convenient access to enterprise services
- Improve security and increase productivity
- Reduce costs and complexity
- Provide a single federated source for all credentials
- Deliver best practices and expertise for use in customer enterprise deployments

Sun's implementation is an excellent example of how smart cards can help enterprises move to a single multi-application ID card or badge that cost-effectively replaces multiple credentials. Sun launched the JavaBadge program to unify a number of Sun credential-based applications on one centrally issued and managed platform. The initial JavaBadge was designed to replace multiple cards:

- Sun's corporate badge/identity card
- The Sun Ray™ appliance session mobility card

²² "Securing the Enterprise," Albert Leung, Group Marketing Manager, Java Card Technology, Sun Microsystems, Smart Card Alliance Annual Conference presentation, October 16, 2003

-
- An authentication token card used by employees to authenticate themselves to systems, applications, and the network from remote locations (e.g., home, hotel), and to digitally sign and encrypt documents and transactions for non-repudiation and improved security
 - A remote access challenge/response token
 - An e-purse/payment card²³

One application of the card is building access, but the main reason Sun adopted smart cards was to implement logical access to the company's network using Sun Ray™ appliances, the thin clients deployed at Sun. "We have flexible offices for 25,000 employees, meaning you do not always work at the same office," said Saleh. "Sun Ray delivers IT services in a very cost effective manner, because all sessions reside on servers. The smart card is the key to the system, because it lets people bring up their own sessions and user environment."

"For example, say you want to leave for the gym. You pull out your JavaBadge from the Sun Ray appliance, which powers down to save energy. When you return from the gym you go to another office and use your card to get your session back up again. Once you insert the JavaBadge into the appliance it powers up, gets your personal session from the Sun Ray appliance and takes you right back to your personal session where you left off. Sun calls it 'Session Mobility,' which is being able to carry your user environment from one area to another," explained Saleh.

"We're entering a new phase with Java Card technology to issue certificates on smart cards," said Saleh. "We'll have three applications secured by a public key infrastructure: authentication/single sign-on, signature, and encryption for secure e-mail transmissions. For higher levels of security we want dual-factor authentication – what you have and what you know. The card is what you have and the personal identification number is what you know in order to log in to services. Down the road, maybe we'll use three-factor authentication with the addition of biometrics."

There were many reasons for Sun to go to smart cards in addition to the ability to use the Sun Ray appliances. "It's technically safer to store PIN and key information on smart card hardware tokens than on a computer hard drive in some server room. It eliminates the inefficient use and inherently weak security of passwords. We were motivated to go to smart cards for legal reasons too. To move commerce to the Internet, we needed a robust system that offers non-repudiation, and Europe dictates smart cards and PKI to achieve this. Finally, the smart cards enabled us to consolidate four or five credentials into one card," stated Saleh.

According to Sun, financial analysis clearly demonstrates savings from using one card instead of many. The JavaBadge costs \$284.80 per person over 5 years and the single function cards cost \$395.20 per person over 5 years.²⁴

"The user reaction is extremely positive. The consolidation of cards, not having to remember as many passwords, mobility and increased sense of security are huge pluses and convenience for them. We are a big proponent of smart cards," he concluded.

²³ "One Card Fits All," Boardroom Minutes: Technology Intelligence for Business Executives, <http://www.sun.com/software/sunone/boardroom/newsletter/0603solutions.html>

²⁴ Boardroom Minutes: Technology Intelligence for Business Executives, op.cit.

U.S. Department of Defense²⁵

One of the most advanced smart ID card programs in the United States is the Department of Defense (DoD) Common Access Card (CAC), a smart card that serves as the DoD standard identification for active duty military personnel, selected reserve personnel, civilian employees, and eligible contractor personnel. The CAC is the principal card used for logical access to DoD computer networks and systems, and it will be the principal card used to enable physical access as systems are installed for authentication and access at DoD facilities in the future. As of July 2004, DoD has issued over 5.4 million smart cards. (This number includes reissues to accommodate changes in name, rank, or status and to replace lost or stolen cards.) As of the same date, approximately 3 million unexpired or active CACs are in circulation. DoD has deployed an issuance infrastructure at over 930 sites in more than 25 countries around the world and is rolling out more than 1 million card readers and associated middleware. A key goal of the CAC program is to meet DoD's mandate to sign all electronic mail and other electronic documents digitally.

Future plans include using the CAC to sign and encrypt e-mail, expanding the number of portals capable of doing Web-based e-business using PKI authentication tools, adding a biometric to the card to provide three-factor authentication, and expanding the use of the cards to include physical access by adding a contactless chip using ISO/IEC 14443 Parts 1-4 with a FIPS-approved algorithm.

DoD's personnel identity protection addresses threats to the privacy of its members, employees, and beneficiaries, establishes a secure and authoritative process for the issuance and use of identity credentials in DoD, and ensures that DoD benefits and access to DoD physical and logical assets are granted based on authenticated and secure identity information. DoD personnel identity protection systems include, but are not limited to the CAC, The Defense Biometrics Identification System (DBIDS), the Defense National Visitors Center (DNVC), and the Defense Cross-Credentialing Identification System (DCCIS).

The DBIDS is a readily deployable system for capturing, storing, and comparing biometric data to use for authentication. The system also provides a means of registering all personnel requiring access, incorporating complex rules of sponsorship and access, linking access to sponsor, and limiting access by location, building, and force protection level. In addition, DBIDS allows installation security personnel to control access and authenticate identity for population elements not already provided for by DNVC and DCCIS, including maintenance personnel, janitorial staff, and contractor personnel from non-DoD organizations.

DNVC is a system that enables participating DoD facilities to perform physical authentication procedures on DoD personnel presenting the CAC for entrance into DoD facilities. The DNVC is part of the DoD identity management strategy, designed to issue tamper-free smart cards to verified individuals and to authenticate both the credential and the credential holder whenever the card is presented. DNVC is designed to accommodate different readable formats supported by the CAC and uses biometric data as the primary method of authentication. The DNVC is Web-based and

²⁵ Additional information about the DoD CAC program and other U.S. government smart card initiatives can be found at http://www.smart.gov/smartgov/smart_card.cfm.

provides a means for strengthening security across participating DoD organizations.

DCCIS is an extension of DNVC. DCCIS is an initial proof-of-concept system that proposes to resolve cross-credentialing interoperability difficulties between DoD and certain of its commercial partners. DNVC can be DCCIS-enabled, in which case a participating DNVC facility connects with the DCCIS member organization database to authenticate visiting personnel from those organizations.

As initial issuance of the CAC nears completion, DoD's focus has expanded to include post-issuance CAC support and ensure interoperability with other smart card initiatives throughout the Federal Government. As the government becomes more aware of the importance of identity authentication and assurance, the need to define common policies, interoperability requirements, and technical standards becomes more apparent.

DoD is also in the early stages of planning to serve other large communities that are closely tied to DoD, including military dependents, DoD recipients of health care services from the TRICARE medical system, and veterans.

U.S. Department of State²⁶

The U.S. Department of State is implementing smart ID cards to function as an individual's identification card. All State Department employees, contractors, and affiliates who work within the department will be issued smart ID cards by the Bureau of Diplomatic Security to be used for physical access. The Bureau of Information Resource Management (IRM), which oversees logical access, will use the smart ID card as a token for a PKI. The Department of State is one of the first federal agencies to use a smart card for physical access, logical access, and PKI.

Employees and contractors will be required to insert a smart ID card in a card reader installed at external and internal entrances that allows only authorized users to access the facilities. The readers are secure, programmable readers provided by XTec™ Incorporated. One beneficial feature of the readers is the ability for a security manager to inject authentication keys into the reader securely. The State Department is one of the first agencies to adopt the Physical Access Interagency Interoperability Working Group High Security Profile for card authentication. In addition, the smart ID cards and the readers adhere to the Government Smart Card Interoperability Specification (GSC-IS).

Another value of the programmable readers is their ability to communicate with the different legacy access control systems currently deployed at the State Department. The State Department has a 3-year migration path to update or replace the current legacy access control system. The programmable reader allows both the legacy MDI OS/2® system and the newly installed Software House C*Care system to operate with the smart cards. From a user's perspective, the conversion is invisible. The State Department therefore has the ability to replace the old Wiegand card technology in a shorter time period.

Approximately 130,000 users will use the new card to access State Department buildings. The State Department has almost completed issuing the cards domestically and is now in the process of issuing cards overseas.

²⁶ This implementation profile was developed by the Smart Card Alliance Secure Personal ID Task Force as part of the report "Using Smart Cards for Secure Physical Access," July 2003, available at www.smartcardalliance.org.

Because it is one of the first agencies to fully adopt the GSC-IS, the State Department is able to issue a variety of smart cards to meet specific needs. Two cards are used strictly for access control: the XTec Secure Mediametric™ memory card and the Oberthur CosmopolIC™ Java™ card. In addition, the Datakey 330G file card is being used for access control and for logical access applications such as secure e-mail, network authentication, and logon using the smart card and biometrics.

The majority of State Department users (80% to 90%) will use their smart ID cards for PKI applications, including desktop security and encryption using Entrust Entelligence™, secure e-mail, and VPN access. As of July 2004, approximately 15,000 desktops support PKI, with the rollout planned to be complete within the next 18 months. Biometrics are currently being integrated to control logical access and possibly physical access into sensitive areas. The State Department plans to store other data on the smart card, including emergency medical information, human resources data, and travel orders.

According to Lolie Kull, former smart card implementation manager for the State Department, "The smart card brings it all down to one simple, safe and secure denominator. One single token will simplify how we practice security as we get in the door or access our computers. At the same time, it heightens security by 100%. The solution to our security challenges is this one smart card that does it all."

Appendix B: Industry Initiative Profiles

In addition to the Smart Card Alliance, a number of industry initiatives are addressing issues that arise while implementing new logical or physical access systems and promoting the use of standards-based technology. This appendix includes brief profiles of the following organizations, with links for additional information.

- Electronic Authentication Partnership
- Liberty Alliance Project
- Initiative for Open Authentication (OATH)
- Open Protocol Exchange Network
- Open Security Exchange
- OpenCard Consortium

Electronic Authentication Partnership

The Electronic Authentication Partnership (EAP) is a cross-industry partnership whose objective is to enable interoperability among public and private electronic authentication systems. Interoperability of e-authentication systems is essential to the cost-effective operation of safe and secure systems that perform essential electronic transactions and tasks across industry lines.

EAP's goal is to provide organizations with a straightforward means of relying on digital credentials issued by a variety of e-authentication systems. The EAP intends to build on the work of other organizations in the electronic authentication world, not replace existing individual industry-wide authentication protocols.

The EAP intends to foster interoperability among electronic authentication systems by:

- Drafting rules for credentials and authentication systems for different and hierarchical assurance levels, to provide a standard set of criteria for evaluating credentials at each level.
- Developing the means to assess credentials and systems against a standard set of criteria and convey that assessment to interested parties.
- Drafting "rules of engagement" that would allow relying parties to use third-party credentials. These rules would take the place of bilateral agreements.
- Creating operating rules for validating credentials and defining how credentials will be validated.

Additional information can be found at the EAP Web site, www.eapartnership.org.

Liberty Alliance Project

The Liberty Alliance Project is an alliance of companies, non-profit organizations, and government organizations from around the world that is committed to developing an open standard for federated network identity that supports all current and emerging network devices. Federated identity offers businesses, governments, employees, and consumers a more convenient and secure way to control identity information in today's digital economy and is a key component needed to drive the use of e-commerce, personalized data services, and Web-based services.

The Liberty Alliance is working to create open technical specifications that enable simplified sign-on through federated network identification using current and emerging network access devices. These specifications also support and promote permission-based attribute sharing, enabling users to control the use and disclosure of their personal identification information.

Another activity of the Liberty Alliance is creating resources that organizations can use when implementing federated identity solutions. These resources include technical specifications, business and policy guidelines, case studies, and white papers.

Membership is open to all commercial and non-commercial organizations.

Additional information can be found at the Liberty Alliance Web site, www.projectliberty.org.

Initiative for Open Authentication

The Initiative for Open Authentication (OATH) is an organization coordinating the collaborative effort of IT industry leaders to provide a reference architecture for universal strong authentication of networked users and devices. Using open standards, OATH helps device manufacturers, software vendors, and service providers integrate these open interfaces within their products to create trusted interoperable solutions. These solutions will create lower cost of ownership and allow customers to replace existing disparate and proprietary security systems whose complexity often leads to higher costs.

The challenges of theft and unauthorized access to confidential data, the inability to share data securely over a network, and the lack of a viable single sign-on framework are all addressed by OATH with standard, open technology that is freely available.

Relying primarily on current standards and specifications for key missing standards, OATH takes an all-encompassing approach to delivering interoperable solutions that allow for strong authentication of all users on all devices, across all networks.

Additional information can be found at the OATH Web site, www.openauthentication.org.

Open Security Exchange

The Open Security Exchange (OSE) is a cross-industry forum that promotes enterprise security management by addressing the lack of integration and interoperability between the various components and technologies that compose the security infrastructure. OSE drives the creation and adoption of interoperability standards by working closely with existing standards bodies and by creating vendor-neutral interoperability specifications and best practices guidelines. OSE promotes these as standards among industry groups for widespread acceptance among users. The standards are available for download by anyone. Using these interoperability standards helps reduce costs and leverages an organization's existing security infrastructure to maximize investment.

As an advisor to government and commercial organizations, the OSE also uses its combined expertise to educate security professionals worldwide about best-practice security.

Any organization can seek an active role in the OSE and membership is open to any organization adhering to OSE operating procedures.

Additional information can be found at the OSE Web site,
www.opensecurityexchange.com.

OpenCard Consortium

The OpenCard Consortium is a standard framework announced by an industry consortium that provides for interoperable smart card solutions across numerous hardware and software platforms, primarily using the Java™ programming environment. The OpenCard Framework (OCF) is an open standard providing an architecture and a set of APIs that enable application developers and service providers to build and deploy smart card aware solutions in any OpenCard-compliant environment.

Since the smart card industry is moving towards standardization and interoperability, smart card vendors need to reduce their mutual interdependencies. OCF facilitates this goal by specifying two interfaces: a high-level API that hides the characteristics of a particular provider's components from application and service developers, and a common provider interface that enables seamless integration of smart card building blocks from different vendors

Additional information can be found at the OpenCard Consortium Web site,
www.opencard.org

Appendix C: Definition of Terms and Acronyms

API

Application programming interface. A formal specification of a collection of procedures and functions available to an application programmer. These specifications describe the available commands, the arguments (or parameters) that must be provided when calling the command, and the types of return values when the command execution is completed.

Asymmetric keys

Two related keys, a public key and a private key, that are used to perform complementary operations, such as encryption and decryption or signature generation and signature verification.

Biometric

Automated methods of identifying or authenticating the identity of a living person based on unique physiological or behavioral characteristics.

Biometric template

The stored record of an individual's biometric features. Typically, a "livescan" of an individual's biometric attributes is translated through a specific algorithm into a digital record that can be stored in a database or on a smart card. The formatted digital record used to store the biometric attributes is generally referred to as the biometric template

BSD

A version of Unix developed at the University of California at Berkeley.

Certificate authority (CA)

A component of the Public Key Infrastructure that is responsible for issuing and revoking digital certificates. Digital certificates may contain the public key or information pertinent to the public key.

Checksum

A computed value that depends on the contents of a message. The checksum is transmitted with the message. The receiving party can then recompute the checksum to verify that the message was not corrupted during transmission.

Cleartext

Data or information that is not encrypted.

Chip

Electronic component that performs logic, processing, and/or memory functions.

Contact smart card

A smart card that connects to the reading device through direct physical contact between the smart card chip and the smart card reader.

Contactless smart card

A smart card whose chip communicates with the reader using RF and does not require physical contact with the card reader.

DES

Data Encryption Standard.

DSA

Digital Signature Algorithm.

Dual interface card

A smart card that has a single smart card chip with two interfaces – a contact and a contactless interface – using shared memory and chip resources.

EMV

Europay MasterCard Visa. Specifications developed by Europay, MasterCard, and Visa that define a set of requirements to ensure interoperability between payment chip cards and terminals.

Gramm-Leach-Bliley

The Financial Services Modernization Act of 1999 (also known as the Gramm-Leach-Bliley Act), enacted to facilitate affiliation among banks, securities firms, and insurance companies. The Act includes provisions to protect consumers' personal financial information held by financial institutions.

GSC-IS

Government Smart Card Interoperability Specification. The GSC-IS was defined to provide the ability to develop secure identification smart cards that can operate across multiple government agencies or among federal, state, and local governments and provides solutions to a number of interoperability issues associated with contact smart card technology implementation.

GSM

Global System for Mobile Communications

Hash algorithm

A software algorithm that computes a value (hash) from a particular data unit in a manner that enables detection of intentional/unauthorized or unintentional/accidental data modification by the recipient of the data.

HIPAA

Health Insurance Portability and Accountability Act of 1996. HIPAA was passed to protect health insurance coverage for workers and their families and to encourage the development of a health information system by establishing standards and requirements for the secure electronic transmission of certain health information. HIPAA mandates that the design and implementation of the electronic systems guarantee the privacy and security of patient information gathered as part of providing health care.

Hybrid card

An ID card that contains two smart card chips – both contact and contactless chips – that are not interconnected.

ICAO MRTD

International Civil Aviation Organization Machine Readable Travel Documents. ICAO establishes international standards for travel documents. An MRTD is an international travel document (e.g., a passport or visa) containing eye- and machine-readable data. ICAO Document 9303 is the international standard for MRTDs.

Integrated circuit

See chip.

ISO

International Organization for Standardization.

ISO/IEC 14443

ISO/IEC standard "Identification Cards - Contactless Integrated Circuit(s) Cards - Proximity Cards."

ISO/IEC 7816

ISO/IEC standard for integrated circuit cards with contacts.

Logical access

Access to online or networked resources (e.g., networks, files, computers, databases).

Man-in-the-middle attack

An attack on an authentication protocol in which the attacker is positioned between the individual seeking authentication and the system verifying the authentication. In this attack, the attacker attempts to intercept and alter data traveling between the parties.

MCU

See microcontroller.

MD5

One of the most popular hashing algorithms, developed by Professor Ronald L. Rivest of MIT, which produces a 128-bit hash from any input.

Microcontroller (MCU)

A highly integrated computer chip that contains all the components comprising a controller. Typically this includes a CPU, RAM, some form of ROM, I/O ports, and timers. Unlike a general purpose computer, a microcontroller is designed to operate in a restricted environment.

Microsoft Crypto API

The Microsoft security framework that developers use to implement security functions for applications that run on Microsoft Windows.

Multi-application card

A smart card ID that runs multiple applications – for example, physical access, logical access, data storage, and electronic purse – using a single card.

NIST

National Institute of Standards and Technology.

Non-repudiation

The ability to ensure and have evidence that a specific action occurred in an electronic transaction (e.g., that a message originator cannot deny sending a message or that a party in a transaction cannot deny the authenticity of their signature).

NTFS

New Technology File System. Windows proprietary file system.

OTP

One-time passwords are passwords that are used once and then discarded. Each time the user authenticates to a system, a different password is used, after which that password is no longer valid. The password is computed either by software on the logon computer or OTP hardware tokens in the user's possession that are coordinated through a trusted system.

PC

Personal computer.

PC/SC

Personal Computer/Smart Card. The PC/SC specification defines how to integrate smart card readers and smart cards with the computing environment and how to allow multiple applications to share smart card devices.

PCSC Lite

Personal Computer/Smart Card Lite. PCSC Lite is open source software that implements the PC/SC specification for Linux.

PGP/MIME

Pretty Good Privacy/Multipurpose Internet Mail Extensions. A protocol for exchanging digitally signed and/or encrypted mail.

Physical access

Access to physical facilities (e.g., buildings, rooms, airports, warehouses).

PIN

Personal Identification Number. A numeric code that is associated with an ID card and that adds a second factor of authentication to the identity verification process.

Public (asymmetric) key cryptography

A type of cryptography that uses a pair of mathematically related cryptographic keys. The public key can be made available to anyone and can encrypt information or verify a digital signature. The private key is kept secret by its holder and can decrypt information or generate a digital signature.

PKI

Public Key Infrastructure. The architecture, organization, techniques, practices, and procedures that collectively support the implementation and operation of a certificate-based public key cryptographic system. Further, a communications infrastructure that allows users to exchange money and data over the Internet in a secure environment. There are four basic components to the PKI: the certificate authority (CA) responsible for issuing and verifying digital certificates, the registration authority (RA) which provides verification to the CA prior to issuance of digital certificates, one or multiple directories to hold certificates (with public keys), and a system for managing the certificates. Also included in a PKI are the certificate policies and agreements among parties that document the operating rules, procedural policies, and liabilities of the parties operating within the PKI.

PKCS #11

Public Key Cryptography Standard #11. This standard defines the interface for cryptography operations with hardware tokens.

Private key

The secret part of an asymmetric key pair that is used to create digital signatures and, depending upon the algorithm, to decrypt messages or files encrypted (for confidentiality) with the corresponding public key.

Public key

The public part of an asymmetric key pair that is used to verify signatures created with its corresponding private key. Depending on the algorithm, public keys are also used to encrypt messages or files that can then be decrypted with the corresponding private key.

Public key certificate

A digital document that is issued and digitally signed by the private key of a CA and that binds the name of a subscriber to a public key.

RF

Radio frequency.

RFID

Radio frequency identification

RSA

Refers to public/private key encryption technology that uses an algorithm developed by Ron Rivest, Adi Shamir, and Leonard Adleman and that is owned and licensed by RSA Security.

Sarbanes-Oxley

The Sarbanes-Oxley Act of 2002, which introduced changes to regulations that apply to financial practice and corporate governance for public companies. The Act introduced new rules that were intended "to protect investors by improving the accuracy and reliability of corporate disclosures made pursuant to the securities laws."

Secure Hash Algorithm (SHA)

One of the most popular hashing algorithms, designed for use with the Digital Signature Standard by the National Institute of Standards and Technology (NIST) and the National Security Agency (NSA). SHA-1 produces a 160-bit hash.

Seed

A random sequence of bits that is used in a cryptographic algorithm as the input to generate other, longer pseudo-random bit sequences.

SIM

Subscriber Identity Module. A SIM is the smart card that is included in GSM (Global System for Mobile Communications) mobile phones. SIMs are configured with information essential to authenticating a GSM mobile phone, thus allowing a phone to receive service whenever the phone is within coverage of a suitable network.

Smart card

A device that includes an embedded chip that can be either a microcontroller with internal memory or a memory chip alone. The card connects to a reader with direct physical contact or with a remote contactless electromagnetic interface. With an embedded microcontroller, smart cards have the unique ability to store large amounts of data, carry out their own on-card functions (e.g., encryption and digital signatures) and interact intelligently with a smart card reader. Smart cards are available in a variety of form factors, including plastic cards, SIMs, and USB-based tokens.

Smart ID card

An identification card that is a smart card.

S/MIME

Secure Multipurpose Internet Mail Extensions. A protocol for exchanging digitally signed and/or encrypted mail.

Sniffing

The act of auditing or watching computer network traffic. Hackers may use sniffing programs to capture data that is being communicated on a network (e.g., usernames and passwords).

SSL

Secure Sockets Layer. SSL is a protocol used to transmit information on the Internet in encrypted form. SSL also ensures that the transmitted information is only accessible by the server that was intended to receive the information.

Strong authentication

The use of two or three factors of authentication to prove an individual's identity. Factors would include some combination of something you know (a password or personal identification number that only you know), something you have (a physical item or token in your possession) and something you

are (a unique physical quality or behavior that differentiates you from all other individuals).

Symmetric keys

Keys that are used for symmetric (secret) key cryptography. In a symmetric cryptographic system, the same secret key is used to perform both the cryptographic operation and its inverse (for example to encrypt and decrypt, or to create a message authentication code and to verify the code).

TLS

Transport Layer Security protocol. The TLS protocol provides communications security over the Internet.

Token

A hardware security device that contains a user's identity credentials and the security keys required to use the credential, authenticate the individual, and/or perform secure transactions. This may include the individual's private key(s), public key certificate, and optionally other certificates.

3DES

Triple DES.

USB

Universal Serial Bus.

VPN

Virtual private network.