Open Security Exchange
Best Practices

Guidelines for
Selection and Issuance of Identification Tokens
For Logical and Physical Systems

There are many factors involved in planning for enterprise deployment of **identification tokens** and **credential issuance systems** depending on whether they are used for physical security, logical (IT) access, for specific applications – or to meet multiple business needs. Successful deployment and operation requires selection not only of the appropriate **technology**, but also must include consideration of **organization**, **people** and **processes**.

This document has been developed by the IEEE-ISTO **Open Security Exchange** (OSE) Technical Committee to provide **Best Practice Guidelines** which are intended to educate users in the selection and management of different types of identification tokens (passive, proximity, intelligent, biometric-enabled etc). Specific best practice recommendations are provided for intelligent identification tokens and readers to enable **smart card enabled access control** for both physical and logical systems. This document also highlights relevant standards and their applicability, and the typical operational procedures and roles needed for effective management of the token issuance lifecycle, and integration within existing business processes.

Table of Contents

1 Introduction

1.1 Business Drivers for Use of Identification Tokens

A critical priority for many enterprises today is enhancement of security posture both to reduce risk of system compromise, and also to meet regulatory requirements. One particular area of security investment is authentication based on hardware identification tokens, whether proximity cards or multi-function smart cards, or combination technologies.

Where not already in place, strong authentication based on identification token technology is now being planned and deployed in organizations worldwide both in commercial and government sectors. This can deliver many benefits relating to privacy and accountability for data access and more effective protection against unauthorized access. Credential issuance systems are critical both for successful rollout of identification token solutions, and also for their day-to-day management. However, there are many technology and process complexities that need to be navigated in order to select, deploy and manage these solutions.

1.2 Open Security Exchange

The Open Security Exchange (OSE) is an independent, cross-industry forum that promotes enterprise security management by addressing the lack of integration commonly found in today's security infrastructure. The OSE drives the creation and adoption of interoperability standards by working closely with existing standards bodies. An advisor to government and commercial organizations, the OSE also leverages its combined expertise to educate security professionals worldwide about best practice security.

The OSE is a program of the IEEE-ISTO, which was formed in January 1999 as an independent 501(c)(6) not-profit Corporation. IEEE-ISTO provides both legal and day-to-day support infrastructure for standards related high-tech consortia. IEEE-ISTO is affiliated with the IEEE and the IEEE Standards Association, and has offices located at IEEE Operations Center in Piscataway, NJ. For more information on the OSE, see: http://www.opensecurityexchange.org

OSE is releasing a series of White Papers that will address the need for practical education and guidance on the selection and use of access card technologies with a particular focus on convergence of solutions across logical (IT) and physical systems. The information provided in this document is intended to educate users in the selection and management of Identification Tokens and Credential Issuance Systems. Highlighted are the difference in cards (or tokens), card producing equipment; and the enterprise systems they connect with; and guidance in defining procedures for credential issuance.

1.3 Goals of this Document

The intended audience of this document includes planners and managers of logical and physical access control systems who are responsible for defining standards, technologies, and processes for use of identification tokens within enterprises.

There are multiple card issuance technologies available, and a number of standards which are still maturing, particularly in the area of converged logical and physical access. Many choices are often possible and depending on business needs, IT legacy systems, security requirements, number of sites, costs and number of contractors (among some of the variables) the best solution for a given company may not be a possible solution for another. This document presents most of the important variables, allowing each planner to base their choices on their specific requirements so that they can be informed when comparing vendors and solutions providers.

This document does not recommend one technology over another; it presents the advantages and disadvantages of each option, allowing the planner to choose the best solution according to their needs – including functionality and interoperability. Also, out of scope of this document are specifications for building access systems, evaluation of alternative biometric technologies, security management systems, audit management, operation within a federated identity environment etc. Some of these will be the subject of future OSE best practice guidelines.

1.4 Document Structure

The document is structured as follows

- Sections 3 defines the requirements for identification tokens in physical and logical environments, and makes recommendations for intelligent tokens and readers
- Section 4 provides practical guidelines for selection of physical card types and issuance system, and discusses security best practices
- Section 5 defines organizational processes needed for deployment of tokens
- Section 6 outlines integration with overall enterprise identity management

1.5 Acknowledgements

This document was developed by OSE Technical Committee members:

Dave Hawkins (Technical Committee Vice-Chair)	Software House
Curtis Ide	VistaScape
Dan Monohan	ActivCard
Dan Schliefer	CoreStreet
Dovell Bonnett	HID
Gilles Lisimaque (Document Co-Author)	Gemplus
Gary Klinefelter (Document Co-Author)	Fargo Electronics
Jim Sheahan	Siemens Building Technologies
Piers McMahon (Technical Committee Chair, Editor)	CA
Sal D'Agostino	CoreStreet
Tong Xu	Software House

2 Glossary and References

2.1 Acronyms

AAMVA	American Association of Motor Vehicle Administrators
AES	Advanced Encryption Standard
CCEAL4	see EAL4
CENELEC	European Committee for Electrotechnical Standardization
COTS	Commercial Off-the-shelf
CSN	Card Serial Number
EAL4	Evaluated Assurance Level 4 (under Common Criteria)
ECC	Elliptic Curve Cryptography
EU	European Union
GSC-IS	Government Smart Card – Interoperability Specification
ICC	Integrated Circuit Card
ID	Identification
IEC	International Electro-technical Commission
INCITS	International Committee for Information Technology Standards
HIPAA	Health Insurance Portability and Accountability Act
HR	Human Resources
IP65	Ingress Protection
ISO	International Standards Organization
LED	Light Emitting Diode
LRA	Local Registration Authority
MOC	Match on Card
NEMA	National Electrical Manufacturers Association
OASIS	Organization for the Advancement of Structured Information Standards
PET	Polyethyleneterephthalate
PIN	Personal Identification Number
PK	Public Key
PVC	Polyvinyl chloride
RFID	Radio Frequency Identification
RIF	Reduction in force
SAML	Security Assertions Mark-up Language
SIA	Security Industry Association
SPML	Service Provisioning Markup Language

2.2 Terms and Definitions

Authentication – Technology and a process of determining an asserted identity with a specified or understood level of confidence.

Card Durability – Durability refers to the ability of cards to stand up to common wear threats such as sunlight, water, heat, mechanical stress, and chemicals.

Card Serial Number – Smart cards have a unique identification number written during the manufacturing process that cannot be altered later. This number allows tracking of the card during its whole life for security purpose as well as quality control.

Card Technology – Technology refers to the additions to a plastic card to enable their use in Access Control and Logical Access Systems.

Contact Smart Card – Contact Smart Cards are credit card sized tokens that use electrical contacts to connect to an integral microprocessor. The token communicates using electrical contacts to an interface device (or reader) compliant with ISO/IEC 7816. The integral microprocessor provides many application options for managing data and security in conjunction with a host application.

Contactless Smart Card – Credit Card size token using a radio frequency technology to communicate with a contactless reader.

Digital Signature – Using a private or secret key to cipher the hash result of a piece of information provides a digital signature attached to the information. It enables verification that information has not been altered and was issued by the correct authority.

Hash Algorithm – These one way mathematical functions produce a string of bits shorter than an initial message they represent. Changing one bit in the initial message completely changes the hash result.

Dye-sublimation Printing – Dye-sublimation printing is a thermal printing process that uses a multi-panel ribbon to produce color images. The most common ribbon for printing on cards is a 5 panel ribbon containing yellow, magenta, and cyan dye panels along with resin black and resin overlay panels. The resin black panel is used to print text and barcodes darker than can be printed with dyes. The overlay panel is used to increase durability. A print head that is the width of an entire card thermally images each pixel line of a card by transferring dye or resin from the ribbon to the card.

ID1 (7810) Form Factor – This refers to an ISO ID1 identification card piece of plastic (as defined in ISO/IEC 7810). The card is 85.6mm x 53.98mm x 0.76mm and is the same as the ubiquitous bank card with its magnetic stripe that is used as the payment instrument for numerous financial schemes

Identification Card – A credit card sized card which is used to identify an individual within an organization - e.g. with a picture, name, and employee id printed on the card. An identification card may also be an *identification token* that can be used for access control to physical and logical security systems.

Identification Token – A hardware token used to authenticate a user to a reader for IT or physical access. An identification token may be credit card sized, or key fob, or other design. A token may be a proximity card, vicinity card, magnetic stripe card, smart card, or other type of technology.

Junk stripe - thin line stripe on the back of a magnetic card that allows information to be placed on it for an off-line application

IP65 – IEC-defined standard for protection in an outdoor environment. Each IEC IP number corresponds to a NEMA-defined enclosure type.

Logical Security – Security for IT systems and applications

Magnetic Stripe Card – This card includes a magnetic stripe much like a credit card, but the stripe is encoded with numbers that provide physical access to a building or logical access to computer systems.

Overlaminate – Overlaminate refers to a clear protective layer that is added to a card for additional security and durability. Overlaminates may include holograms or other security layers.

Print Technology – Technology refers to the method of printing like: Inkjet, Thermal Transfer, Offset Printing Press, etc.

Proximity "Prox" Card – This card includes technology to transmit a number to an Access Control System. In simple implementations the number is limited and fixed.

Relying Party - A recipient who acts in reliance on a certificate and digital signature

Wiegand – This card includes technology to transmit a number to an Access Control System. In simple implementations the number is limited and fixed.

2.3 Standards

- ISO/IEC 7810 : Identification Cards – Physical Characteristics
- ISO/IEC 7811 : Identification Cards – Recording techniques
- ISO/IEC 7812 : Identification Cards – Identification of issuers
- ISO/IEC 7813 : Identification Cards – Financial transaction cards
- ISO/IEC 7816 : Identification Cards – Contact Integrated Circuit(s) Cards
- ISO/IEC 14443 : Identification Cards – Contactless Integrated Circuit(s) Cards – Proximity Cards
- ISO/IEC 15693 : Identification Cards – Contactless Integrated Circuit(s) Cards – Vicinity Cards
- ANSI/INCITS 322:2002 : Card Durability Test Methods
- Technical Implementation Guidance - Smart Card Enabled Physical Access Control Systems – Final Version 1.0, dated 2 July 2003
- "Personal Identification – AAMVA International Specification – DL/ID Card Design" - http://www.aamva.org/.
- SIA AC-01 (1996.10) Access Control Standard - Wiegand™ Card Reader Interface.
- UL-294 : Performance standard that governs the design, construction, performance, installation and operation of access control systems hardware

2.4 Industry Specifications

- Global Platform - http://www.globalplatform.org
- JavaCard 2.1.1 - http://www.javacardforum.org
- PKCS #11 - www.rsasecurity.com/rsalabs/pkcs/pkcs-11
- MS-CAPI - http://msdn.microsoft.com/library/en-us/dncapi/html/msdn_cryptapi.asp

2.5 Government Specifications

- Technical Implementation Guidance - Smart Card Enabled Physical Access Control Systems – Final Version 1.0, dated 2 July 2003
- Department of Interior, Bureau of Land Management, SRS titled *"Requirements Specification for Access Monitoring and Control"* Version 1.0, dated February 2003.
- SEIWG-012 Specification, "*Code IDENT 50464"*, dated 28 February 1994.
- NIST Internal Report 6887, Government Smart Card Interoperability Specification, version 2.1 dated July 2003
- AAMVA White Paper on Over-the-Counter, Central and Hybrid Issuing Systems
- AAMVA Internal Controls Driver Licensing and Identification Processing Best Practices
- AAMVA Personal Identification – AAMVA International Specification – DL/ID Card Design
- HMG's Minimum Requirements for the Verification of the Identity of Individuals - www.e-envoy.gov.uk/assetRoot/04/00/08/52/04000852.pdf
- Common Criteria : Common Criteria for IT Security Evaluation - http://csrc.nist.gov/cc/index.html

2.6 White papers and other documents

- Smart Card Alliance, *"Contactless Technology for Secure Physical Access: Technology and Standards Choices"*, October 2002.
- A Study by the Security Equipment Integration Working Group (SEIWG), *"Development of a specification for the SEIWG-compliant Access Control Components",* dated 30 September 2002.
- A Study by the Security Equipment Integration Working Group (SEIWG), *"Access Control Technologies for the Common Access Card"*, April 2002.

3 Access Control Requirements for Identification Tokens

This section defines the requirements for identification cards based on an analysis of requirements for physical and logical access control.

3.1 User Access Control

Table 1 introduces the main concepts of user access control, using the example of a passport:

Access Control Concept	Generic Meaning	Passport Example
Identity	Your unique attributes	Name, face, date of birth
Authentication	Proving your identity	Picture on passport
Authorization	Process of granting privileges	Privilege to enter a country
Credentials	*Evidence* of relationship or privileges	Passport shows residency, visa shows privilege
Validation	Verifying credentials are in good standing	Has the passport or visa been revoked?

Table 1 – Access Control Concepts

These concepts will be found in any access control architecture whether these concern building access, or controlled entry to computer systems.

In general, access control is broken down into two steps: authentication and authorization

(1) Authentication : "Are you who you say you are?"

There are many options for authenticating. These include:

- One time password generators
- Biometrics
- PINs, passwords
- Magnetic stripe cards
- Proximity cards
- Intelligent Identification tokens, e.g. smart cards

The trade-offs between selecting one technology versus another depend on the level of security required. In some cases, enterprises may choose to have multiple authentication mechanisms, and require more stringent forms of authentication for remote users or for highly privileged users. Identification token technology may be chosen in order to enable the authentication mechanism to also be used for physical access, or to support other business applications.

The important characteristic is that user authentication is based on long lived data that should have the following characteristics:

- Infrequently changed
- Can handle different types of credentials without making any locale-specific assumptions
- Optionally, can be evaluated without a server (to enable off-line operation)

Personal information used to support authentication is typically relatively long lived and once established will rarely be updated (except for life changes). Other items like PINs and passwords should be modified based on the frequency of the corporate policy (e.g. once every 4 weeks) – and will therefore be forgotten by the user. The architecture should make sure that authentication information is not accessible by unauthorized insiders or via outside connection. Authentication information should be protected using hardware security modules or appropriate controls based on a risk assessment. Personal information maintained on an identification token or used for verification of identity, should match the information in the HR system and could be established via this route during the credential issuance process – as discussed in Section 6 below.

When an **identification token** is used for authentication, then the verification of a user being the legitimate owner of a token can be based on:

i. What they have (being in possession of the token)
ii. What they know (presenting the correct password or PIN)
iii. Who they are (biometric verification)

or some combinations of the above.

The user's credential comprises the identification token itself and the data that the credential issuance system sets up on the card.

The method of authentication with an identification token is dependent on the security level associated with the particular relying party. In the case where high security is required, then secure credentials are essential (difficult to copy, cannot be changed) and then there may be a need for multiple identification factors. Lowest security uses (i) above, higher security (i) plus (ii) and the most secure is having the three (i, ii and iii)

(2) Authorization : "Are you allowed to do something"

These permissions are typically set by administrators for network, system, application, file, and other resources. These permissions may be revoked, suspended or changed. Authorization information changes over time, and may be administered centrally or by the owner of each resource.

Logical access approaches can support different levels of security (discretionary, label-based, mandatory etc) and different segregation mechanisms (operating system controls, encryption etc).

A part of authorization is validation: **"Are you currently allowed to do what you are trying to do?"** This is the process of checking authorization at the time of a transaction. It needs to be real-time and may be off-line, or on-line, or a combination of both (e.g. certificate expiry and revocation checks).

The remainder of this section discusses the physical and logical scenarios for use of identification tokens, and provides best practice recommendations for intelligent identification tokens that can meet these requirements.

3.2 Physical Access Control

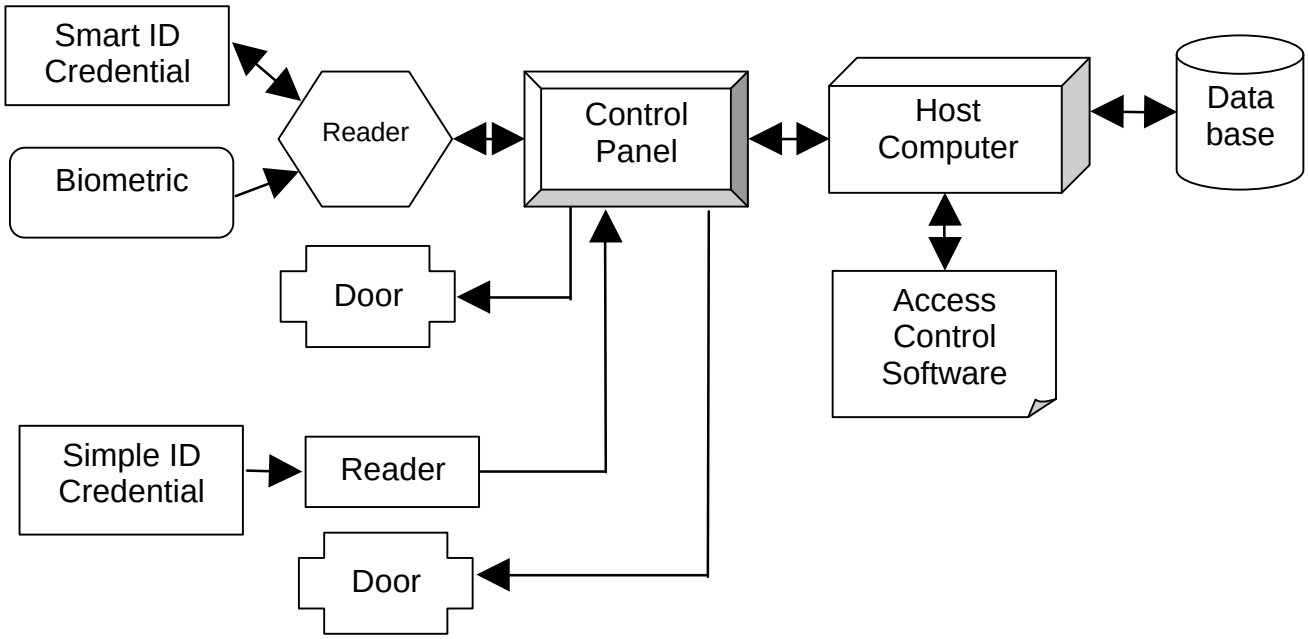

Figure 1 – Physical Access Control Architecture

Figure 1 represents the two main possible architectures for a physical access control system depending on two factors: the intelligence of the token and the use of biometric authentication mechanisms.

Most access control systems today use simple passive identification tokens ("Simple ID Credentials" shown on the bottom left of the diagram). These tokens store a unique number and are available in various proprietary solutions based on technologies such as magnetic-stripe, bar code (one or two dimensions), optical stripes, as well as RF devices with a frequency of 125 kHz or 13.5 MHz. Some more recent tokens also use interfaces based on either ISO/IEC 14443 or ISO/IEC 15693 contactless standards. The token information is only read by the reader and transmitted to the controller which, in turn, will

open the door (after the host computer has given the authorization). No information is written back to the token.[1]

With the development of radio frequency (RF) technologies, it has become possible to interact securely with newer "smart tokens", enabling them to support a challenge-response exchange (as part of authentication) or updates to their content. Use of such a smart token is also shown in Figure 1 ("Smart ID Credentials" in the diagram in the upper left corner). Besides just storing a unique identifier on the token, smart tokens support active authentication whereby a challenge response takes place between the token and the back-end system. This increases the level of security for applications where there is a risk of token cloning. The ability to update token memory (but never its unique identifier), also enables information to be stored in the token itself. This makes it possible to have off-line decisions when the host system is not available (when two sites are physically disconnected).

3.3 User Authentication

The use of a password (or PIN code) as well as biometric verification requires readers at the access point that can accept numbers from a keypad or characters from a keyboard. More sophisticated devices have to capability to obtain biometric information from the user.

PIN and Passwords:

The token itself, the controller, or the host computer may verify the pin or password with the back end system. For PIN and passwords, many intelligent tokens are able to do such verification. To protect against password guessing attacks, they can lock themselves after a certain number of invalid authentication attempts, and then need to be reset by an authorized administrator (e.g. security officer). Alternatively, a host computer in the back end system may perform PIN/password verification in case the token is not intelligent enough to do so. Whatever design is chosen, it is important to keep in mind many users can and will forget their password, will enter it incorrectly, and lock out their token – and then will require assistance to unlock the token (or the password in the back end system). Whatever solution is chosen, the procedure (easy but secure) to unlock the password should never be underestimated during the design phase of the system.

Biometric Verification:

Many biometric technologies are available, and the choice of which one to adopt depends on the application, interpretation of regulatory requirements, and overall system and budgetary constraints. Two basic design options are available for such a system: to store the user's reference template in the database of the back end system, or to store it on the intelligent token. In both cases a biometric device is required at the point of verification.

This biometric reader is used to obtain the live biometric information of the user that is to be tested against the reference template of the legitimate user of the token. The verification between these two templates can be done:

[1] Physical access systems using smart cards may use the Card Serial Number (CSN) of the smart card as the physical token unique identification for access control systems. This allows a physical system to use a smart card issued for other purposes without having to create its own application number in the smart card.

- In the biometric reader itself – this needs the reference template to be securely transmitted,
- In the smart token - biometric verification can involve quite complex calculations and many tokens are not able today to do such verifications,
- In the controller or in the host computer

Such biometric systems require the biometric software and data to be split between two or more locations or devices. As many of these biometric techniques involve proprietary techniques to improve speed and accuracy, caution need to be taken if interoperability between systems is a requirement.

The document does not make recommendations for biometric techniques or readers.

3.4 Information stored on the token

Table 2 below summarizes the information stored on tokens, together with the associated security threat that this information is used to counter:

Information Stored on Identification Token	***Threat Countered***
Token unique identification number: Mandatory - Allows each token to be associated with a given user (for example in a back-end database or directory). In order to be "active" the token number needs to be loaded and activated in the database. This is handled during the issuance lifecycle (see section 6)	*Unauthorized tokens will be detected as they lack valid identification numbers, or collide with another token*
Active Token Authentication: Optional – Requires a more complex key management in the tokens as well as in the rest of the system (host if online, controller if semi-offline). This prevents information stored in the tokens being used without the physical token itself. It also prevents any kind of replay attacks between the token and the reader.	*A forged token is made harder to achieve as it needs knowledge of secrets of an original token to emulate correct behavior.*
User related information: Optional – On intelligent tokens, information related to the user can be stored securely on the token. User information such as biometric data or template, digital picture, personal information (name, title, address, etc.) can be stored on the token and used by various devices for access control or other functions	*False user claims of attributes and entitlements are prevented as the information is protected by the card*
Passive Token information signature: Optional – Used when the token contains information in addition to the Unique Identification Number user information (Identity, Biometry, etc.). Information stored on the token (even if not updated) enables off-line functioning, e.g. for mobile users. This technique used alone does not prevent against cloning – as signatures can be copied.	*Information tampering is prevented as information must be signed using a public key mechanism from a recognized authority*
User verification by the token: Optional – Before releasing its information, some tokens can ask their legitimate user to prove who they are by showing their knowledge of a password for example. In intelligent tokens, the password is stored on the token itself and locked after too many consecutive authentication	*Stolen tokens used by unauthorized users are useless without a combination of something possessed*

failures. This requires the reader to have a keyboard entry or at least a numeric keypad. If a password is required and the token is not intelligent, it is also possible to verify the user password by involving the back end system.	*(the token), AND something known (the password)*

Table 2 – Identification Token Information

3.5 Intelligent Tokens - Best Practice Recommendations for Physical Access Control

The following gives a list of best practice recommendations for use when specifying standards-based intelligent tokens:

a. The contactless interface access cards shall be used with access readers to gain entry to access controlled portals (such as doors, gates and turnstiles) and to hold information specific to the user.

b. The card may have more than one technology but must have at least the following
   i. The card shall meet the following standards for contactless smart cards: ISO/IEC 14443 Part 1, 2, 3 and 4.
   ii. The card shall meet ISO/IEC 7810 specifications for length, width, thickness, flatness, card construction and durability, and shall be in a form suitable for direct, two-sided dye-sublimation or thermal transfer printing on the specified badge printer.
   iii. Unique 64-bit, fixed card serial number, used for anti-collision and key diversification
   iv. The card shall support read/write capability, with two or more Application Areas to support future applications. Data retention shall be 10 years, nominal. Wiegand compatible card data up to 144 bits in length shall be factory programmed in at least one application area for use with access control systems.
   v. Application Areas on the card shall be secured with a unique diversified key (DES or better), such that data stored in that area cannot be modified by an unauthorized party.
   vi. When a system requires the card and the reader to go through a mutual authentication process, critical information on the card shall not be accessible by any reader until the correct mutual authentication is performed.
   vii. The integrity of the card data structure as well as the integrity of individual data elements stored in the card shall be maintained by the card, even if the card is removed from the RF field during a write or update operation.
   viii. The card shall be capable of accepting a slot punch on one end, allowing it to be hung from a strap/clip in a vertical orientation.

[Note that other physical access control solutions are possible based on passive tokens, or proprietary mechanisms – in which case these recommendations may not apply.]

3.6 Readers Using Intelligent Tokens - Best Practice Recommendations for Physical Access Control

The following makes a recommendation for readers using intelligent tokens – assuming that ISO/IEC 14443 or ISO/IEC 15693 RF tokens are used.

Card readers shall use contactless technology and be "single-package" type, combining controller, electronics and antenna in one package, in the following configurations:

a. Provide “single-gang” mounting style contactless smart card readers for wall mounting, vehicle stanchions and pedestals.
b. The reader shall be of potted, polycarbonate material, sealed to a NEMA rating of 4X (IP65).
c. The reader shall contain an integral magnet for use with an external magnetic reed switch to provide tamper protection when connected to an external alarm system.
d. The reader shall be UL/C 294 listed, and shall be FCC and CE certified, and shall conform to one or both the following ISO Standards:
    i. ISO/IEC 14443 Parts 1, 2, 3 and 4
        1. shall be able to accommodate Type A as well as Type B cards.
        2. do not need to comply with the anti-collision requirement of ISO/IEC 14443, but must reject multiple card presentations
    ii. ISO/IEC 15693 Parts 1, 2 and 3
e. Transmit Frequency — 13.56 MHZ
f. The reader shall require that a card, once read, must be removed from the RF field for one second before it will be read again, to prevent multiple reads from a single card presentation and anti-pass-back errors.
g. The reader shall be capable of reading access control data and transmit that data in SIA standard Wiegand format.
h. The reader shall have a Wiegand output and shall operate under internal control for read-only Access Control Applications(*).
i. The reader shall have multiple LEDs (e.g. green, red) for increased visibility.
j. The reader shall have separate terminal control points for green and red LEDs, and for the audible indicator.
k. The reader shall have an audio transducer capable of providing unique tone sequences for various status conditions.
l. The reader shall have a configurable hold input, which when asserted shall either buffer a single card read or disable the reader, until the line is released. This input may be used for special applications or with loop detectors.
m. If card and reader mutual authentication is required: Security keys in the cards and readers shall be required to match and may be customized for individual sites.

n. The reader shall have flash memory to allow future feature enhancements to be added in the field.

* Alternative acceptable reader configurations:

1. Some Access Control applications may require additional levels of security requiring for example a PIN to be presented. To achieve this, a reader as stated above can be used with an integrated keypad. In case biometric verification is required the token reader and the biometric device shall be tightly integrated to prevent tampering with connections between them.
2. For read and/or read/write applications for connection to PCs or dedicated microcontrollers, a reader as stated above can be used with an RS232 or USB Port.

[Note that if other technologies than ISO/IEC 14443 or ISO/IEC 15693 RF tokens are used, the above recommendations may not apply]

3.7 Logical Access Control Architecture

Figure 2 below shows a simplified view of an intelligent token being used to access IT resources held on a remote system. The user authenticates with a "Smart ID credential", and mutually authenticates with a remote system whose keying material is protected with a Hardware Security Module (HSM).

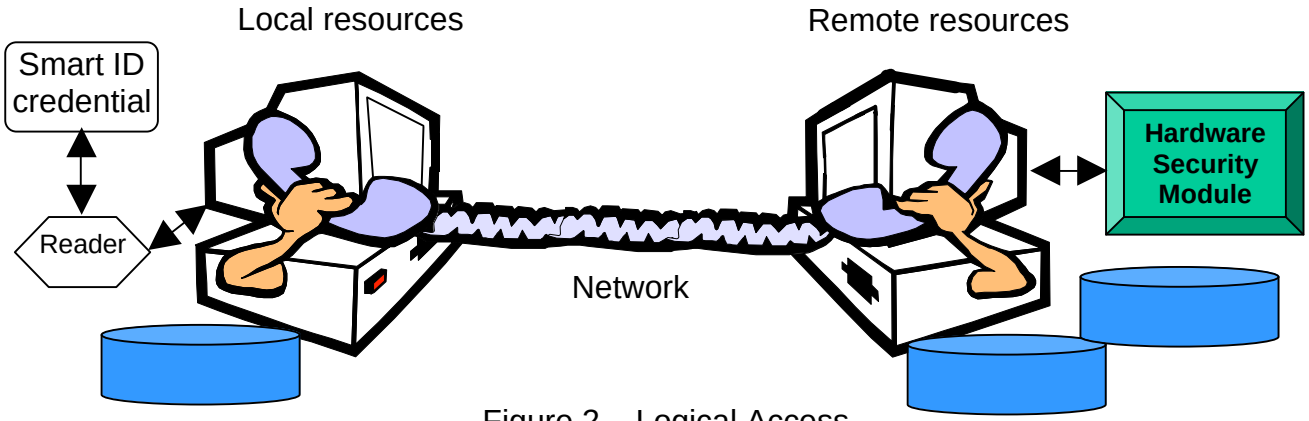

Figure 2 – Logical Access

An enterprise logical access control architecture may have a number of additional tiers, which can include:

- Public Key Infrastructure (PKI) components for certificate issuance, directorys for certificates and CRLs, trust path validation, revocation etc
- LAN authentication – which grants access to corporate network file and print servers etc based on token authentication

- Authentication, Authorization, and Accounting (AAA) servers – which control network access based on access profiles
- Security Policy Servers – which can provide identity mapping, sign-on to other applications, handle, entitlements management, and broker trust relationships with external organizations
- Application-level security – which may have additional security requirements

There are a number of ways of architecting the functionality required to achieve logical access control. In many cases this is determined by the particular application requirements. Some of these requirements include:

- Number of users
- Number of locations
- Number of applications requiring access control.

These requirements will determine the manageability and scalability needs of the solution. This section does not define a single IT security architecture but focuses on how different logical access control architectures can be supported by identification tokens.

The remainder of this section discusses the requirements on the identification token arising from support for logical access control.

3.8 Intelligent Tokens - Best Practice Recommendations for Logical Access Control

In logical access control applications (e.g. access to networks), the reader is attached to the computer or work station that the user will operate to access to local and remote resources after they have been authenticated. Unlike in most physical access control applications for which a reader (attached to a door for example) is shared by many tokens granting access through the door, logical access control systems therefore have nearly as many readers as tokens in use. As a consequence the cost of the reader become quite important and when intelligent tokens are being used, this favors contact smart card technology for which the reader is about a tenth in cost of the contactless smart card technology.

Another reason for contactless technology not being the primary choice for logical access control systems has to do with the performance of existing contactless smart card technologies when related to public key cryptography. Contactless technology is most often used for fast interactions – and isn't optimized for complex high secure cryptographic exchanges between a smart card and the Hardware Security Module (HSM)

The following best practice recommendations assume the token is using ISO/IEC 7816 (contact) technology:

a. The contact interface of the access cards shall be used with smart card readers connected to computers to gain access to the computers, applications and/or networks they are connected to.
b. The access card holds information specific to the user and must identify its user by the use of a Password or Pass-phrase, or biometric technology.

c. The card may have more than one technology and multiple applications, but must at least have the following:
    i. The card shall meet the following standards for contact smart cards: ISO 7816 Parts 1, 2, 3, 4, 5, 8, 9, and 15 (Parts 6, 7 and 11 are optional).
    ii. The card shall meet ISO/IEC 7810 specifications for length, width, thickness, flatness, card construction and durability, and shall be in a form suitable for direct, two-sided dye-sublimation or thermal transfer printing on the specified badge printer.
    iii. Unique 64-bit, fixed card serial number, used for traceability and key diversification
    iv. The card shall support read/write/update capability, and be able to have up to 16 Applications. Data retention shall be 10 years, nominal. One of the applications shall contain the Wiegand data for use with access control systems.
    v. Each Application on the card shall be secured for load/activation/instantiation according to the Global Platform specification and be protected during use by the security rules defined by the application (Password, Authentication, etc.)
    vi. The integrity of the card data structure as well as the integrity of individual data elements shall be maintained by the card, even if the card is removed from the reader during a write or update operation.
    vii. The card shall be capable of accepting a slot punch on one end, allowing it to be hung from a strap/clip in a vertical orientation.

[Note that if contactless cards or other technologies are used for logical access control, then the above recommendations may not apply]

3.9 Multi-Technology Identification Tokens

Multiple technology cards may have, in addition to the contact and contactless interfaces described earlier, one or more of the following technology:

- 125 kHz Proximity Chip and antenna
- Magnetic Stripe
- Bar code
- 2D bar code
- ISO/IEC 15693 Vicinity contactless interface
- Optical storage

In general, the use of multi-technologies on the same card eases the migration path from an existing system to a new one, but is not recommended to use more than two technologies on the same token as a choice for new systems. Where many technologies are used on the same card, then the higher the risk of one technology failing will require the replacement of the whole card.

3.10 Passive Technologies

3.10.1 Printing

In addition to their use in conjunction with contact or contactless readers for automated access, ID badges are often used as a visible identification for individuals. Many security features have been developed over the years such as holograms, variable optical inks, microprints, etc. These features have the benefit that they allow a security guard to verify by inspection whether a given person should be in a given area. However, printing on a plastic card which contains integrated chips (contact smart cards as well as contactless smart cards) can sometime cause unexpected challenges. Special precautions have to be taken when on-site issuance of printed smart cards is planned. The compatibility of the selected card printing/issuing equipment should be verified to insure that it accepts the card technology that is planned for enterprise deployment.

3.10.2 Bar Code

Bar codes are used to provide easy automatic reading of small numbers (in the tens of digits) such as serial numbers or user identification numbers. This number appears on the plastic of the card, and is engraved or printed either at the manufacturing site or at the time of credential issuance.

3.10.3 2-D Bar Code

Two-dimensional bar codes allow coding up to two thousand bytes but require some space on the surface of the plastic and a rather smooth surface for printing.

3.10.4 Magnetic Stripes

Different type of magnetic stripes can be used on plastic cards. ISO/IEC 7811 defines the various options for encoding interoperable magnetic stripe information. Depending on the density and coding used, it is possible to store between a hundred and fifteen hundred bytes. Some systems use “junk stripes” which have proprietary encoding and location fields.

3.10.5 Optical Stripes

Similar to CD laser engraving technology, optical encoding on ISO/IEC 7810 ID1 card is used when a very high quantity of information has to be stored on a plastic card. This technology was initially intended for portable personal medical records and offers the capability to store between one and six mega-bytes of information, and is used today by the US and Canadian immigration services. The high price of the readers limits this technology to applications where a given reader is used by tens of thousands of cards.

3.10.6 Read-Only RF tokens

The tokens are a simplified version of proximity tokens - but they use the same technologies as other proximity or vicinity tokens. Read-only RF tokens provide an easy way to read a number from the card quickly and conveniently. As their name indicates, no information is written back in the card and the card is not capable of being challenged by a reader (i.e. active authentication can’t be supported).

3.11 Active Technologies

3.11.1 Contact Circuit Cards

Contact circuit cards are used in applications such as financial payment, cellular digital phones, logical access control to networks as well as health care insurances, or student identification. A secure electronic component able to store program and data up to 200 kilobytes is embedded in the plastic of the card, and is used to execute complex cryptographic algorithms that can authenticate the user as well as the application computers interacting with the applications in the card. The smart card acts as a portable computing device, and is able to protect the confidentiality of the information it carries and encrypt it during an exchange with another computer. Considered today as the most secure device using an ID1 7810 form factor, these tokens are tamper resistant but not tamperproof. Many commercial products are today certified as FIPS 140 level 2 compliant as well as assured to EAL4 under the Common Criteria.

3.11.2 Contactless Circuit Cards

Used mainly in physical access control, payment for transportation or small financial transactions (Electronic purse) there are a large variety of technologies in this category. Most existing proprietary existing systems use the older 125 Khz frequency but they do not offer interoperability. RFID tags, proximity and vicinity ISO compliant products all use the same 13.5 Mhz frequency. However, differences in the protocols and the use of option bits in the chips do not always guarantee a given ISO compliant card will work in any other's vendor reader. The industry is currently working on eliminating these differences but enterprises should carefully validate specific interoperability needed to meet their requirements rather than assume it.

3.11.3 Hybrid Circuit Cards

When the same card is used in a physical access control system (which favors contactless technology) and in a logical access control system (which favors contact technology), it is quite easy to have both technologies in the same plastic card. The two different chips (contact and contactless) are distinct in the plastic of the card and have no connection at all. The chips are separated, so for the most part they have no common command formats, security feature and very different memory structure and management. Hence card information needs to be synchronized.

3.11.4 Dual Interface Circuit Cards

Many integrated components used for contact cards are now able to have a dual interface and communicate with a reader using either a contact connection or a contactless (RF) connection. These chips are starting to appear on the market and represent state of the art in technology, and have very high security standards (as contact smart cards) and in general have similar behavior on either communication interface (contact or RF). The same memory information, application program or security algorithms can be used on either interface. As only one chip is in the card, the risk of information being out of synchronization between the different applications is eliminated.

4 Selecting Identification Tokens and Credential Issuance Systems

4.1 Selecting Token Type and Design

In the majority of installations for physical and logical security, an individual gains access using an identification token the size of a credit card. But identification card requirements are not the same for all organizations. Environmental and security factors influence the choice of card materials to be used and how the cards should be carried – e.g. a business that requires their card holders to swipe their cards through a magnetic stripe reader may want to replace this with a more durable card so that the photo or any information on the opposite side of the magnetic stripe does not get damaged over time. Some organizations may need multiple cards designed for a variety of security levels and to integrate with access systems that are already in place. Intelligent identification tokens can be used to simplify the overall system and provide a high level of security.

4.1.1 Card Types and Durability

Table 2 lists some common types of identification cards and the durability considerations for each. Offset Printing Press printed cards may be more fade-resistant than dye-sublimation cards, but may have lower scratch resistance unless they are laminated.

Durability Level / **Card Type**	**Low**	**Medium**	**High**
Inkjet Card	Cards may fade in sunlight, smear in liquid, or break when laminated		
PVC Card		Cards may fade in sunlight or wear through from abrasion	
Composite Card			Very durable card stock, printing should be laminated for best durability of printed image
Laminated Card			Lamination can be applied to any card using the right adhesive to improve scratch resistance and image

			fading due to UV degradation and dye migration.

Table 2 - Card Types and Durability

The International Committee for Information Technology Standards INCITS has produced a document 322 that sets standards for card testing. INCITS has also started a working paper B10.3 03-016 "Card Durability / Service Life". Understanding card durability and applying the practices recommended in these standards can prevent cards from wearing out prematurely.

4.1.2 Card Environment and Durability

The environment in which a card is used is important to its longevity. Adverse conditions can be detrimental to any card. For example, even credit cards delaminate under harsh conditions of wallet pressure, heat and humidity. Understanding the tradeoffs in the various kinds of environments against the types of card constructions available will help optimize the selection of cards.

The factors to consider are summarized in Table 3 below.

Durability Influence **Card Environment**	**Low**	**Medium**	**High**
Indoor	Most card and print technologies will work satisfactorily		
Indoor/Outdoor		Sunlight and water should be considered	
Outdoor			Water, Sunlight, and Pollution can all affect card life
Card Swipe			May need protection against swipe abrasion

Contact Chip Reading		Abrasion on contact smart cards between the contacts and the edge may be a card design consideration.	

Table 3 - Card Environmental and Durability

4.1.3 Identification Token Technologies and Security

The required level of token security and resistant to threats can vary widely by organization. For example, banks have legal and fiduciary responsibilities to maintain security of financial information; police departments have personnel-related security concerns; corporations may be trying to guard trade secrets, or ensure the safety of their employees. There are a variety of card technologies and security features that can help each organization meet its security needs.

Ideally, a single identification token technology is desired to provide all of an organizations needs. When a card contains multiple technologies or the user has multiple cards, there is more opportunity for user difficulties and errors in card issuance – which result in additional cost for the card issuer. Contactless smart cards can be used to handle access control and computer security in a single technology – however as discussed in Section 3.8, this needs to be balanced with the need to handle computationally expensive cryptographic operations, which may favor contact smart cards.

As discussed in section 3.9, 3.10, and 3.11, there are many other options that combine barcodes, proximity, magnetic stripe and smart chips on a single card to cover multiple applications to handle legacy systems.

Most of the time, the use of multi-technologies on the same card eases the migration path from an existing system to a new one, but is not recommended as a choice for new systems. Complex cards may also be less durable.

Security Level **Card Technology**	**Low**	**Medium**	**High**
Magnetic Stripe	Limited data encoded on card. Easy to forge		

Proximity Card		Number embedded in card. Hard to forge	
Smart Card (Contact)			Data embedded in card and protected cryptographically
Smart Card (Contactless)			Data embedded in card and protected cryptographically

Table 4 - Card Technologies and Security

4.1.4 Card Security Features

As discussed in 3.10.1, in some organizations, the card that provides logical access to computer systems or physical access to facilities is also used for identification. The card may be required to have additional security features. For instance, a card may be laminated with a hologram that can be used for authentication. By combining visible and covert security features into one card, it can serve both as an access key and identification card.

Here are a few guidelines for implementation:

- Use a security feature in the form of a hologram to reduce the risk of forgery.
- Keep identity photos up-to-date. Renew card periodically.
- Make names and organizations clearly visible and easily read.
- Authorize the use of company resources (e.g. being on site outside normal working hours, borrowing of company documents, computer access) via the identification card.

Visible security features improve security by making it easier to instantly identify if a card is valid and if it's authenticated to the cardholder. Visible security features can include photos, logos, designs, background colors, holograms or hot stamp foils. Covert features heighten security with technology that may require special equipment to authenticate, thereby discouraging potential counterfeiters. Covert features can include encrypted data, micro text, ultraviolet inks and digital watermarks.

Cryptographic security is an important companion to visual security. Some card technologies like barcodes and magnetic stripes are easier to counterfeit than smart chips. Identity security measures like photos are harder to alter if they are laminated to a hologram. A combination of features provides the best security. For example, a Contactless Smart Card with a picture under a hologram and a fingerprint stored in the smart card IC should be very secure. In this case the card can be identified as belong to the cardholder, the card is an electronic key, and the key can be verified as belonging to the cardholder with the fingerprint.

The American Association of Motor Vehicle Administrators (AAMVA) has provided a complete list of security features in its "Personal Identification – AAMVA International Specification – DL/ID Card Design". Their web site can be found at http://www.aamva.org/.

4.1.5 Card Design and Application

Most card technologies are combinations of PVC and PET. PVC material is durable, flexible, and accepts direct imaging from dye-sublimation printers. The PVC material can be manufactured for a glossy or matte finish. Matte finish is not recommended for dye-sublimation unless a reverse transfer printer is used. Inkjet coated PVC cards are just starting to emerge on the market.

Cards should be handled with care to avoid contact with dust, dirt, lint, oils, and fingerprints. If possible wear thin cotton gloves, surgical gloves, or finger cots while handling the cards prior to imaging. Otherwise handle cards by the edges, as with a photograph or record. Mishandling the thin cards prior to imaging could result in unsatisfactory print quality.

It is generally best to avoid areas on the card like card edges, smart chip contacts, embedded antennas, and embedded chips. Slot punching if desired should be done after printing for best results. The exception to this is when reverse image printing is used. In which case, most of these areas will be printed properly when the image is transferred to the card.

Multiple graphics designs should be considered for visual security. Determining cardholder status by viewing badge graphics can add to an organizations security.

4.2 Selecting a Credential Issuance System

Selecting a card issuing system depends on many factors. For example:

- What type of card readers are being used
- What type of printing is required
- What type of computer infrastructure is implemented
- What resources are available
- What level of security is required to protect the inventory of cards
- What level of security required to protect the transfer of users' personal information as well as the cryptographic keys used to certify the cardholder data

These factors and more influence how the credentials, cards, and issuing systems will be configured. For instance, a lack of resources or computer infrastructure may mean credential issuance has to be done outside of an organization. There are a variety of desktop card printing systems available. For instance, thin cards can be printed on a low cost inkjet printer and then laminated for higher durability. A more expensive desktop dye-sublimation printer can not only print, but also encode, a smart card with an option for adding a holographic lamination for security and durability.

4.2.1 Matching the Issuance System to Card Type and Application

Card type and design are important selections along with the system in which the cards are used. Once these selections are made, selecting a card issuing system becomes easier. The card issuing system includes both printing and encoding of the card. Choosing the right card issuing system can avoid problems in cards associated with:

- Irregular card surface due to embedded antennas and chips
- Too many card technologies on a single card
- Dirty cards

Proper distribution and activation of cards will vary by organization. Certainly in the case of credit cards, there is a very strict process to centrally issue, mail, and then activate cards. For credit cards, ISO/IEC 7812 and ISO/IEC 7813 define registration and encoding standards. AAMVA set guidelines for issuing cards in the document “White Paper on Over-The-Counter, Central and Hybrid Issuing”. Considerations such as systems access, location of cardholders, security level, and card technology can influence card-issuing selection. If an organization has multiple facility locations, they will have to decide whether to have multiple issuing sites. Distributing issuance is flexible and easy for cardholders, but the security level of the organization may dictate a single issuance site for security reasons. The most secure is to have the cards fully personalized before distributing to the cardholder, but in some cases remote facilities have to encode cards after they are issued.

4.2.2 Printing on Cards with Irregular Surfaces

Card technologies can also influence how cards are printed. Some proximity cards are difficult to print because they are thicker than a standard credit card. They may require either printed adhesive-backed cards that are attached to their surface or reverse image printing that doesn’t print directly to the card.

Reverse image printing is especially well suited for cards that are thick, or ones with irregular surfaces such as smart cards with exposed chips and contactless smartcards with embedded antennas. The reverse image process prints graphics and text on the underside of a clear film, which is then applied with heat and pressure to the surface of the card. This process sandwiches the image between the film and the card for greater durability.

4.2.3 Issuance for Multiple Readers

Issuance for multiple card readers needs to be considered when selecting credential issuance systems. Some equipment may be able to encode smart chips and magnetic strips as well as printing graphics on the card to be issued. Some organizations may already have means to encode cards separate from printing and decide the steps are separate. Card issuance applications also differ in there ability to support printing and encoding of cards. Using a single card technology like a Contactless Smart Card can make the issuing process easier and the cardholder experience more consistent.

4.2.4 Centralized and Decentralized Card Issuance

Part of selecting the Card Issuing System involves printing the card and another part involves encoding the card. If the cards are pre-encoded, then the number encoded needs to be correlated to an individual. If photo ID is not required, then the issuing process becomes simpler. Central Issue systems are large modular systems that are configurable for printing and encoding and packaging.

In high security situations where the card has to be used on a network it will most likely use a cryptographic mechanism to be authenticated. This requires a key (either symmetric or private/public system) to be generated, stored in the token and matched with some kind of credential/account/key. This can be done by a central issuance system more easily than with a decentralized system as the cost of a secure key generation station is quite expensive. If information needs to be electronically signed, a signing authority is required. This needs to be done in a secure place and in a trusted environment. So the cost of the card issuing system may depend on the key management for smart technology cards.

Printing Technology	**Encoding**	**Cost of card issuing system** *(not factoring in security)*
Inkjet	Integrated encoder not yet available	Low
Direct to Card	Encoder – printer systems available	Medium
Reverse Image	Encoder – printer systems available	Medium
Offset Printed	Integrated Encoding not practical	NA
Central Issue System	Encoding is part of System	High

Table 5 - Centralized and Decentralized Card Issuance

4.2.5 Central Issue for Large Volume Issuance

Economies of scale may make centralized issuance attractive when issuing cards in large volumes. Conversely, small volumes may make central issue, too expensive. Another alternative is to use a Service Bureau. Secure issuance is typically more effectively achieved with central issuance (inventory management, secret key management, etc.)

4.2.6 Service Bureau for Outside Issuance

A Service Bureau may be required for some organizations. If an organization lacks the required personnel to manage the issuance process, a Service Bureau should be considered. If an organization wants high security, but can't afford the necessary equipment, a Service Bureau may be required.

Another area Service Bureaus can help is with pre-printing cards. It is recommended to pre-print common image features, for example company logos and return addresses, on a card prior to the issuing process. This leaves white, unprinted areas on the cards for variable information such as photos, bar codes, and names. Complex graphics containing multiple colors or solid blocks of deep colors will have a better-finished quality when pre-printed. Pre-printing before the issuing of cards will benefit an organization in several ways: lower fall-out rates during final printing; reduced wear on printer equipment, i.e. rollers and printer heads; and most important a consistent high quality finished product.

4.3 Credential Issuance Security Best Practices

Issuing credentials is a serious endeavor if security is the desired result. A carefully controlled process must be documented and maintained. All steps in the process must be scrutinized for breaches of security. Issuing personnel must protect the security of the credential issuing process and if there are users' rights to information privacy (not always the case in a corporate environment), then this must be maintained.

4.3.1 Validating User Identity for Enrollment

It is important to authenticate the user's identity at time of issuing a card. Two documents that highlight best practice are the AAMVA "White Paper on Over-The-Counter, Central and Hybrid Issuing" and the UK government's "HMG's Minimum Requirements for the Verification of the Identity of Individuals".

As discussed in section 3.1 above, authentication can be based on up to three factors. In the credential issuance process, the card (token) must be produced with the required password/PIN or biometric in mind and then verified as part of the issuing process.

4.3.2 Capturing User Data and Biometric

When capturing user information, it is important to be accurate and only collect necessary data. The user should verify data as part of the issuing process. In addition, it is important to ensure that biometric reading equipment is well maintained. Photographs should be taken to produce a professional looking image. In a typical photographic studio, the lighting consists of 2 or 3 bright lights with umbrella-like reflectors behind the lights. The purpose of all these lights is to direct a lot of light at the subject to eliminate any shadows. Illumination of the face for identification photos is important because shadowy, poorly lit pictures are hard to identify. This is especially important for darker skin tones. Wherever possible, use a photographic studio setup – however where this isn't possible, flash

photography is a good second approach. Bright overhead lighting can also help, but usually creates shadows under the eyes.

4.3.3 Securing Card Production and Distribution

The level of security for credential production will vary depending on the organization, but in most cases, the equipment will need to be secured. There are many ways of doing this. One way is to have security personnel keep the equipment locked up. In some cases, the equipment may need to be physically secured so that it cannot be removed. Another security measure is to remove the printing supplies from the printer while it is not being used.

In some large organizations, many individuals may issue cards. In those situations, security procedures and security audits may be necessary. The AAMVA document "Internal Controls Driver Licensing and Identification Processing Internal Controls" provides a good set of guidelines.

4.3.4 Building Security

The most obvious way to secure a card issuing system is to lock it up. This can take various forms:

- Locked buildings
- Locked card issuing room
- Locked card issuing cabinet
- Access controlled room

Security cameras and access control procedures used for other secure areas of a building may also be appropriate for credential issuing equipment locations.

4.3.5 Equipment Security

The security of card issuing equipment may need protection beyond building facilities. If the equipment is easily accessed, it may need to be physically secured to tables and floors. Special cabinets are sometimes used that make stealing more difficult. Some card printers and systems have features that ensure that only authorized individuals are allowed to print cards. This might be an access card that has to be inserted into the printer before it will operate or a biometric reader connected to the card issuing application.

Authorization of applications and application procedures for the issue/modification of cards should be regulated. Card issue requests and distribution of the card should be documented

The staff employed for card issuance should be "trustworthy" and provide suitable evidence to this effect (certificate of good conduct, authorization to handle classified material, vetting under the Atomic Energy Act – as applicable). In addition, the staff should sign a "Declaration of Confidentiality in the Handling of Personnel Data" relative to governing authorities.

4.3.6 Card (Token) and Printing Supplies Security

Depending on the level of security, some cards and printing supplies may be proprietary to the card issuing organization. For instance, the card may have an organization specific code or a holographic lamination may contain an organizations graphic. In these cases, the printing supplies should be securely locked away when not in use.
Some added security measures include:

- Separating the supplies from the printer.
- Special security systems, e.g. intruder alarms for staff safety.
- Divided the card issuing area into a public and a security area.
- Set procedures for control of card stock and distribution of finished cards.
- Backup and protect data from electronic intrusion.
- Disks and documents containing personal data should be locked away and protected from fire.

4.3.7 Credential Issuance System Maintenance

In a credential issuance environment, there are pieces of equipment to maintain. One of the most important things to remember is to keep card-issuing equipment clean. This includes the following considerations:

- Keep the camera lens clean
- Keep the printing supplies clean
- Keep the card readers clean
- Clean the printer insides like rollers and surfaces regularly
- Clean the fingerprint reader regularly

It is important to become familiar with the maintenance procedures for all card issuing equipment so that production of a bad credential is not likely. Also, enterprises should include in their credential issuance procedures a means to verifying the quality of a card once it is issued.

Computer maintenance is also of prime importance in a credential issuance system. Computers need to be maintained, virus free, and data backed up regularly. A computer security breach could expose data that would make illegal access to buildings or computer systems possible. “System Security” below discusses this in more detail.

4.3.8 Card Distribution

Distribution of cards to cardholders needs to be secure. Transfer of cards without proper procedure will make other security measures worthless. Verification that the card got the correct cardholder is essential. Activation of card keys with the proper timing is essential. As part of the rollout of the Identification Card, the end-user card-holders need to educated on their responsibilities – see section 5.1.3 below for an example checklist.

4.4 System Security

4.4.1 Introduction

The operating environment of smart card enabled access control systems will vary, as will the associated threats and required procedural and technical security controls. Hence, when considering overall system security in an environment where access cards are used for securing access to IT infrastructure, a threat analysis needs to be performed which identifies all the potential attacks against the infrastructure, their likelihood of success and the impact, and the need for security controls to protect applications, data, platforms, and network communications.

In this section, we focus on system security for the access control management system itself. This also needs to be considered as part of a broader risk assessment that identifies the required processes, people responsibilities and technology enforcement mechanisms. Hence this section provides a generic set of issues which organizations should consider relating to security, but will need to adapt depending on the specific concerns, regulatory requirements, application requirements, and system assurance requirements that they have.

In general, there are a number of system security considerations when specifying smart card enabled access control systems. These can be considered under the following headings:

- Administrative security and accountability of the access control system
- Tamper resistance of the cards and management system

4.4.2 Administrative Security

Attacks with the greatest scope for financial impact and disruption of operations arise from insiders abusing their privileges. So it is critical that security management of the access control system itself be tightly controlled.

Hence roles will typically need to be defined which clearly separate the different duties of Token Management within the Identity Card Office and Trust Center parts of the organization (as discussed in more detail in the next section “Organizational Policies and Processes”).

Identity Card Office and Trust Center administrative roles include:

- Policy and profile definition (e.g. the definition of a constrained set of certificate extensions, card applications etc which day-to-day user management should be able to select from – and their prescriptive relationship to HR-driven attributes)
- Organizational trust policy definition – i.e. which external organization’s are trusted, and for what
- Local registration authority (i.e. checking users’ identities, making a certification request on their behalf)
- Certification issuance and revocation using the organization’s policies and profiles

- Card issuance (including photographing or collecting biometric information about the user)
- Auditing of smart card administrative operations
- Management and configuration of supporting directory, policy servers, and OCSP responders
- Configuration management and change control (e.g. careful constraints over who can make changes, and how these get documented and authorized)
- System maintenance (e.g. performance, back-up of supporting platforms)

In addition, the overall system needs to support security administrative roles that include the ability to:

- Authorize panel access
- Define, modify, and revoke access control of users to physical facilities
- Define the IT networks, applications, and platforms that require the use of smart cards to gain access. In many cases, these require administrative facilities that will be embedded within applications and platforms (e.g. Oracle, Windows).
- Define policies and supporting procedures which handle situations for smart-cards can be overridden (e.g. in single-user console maintenance mode, for medical emergencies in healthcare environments)
- Define alerting levels for, and monitor smart-card-based building and IT access
- Obtain and analyze reports

An access control system needs to be able to support:

- The definition of such administrative roles
- The assignment and de-assignment of roles to administrators
- Enforcement of role separation

For separation of administrative duties to be effective, the management facilities of access control system need to be able to:

- Strongly authenticate administrative users (using access cards, apart from exceptional cases)
- Enable administrators' access to authorized functions
- Audit administrative actions

For business continuity reasons, it must be possible to back up the systems and data which support the access control solution – and then restore these in the event of damage to the machine(s) or site. The system maintenance administrator performing the backup and restore must not be able to gain unauthorized access to administrative functions or keying material.

The organization's security group (whether part of the Identity Card Office or not) will need to validate applications' correct use of Smart Card enabled access control systems – so that before being introduced, an application is approved to work correctly, and not conflict with other applications' use of card data. This needs to happen before new applications are introduced.

4.4.3 Tamper Resistance

The access control cards need to be able to withstand tampering attempts, which if successful could enable adversaries to obtain keying material, or access or modify protected information. Standards for this are defined within FIPS 140 and referenced in section 4.1.3 above.

In addition, the supporting operating systems need to be able to withstand attempts to bypass administrative security controls of the access control systems. This requires best practice security configurations which should close known security holes that would enable the box to be hijacked (e.g. through a buffer overflow attack), or otherwise be penetrated by a knowledgeable insider or outsider.

Best practice system security protection includes

- Hardening of the operating system through
  - Correct configuration of platform access
  - Additional access control components
  - Ongoing manual or automatic vulnerability monitoring
  - Regular scanning for malicious code
  - Removal of unnecessary network services
- Maintenance of current security patches on platforms
- Constraints on network connectivity to the access control security management components
  - Internal routing / firewall controls
  - Limits on panel network access to authorized management software
- Auditing, log retention, and log review

4.5 Example Scenarios

4.5.1 Standard Physical Access Control Card Smart Card Token

In many cases, cardholders will possess smart card tokens that are used to gain access to physically controlled portals. In this case, readers interfaced to access control systems typically utilize Security Industry Wiegand electrical interface based on the SIA AC-01 (1996.10) Access Control Standard - Wiegand™ Card Reader Interface.

Other, more advanced, systems allow direct connection of smart card readers to the access control systems, typically through reader interface modules. These systems have extended capabilities, including, but not limited to, key management.

Presentation of the token to a designated reader, normally located on the unsecured side of a portal, initiates a process by which the reader accesses an ID number and formats it for use by the access control system. The access control system then validates the ID number against its database.

There are two methods of identification:

1. Smart card serial number

2. Programmed card number from memory segment.

Smart Card Serial Number
Applications using serial number only for identification typically have no other means to utilize the capabilities of the smart card token. The reader accesses the serial number of the card programmed by the manufacturer, then structures the number for use by the access control system.

Applications utilizing this form of identification are generally one step above the passive 125 KHz token, and are extremely limited in its use.

Programmable Card Number
Applications in compliance with smart card standards thereby implement secured access to pre-defined memory location for retrieval of access control information. At a minimum, ID numbers used to identify the cardholder within the access control system are retrieved through secured and cryptographically protected communications.

4.5.2 Biometric Authentication

Access control biometric authentication provides a greater sense of security by validating the person in possession of the token as opposed to the token itself. Solutions employing biometric authentication include a number of deployment objectives on how template management occurs:

1. Standalone biometric readers with local enrollment. Templates are stored in the reader. All biometric readers are autonomous with a hard-wired connection to the access control panel utilizing industry standard Wiegand protocol.

2. Central database with biometric readers networked, and managed, outside of the access control application.

   Template management is completely segregated from the access control database, and is maintained as a separate infrastructure with connectivity through a hard-wired Wiegand interface to the access control panel. Templates are distributed to the biometric readers through Ethernet connection to the central enrollment database.

3. Standalone readers with biometric templates stored on the token during the enrollment/issuance procedure. Two implementation scenarios offer a varying degree of security:
   a. Validation at Reader
      Biometric templates transferred from the token to the reader for validation. Secured template becomes vulnerable during transmission if a mutual authentication process between card and reader is not available
   b. Match on Card
      Biometric reader transfers scanned biometric image to the card for validation against secured template.

Access control validation becomes a two step process with biometric readers being the first validation barrier, authenticating the biometric scan with the enrolled template before passing the access control ID number to the access control system for further validation.

Under most circumstances, the access control system knows nothing about the biometric component, and after a proper validation of the biometric image, the biometric reader looks like a generic COTS Wiegand reader.

5 Organizational Policies and Processes

When an organization has made their selection of technology (section 3) and best practices (section 4), then the identification token needs to be deployed within an organization.

Bringing together the concepts introduced by this document so far, this section discusses, ownership, processes, and phasing needed to make this process successful – with supporting **checklists** that can be used/modified as needed to meet specific business needs.

5.1 General security requirements

5.1.1 Company Identity Card

- Company Identity Cards and Identity Cards for Business Partners should be clearly distinguishable from one another.
- The Identity Card should contain a security feature in the form of a hologram to reduce the risk of forgery.
- The photo on the Identity Card must enable identification of the Identity Card holder. It must therefore be up-to-date. It must be renewed on certain occasions, and at the latest after 10 years. Any replacement of the Identity Card should be synchronized with the period of validity of the certificate stored on the Identity Card.
- If the Identity Card is worn, the name of the Identity Card holder must be clearly visible and easily read. This makes it easier for security staff to monitor staff “visually”, and it also encourages people to talk to one another.
- Authorization for the use of company resources (e.g. being on site outside normal working hours, borrowing of company documents) must in future be issued only on the basis of authentication via the Company Identity Card. The necessary card-reading technology must be available at the sites.

5.1.2 Identity Card offices

The Identity Cards (including the “blanks”) and the equipment for their production and/or personalization must be protected against unauthorized access, manipulation and sabotage. The following are required for this purpose:

- Special security systems, e.g. intruder alarms or staff safety.
- The Identity Card office must be divided into a public area and a security area. Unauthorized entry to the security area must be prevented.
- Stock control and administration of Identity Cards and card blanks must be carried out according to relevant security and fiduciary principles and must comply with the regulations governing data and information security.
- Data backup: the DP system used for producing Identity Cards must be regularly backed up in accordance with the IS rules.

- All data carriers and documents containing personal data, blank cards and the Identity Cards must be locked away and protected from fire.

The staff employed in the Identity Card offices must be “trustworthy” and must provide suitable evidence to this effect (certificate of good conduct, authorization to handle classified material, vetting under the Atomic Energy Act).
In addition, the staff must sign the “Declaration of Confidentiality in the Handling of Personnel Data” relative to governing authorities.

Authorization of applications and application procedures for the issue/modification of Identity Cards must be regulated. The application for and handover of the Identity Card must be documented; Identity Card holders (and, if necessary, applicants for them – e.g. in the case of business partners) must provide a suitable form of identification (e.g. identity card).

5.1.3 Identity Card holders

The safe handling of the Identity Card by the Identity Card holder (or wearer) is important to the security of the enterprise. Typical policies include the following elements:

- The Identity Card is the property of the corporation
- The Identity Card must be shown at staff entry and control points
- Access control systems should be used
- The Identity Card may not, under any circumstances, be transferred to a third party
- Loss of the Identity Card must be reported immediately
- The Identity Card must be surrendered when the employee leaves the company or transfers or, in the case of Identity Cards for business partners, at the end of the contract.

Additionally, the following security requirements may apply:

- No handwritten or unauthorized amendments or additions to the Identity Card are permitted (e.g. noting of password or PIN, entry or coding of authorizations).
- Where an appropriate local works council agreement has been reached, the Identity Cards are to be worn visibly in accordance with the agreement.
- Carrying and using of copies (e.g., colored paper copies) is prohibited.

5.2 Tasks and responsibilities

This section describes the tasks and responsibilities of the bodies involved in the production, issue and withdrawal of the Company Identity Card. Roll-out is defined in 6.6 below.

5.2.1 Identity Card office (service provider)

The Identity Card office produces the Company Identity Card, checks the identity of the user, manages the data, recalls the Identity Card when the employee leaves and destroys (disposes of) it in accordance with the regulations of the general agreement. It also administers the stock of blank cards and the materials. It generally includes the LRA function.

5.2.2 Procurement office for card blanks

Subject to an order and a contractual arrangement (general agreement), SRE E WBS will handle the selection of suppliers, the central procurement and the distribution of card blanks to the Identity Card offices on a national and international basis.

5.2.3 Management:

Applies for the Identity Card, determines what authorizations and what period of validity should be assigned to the Identity Card, is responsible for recalling the Identity Card (and canceling authorizations) when the employee leaves/is transferred, is responsible for the modification of authorizations in case of job transfers and has fiduciary responsibility. This applies to staff and business partners.

5.2.4 LRA

Authorized department located near to the user to ensure correct user identification and authentication, manages the key material and hands it over to the user.

5.2.5 User

Obtains, uses and returns the Company Identity Card (according to the rules laid down in the Code of Practice and the information security guidelines).

5.2.6 HR/Personnel organization

Supplies information from the employee's master data to LRAs / Identity Card Office. HR also becomes involved where a situation requires resolution (e.g. if an employee leaves the company without surrendering his or her Company Identity Card).

5.2.7 Smart card administrator

This function is usually handled in the Identity Card office or in any LRA. The function includes the following tasks:

- Resetting the PIN to a standard value if the holder has forgotten the PIN
- Resetting the retry counter if the card has been blocked after a certain number of failed entry attempts.

5.2.8 Trust Center

Corporate service responsible for the generation of key pairs, secure storage of key material, and the issue, publication and withdrawal of public key certificates.

5.3 User groups

Groups of users have identity cards that are either person-specific or non-person-specific, and/or physical versus logical

5.3.1 Person-specific Identity Cards

- Serving employees
- Work placement students, student trainees, diploma candidates and PhD students
- Trainees/apprentices

- Business partners: minority stakeholders, joint ventures, service providers
- Consultants, suppliers

5.3.2 Non-person-specific Identity Cards:

- Key cards (without certificate)
- Function identifier (FCT) (e.g. team, management unit, organizational unit) on the contact chip (with certificate).

5.4 Cryptography requirements

The effectiveness of encryption essentially depends on the encryption algorithms used and the key lengths employed. Weak encryption algorithms or short key lengths can make it possible for the procedures to be broken, especially by professional hackers.

Encryption levels can be divided into weak, medium-level, and strong. As a general rule, strong encryption should always be used. Medium-level encryption should only be used in exceptional cases. Weak encryption should be used only if no other encryption method is available.

Even if active cryptographic tokens are not used, it is highly recommended to use digital signatures on all machine-readable information in order to prevent data alteration. This can be achieved by the use of symmetric (e.g. DES, 3DES, AES, etc) or asymmetric cryptographic (e.g. RSA, ECC, etc) algorithms depending on the key management chosen to validate these signatures.

5.5 Process and Planning

Implementation of new identification tokens within large organizations need to be performed in a systematic manor with well-defined procedures. Endeavors of this magnitude should be phased in with measurable and quantifiable metrics (e.g. for performance and functionality).

Definition of the project scope and coordination with various business units is essential to project success. All aspects of the rollout should be defined and documented including:

- Schedules
- Resources
- Project team leaders and participants
- Requirements associated with all phases
- Definition of all required tasks

There are a number of analytical and conceptual activities typically needed to assist in architectural design of the proposed Identity Management infrastructure. These include:

- Analysis and design of the new company ID Card
- Analysis and definition of admission system infrastructure
- Analysis and definition of access system infrastructure
- Development of operational concepts (e.g. processes and ownership)
- Coordination of data delivery (e.g. for users, entitlements from HR)

As part of the implementation and rollout of the new ID card, policies and procedures should be defined to handle situations including the following:

- Hire of new employee
- Reorganization
- Transfer within a company
- End of employment
- User “forgets” the company identity card
- User loses the company identity card
- Denial of site access
- Change of name
- Defective company identity card
- New certificate
- Promotion to upper management
- Non-person-specific identity cards
- Outsourcing and implications
- Business partner use of cards

5.6 Organizational issues

A number of risks can arise in a project to deploy corporate identification cards. This table discusses some of the counter-measures which can be taken to reduce the risk ahead of time, and where necessary to take remedial action to avoid a repeat of the situation.

Project Risk	**Counter-measure**
Chip modules and card blanks not available	Inform chip supplier in good time both from the corporate project as well as local projects, and insure the schedule allows time for delivery and issuance procedures
LRAs/Identity Card offices not installed across a wide enough area or not operational	Increase investment (manpower) and training
No standardized PC equipment at the sites	Define a substitute solution, and coordinate the card project with the new plans for the new equipment
PKI technology not sufficiently advanced	Defined a phased process for implementation
Responsibilities for implementation are not clearly defined	Document the introduction process, and implement in a consistent manner
Enterprise not ready for (mass) rollout or specific functions are not stable	Specify processes, stabilize functionality, issue information about rollout in good time
Departments involved (site security, Project Office, management and employees) are not informed of the new	Implement company-wide projects for information and communication, where necessary specifically tailored for target groups

processes and procedures	
Issues too complex and expenditure too high for smaller groups and regional companies	Corporate departments need to issue mandatory procedures for implementation in good time. Best practices from pilot studies need to be documented and applied globally.
Delays due to organizational and financial reasons. The system lacks a central process owner	Appoint a specialist management unit
Smart cards don't meet functional requirements	Ensure functionality is approved (through clearly defined acceptance tests)

Table 6 – Project Risks in Identification Token Roll-out

6 Best Practices for Managing User Provisioning

6.1 Multiple Systems to Manage

An organization's success depends on the integrity, confidentiality and privacy of its information and processes with the ability to audit governance, compliance and use. To allow users to utilize and benefit from the many applications and services offered today, organizations of all types assign identifiers to individuals in order to grant the necessary rights and privileges for physical and IT access. Hence, effective provisioning of users and ongoing management are at the core of enterprise management.

Identities are required for all users, including employees, business partners and customers - but there are however special challenges in provisioning and managing enterprise users. Within an enterprise, users will need to be defined by HR (with sensitive personal information), and enabled to have facilities access (e.g. with access cards), and network access (across multiple applications and systems). Super-users pose a special concern since they can gain unrestricted access to virtually all a system's files and commands — regardless of their permissions. "Ghost" users — credentials that are not revoked after an employee leaves a company – are another common weakness within the identity management of most enterprises. Today, organizations need to provide auditable proof that only appropriate access is granted to critical data.

Hence appropriate identity verification is required, as well as ongoing management (e.g. for life changes, requirements for new levels of access, and lost/damaged access cards). Individuals take on multiple roles using these identifiers as their digital identities when they move through the organization. These identifiers may change as a transaction flows through the IT infrastructure, but need to be traced back to the original user for correct auditing and accountability.

The proliferation of identities has also increased the need to manage access to business assets. Because today's business systems are all too accessible, organizations need fine-grained, policy-based protection to protect their mission-critical data and services. Individuals take on multiple roles using these identifiers as their digital identities when they move through the organization. And within the IT environment, identifiers may change as a transaction flows throughout the tiers of web servers, application servers, and database servers - but need to be traced back to the original user.

6.2 The Challenges of Consolidating User Management

Typically there are multiple, parallel approaches to managing identities within a single company. A consistent, efficient and secure method is essential to manage identities both internally and externally - and this may be accomplished with a combination of procedures and technical automation (e.g. by replicating HR changes to determine physical access, and also into the IT infrastructure). Managing identities and identifiers across this complex landscape is now a core organizational survival skill that requires consistent, cost-effective

administration and enforcement of access privileges with end-to-end auditing of all identity-related activity.

Today's organizations must ensure they control and audit the process of issuing a user credential, conducting business transactions inside or outside of an organization, or allowing employees, partners or customers to access Web services, files or databases. To accomplish this, organizations need a single view of all activities, such as user management and policy management, or creating a new user account. To securely manage the end-to-end identity life cycle while protecting corporate resources, organizations must adopt a complete, integrated, modular approach to identity and access management in order to fully manage their environment and integrate with their business processes. This approach must take into account the existing systems that organizations have already invested in.

6.3 Types of Users

Organizations need to manage relationships with multiple and distinct populations of identities. These may include employees, customers and business partners. Every type of population requires identity and access management, but has its own unique requirements:

- Employee populations need a traditional, inward-facing approach to security management that focuses on users' access to physical resources and IT systems, and protects internal systems. This solution requires coordination of account management for employees and contractors, access control for internal systems and files, provisioning of physical access to buildings, single sign-on, strong authentication mechanisms and work flow. In addition, it must reduce costs and improve auditing while supporting tens or hundreds of thousands of users. Key to its success is the integration of the solution itself (including the identification token component which is the focus of this document), as well as with business processes.

- Customer populations need an outward-facing security approach that enables secure web access to customer services. From the business perspective, its focus is on customer acquisition and enabling new customer services. From the customer's perspective, its focus is on ease of use, and providing confidentiality of personal data and transactions. The solution must include extranet management, Web services infrastructure and large-scale directories. Additionally, this solution must be scalable to support tens of millions of customers. In some cases, e.g. for high value transactions, physical tokens will be required as part of strong authentication - but building access, or HR system integration will typically not be required.

- Business-oriented identity and access management, also known as B2B (business to business), is focused on cross-organizational transactions. It depends upon legal frameworks, which allow transactions to securely occur between independent entities. It supplies a secure Web services infrastructure to

address the issues associated with cross-company authorization and provides implementations of applicable standards, including: Universal Description, Discovery and Integration (UDDI), Security Assertion Markup Language (SAML), Service Provisioning Markup Language (SPML) and Public Key Infrastructure (PKI). The keys to this solution's success are trust models and bilateral agreements on mutually agreeable trust relationships.

6.4 Drivers for User and Credential Management

The need to react to business priorities has never been greater. A focus on operational procedures drives requirements around efficiency while the continued evolution of on-demand computing — the next level in automated systems management — drives an urgency factor unseen to this point. On-demand computing dramatically increases the need for identity and access management due to its need to provide, provision, and secure. Organizations (particularly IT departments) are also being asked to "do more with less." At a time when the number of identities involved in daily transactions is exploding, the requirements from auditors have multiplied. The rate of mergers and acquisitions may have slowed, but it has not stopped — leaving IT departments with larger user populations, more consolidation and decreasing budgets.

Due to the need to sign on to multiple applications — represents a considerable cost overhead to many organizations. Lost credentials and account lockouts due to sign-on errors further increase these costs. Manual user provisioning and administration are inefficient, and expensive. In today's on-demand computing environment, system management tools monitor the computing capacity of the environment and automatically bring additional computing power online when thresholds are crossed. Identity and access management tools instantly provision user accounts without any human intervention, and allocate access to the new systems and services while installing access controls on system resources — such as files, databases and directories. While promoting efficiency in one's environment, identity and access management needs to be both flexible to allow absorption of the new systems, and scalable to help ensure costs are not exponential with any additional load or reduction.

In addition to the growth in complexity in today's business environment, organizations are experiencing a heightened focus on security. When planning business architecture for the distributed environment, organizations need to include security considerations at the earliest possible stage. Organizations need a comprehensive approach to all aspects of security management, including threat and vulnerability management, as well as identity and access management. The effectiveness, quality and strength of a security infrastructure benefit from the interoperability of the security solutions within it.

The amount of personal and financial information existing in distributed databases, coupled with the demand for open access, has increased demand for protection and highlighted the need for regulations against unauthorized access to information and comprehensive auditing of information accessed by any type of identity. Regulations focus on data in two ways: personal privacy and financial validity. Governments and industry regulatory bodies worldwide are responding with regulations and directives for the privacy

and confidentiality of health care records — the Health Insurance Portability and Accountability Act (HIPAA), as well as financial data — the Graham-Leach-Bliley Act (GLBA) and the EU Data protection Directive (95/46/EC)) and with new controls on accounting practices (Sarbanes-Oxley Act).

Provisioning, authentication, monitoring, reporting and de-provisioning now extend to all aspects of the business and extended enterprise. Employees and contractors are granted access to a wide range of corporate assets, from office buildings and secured test labs to computer systems, files, directories, databases and PCs. In addition, they may be assigned laptops, calling cards and corporate credit cards. Provisioning is no longer limited to IT practices. Additionally, a single credential can be utilized for authentication for both physical resources and cyber access. Specifications, such as ISO/IEC 7816, are trying to deliver on the promise of platform-independent smart card applications. Organizations need to manage the digital identity across entire organizations, authenticating to all corporate assets with a single credential, provisioning all IT systems, Web services, devices and entrance badges and securing access to files, directories and databases while monitoring of all these activities with an end-to-end audit.

6.5 Standards as Protection of Technology Investment

IT departments leverage standards to protect their investment in new technology. Standards come with the promise that current products will continue to interoperate with products from other vendors as technologies evolve and that these technologies can be deployed securely. Today organizations need to adopt strategies for technology and standards adoption to position themselves for participation in the new web economy. For example, identity mapping addresses the problem of reconciling different identifiers with a single individual by allowing an organization, its partners, suppliers and contractors to manage multiple instances of an individual’s identity in context.

Web services enable interoperability among distributed systems/services built and deployed by different vendors or organizations. They use standard interfaces so that one could connect to any Web service and interact with it without any additional knowledge. The service could be anywhere on the web and owned by anyone. Web services are called as objects described by the Web Services Description Language (WSDL) and are published and discoverable from the UDDI registry. Standards and Specifications used in a Web services infrastructure include: SAML, Liberty Alliance, SPML, XML Key Management Specification (XKMS), Passport, Kerberos and Public Key Infrastructure [X.509] (PKIX).

As a benefit to enterprise, their partners, suppliers, contractors and other respective organizations that do business with each other, the large number of identities being processed and passed within the federated network brings up the issue of management of identities. In the Liberty Alliance's work, and the concept of WS-Federation, management is simplified by mapping a user to a particular group of profiles with a role designated to each profile providing business benefits for the management of the federated network but also provides ease of use and delivery to the user of this environment.

Trust management allows for secure transactions across organizational boundaries, enabling individuals in trusted organizations that have common trust agreements or trust models to securely share information. Then cross-domain federation of identities: enables web applications or products from different vendors to share information about the authenticated user across the multiple parts of a business transaction — eliminating the need to for the individual to re-authenticate to each application or Web service. It is defined as the secure trust relationship between multiple disparate security systems that may have one or many trusted parties reviewing and accepting authentication. Standards supporting federated identity include SAML from the Organization for the Advancement of Structured Information Standards (OASIS) and the Liberty Alliance. Microsoft Passport also provides a technology that enables the same credential to be used by different Internet-based services.

6.6 Provisioning Credentials in the Extended Enterprise

Provisioning is the automation of business-oriented workflow of systems, resources, services, and devices to employees, partners, contractors, temp workers is defined as Provisioning. Provisioning of user objects, monitoring of all activities, reporting of all transactions, and de-provisioning of user objects is a fundamental concept of user lifecycle management and how your business operates day to day.

Employees, contractors, temp workers, partners, and suppliers should all be granted access to a wide range of corporate assets, from office building access to accessing of computer systems, files, directories, databases, mail systems, and financial systems. In addition, they may be assigned laptops, calling cards and corporate credit cards. Provisioning is not limited to IT practices. Organizations need to manage the digital identity across entire organizations, provisioning all IT systems, Web services, devices and entrance badges and securing access to files, directories and databases while monitoring of all these activities with an end-to-end audit.

Where provisioning differentiates from standard manual business practices is that when employees, contractors, temp workers, partners, and suppliers no longer are terminated, access rights to all systems, devices, files, etc are all terminated. This reduces the probability of any former employee, contractor, and other affiliates from illegally using corporate assets.

For large organizations like international businesses, government agencies or universities, that need complete identity management, a provisioning system should provide automated provisioning to all needed resources, integration with authentication systems for access, integration with business processes (e.g. through extensible work flow or equivalent automation systems), and auditing of all provisioning and access events. A provisioning system should also facilitate interoperability with business processes and external provisioning or extranet access management systems through implementations of the SAML and SPML standards.

6.7 Provisioning – Parties Involved

The organizational responsibilities for identification tokens have been identified above in section 5.2. In addition, there are number of groups that have interests in the provisioning and de-provisioning of users within an organization. These different groups have different needs that need to be met with a systematic approach to provisioning. These groups include:

- HR - They need to add/amend/delete users, and then expect the resultant user access be consistent with their job-function. When a user leaves the organization, the process of deleting them in HR should trigger their deletion from physical access and IT access.

- IT Managers - They require a comprehensive and modular approach to provisioning. They need to insure it addresses their critical needs, and is easy to use to minimize the support burden. Any automated approach to provisioning must be integratable with their existing infrastructure - and must have an acceptable timeline for deployment, implementation.

- Line of Business Managers - They need to be confident that the provisioning process is going to make the company operate more efficiently. And that it can keep up with the business as it changes, and meets the regulatory requirements that the users face.

- System Administrators - They need to be able to insure that the provisioning approach is reliable, scalable and secure. And that the system easily configurable and manageable - including tracking changes, maintenance of audit logs, and providing the ability to build reports.

- End Users - need the system to be as transparent as possible, so that the building access and system access they need is ready when they are - so that impact on productivity is minimized. When they need to make changes (e.g. to passwords or credentials), the ideal approach to security management would enable them to authenticate using one credential to the different applications. Users also need the system to be able to handle situations of lost/damaged credentials and forgotten passwords as efficiently as possible, while still being secure.

6.8 Provisioning Scenario - Provisioning Work Flow for the First Day at Work.

Figure 3 below shows that a new user, Joe Newguy, is being added to an organization as a VP of Finance role and needs to get the required end-system access to enable him to do his job. An approval request needs to be made and routed through the necessary approvers (either manually or else via an automated workflow process).

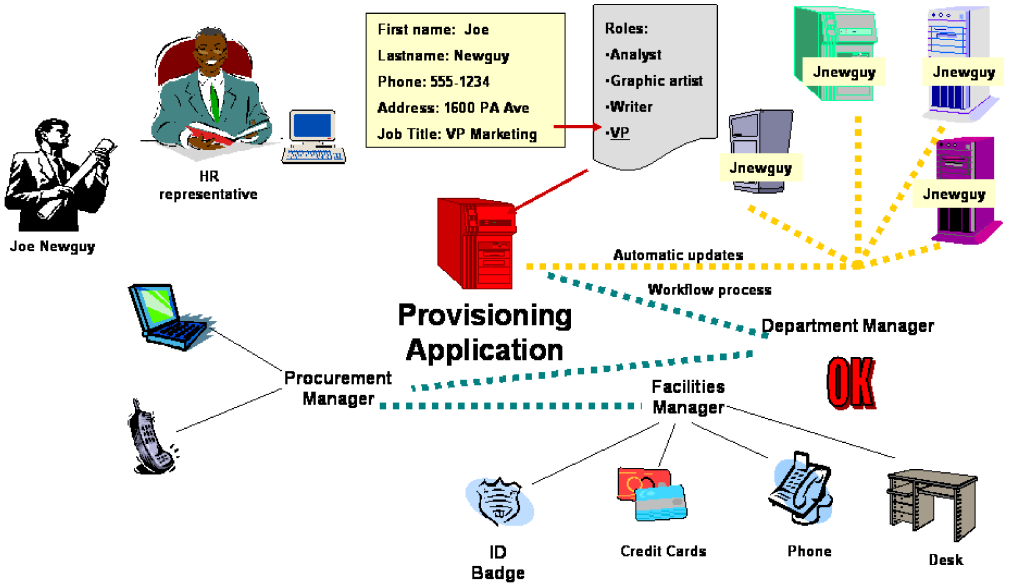

Figure 3 – Provisioning Process

If present, a provisioning automation application would need to translate these business requests and translate them to business and IT activities for resources and services – including the acquisition of an identification token (shown as "ID Badge" at the bottom of the figure). For example, the user must get a building access card for physical access, and will need access to intranet and basic services. They will also need a laptop with a number of office tools, an email account, access to the financial system, a telephone extension with a speakerphone, and business cards. Once approvals are received, updates are made to respective systems where Joe Newguy will be performing his job function.

In the process of obtaining these approvals, certain manual activities may need to take place including buying the laptop, install the software on the laptop, setup the user accounts and database access. In parallel, the telephone must be installed and setup on the provisioned desk, and the business cards need to ordered. For maximum automation capabilities, a robust notification and escalation mechanism would need to be in place for the provisioning activities to address certain workflow activities including buying the Laptop and ordering business cards – and this would typically integrate with existing trouble ticketing and helpdesk infrastructure.

Some organizations may sequence these tasks differently – for example giving the employee an identification token before they are allowed access to logical (IT) systems. In any case, the provisioned user, Joe Newguy, must be maintained, over his lifecycle as an employee with the company, so on the day the Joe leaves, the system would be able to get him "out of the system" immediately. (See de-provisioning in section 6.10 below)

6.9 Provisioning Security Requirements

6.9.1 Provisioning and Security

Provisioning and Security Management fit hand in hand. Communication between the provisioning server(s) and the managed endpoints (target systems) must be secure and encrypted but also the fundamental business process for which workflow is dynamically being generated to support the security policies and business practices of the organization, for which the provisioning of users if being conducted for.

The user information should be usable to create a profile of a person/role that indicates exactly what resources should be allocated to that person/role. Changes to the profile can automatically trigger provisioning or de-provisioning activities. This means that when an employee moves to another business unit, for example, all of the necessary workflow items would start and proceed to the reassignment of provisioned items, of course based on approvals received and external systems like those from HR. Security to the organization is improved when organizations can automate the process of managing access to managed endpoints. You can also essentially rollback the provisioning process, clearing all access rights for any terminated employees via a single process while maintaining a complete audit of all changes.

6.9.2 Provisioning and Credential Systems

Any approach to user provisioning should be able to interoperate with and provision to an authentication subsystem for IT systems and physical access. This needs to support flexible security mechanisms - each authentication point where a user or administrator is authenticated, including web resources, single sign-on, self-service interfaces, and administrator and delegated administrator logins. Organizations may need to plug in a third-party password authentication, security token authentication, biometric authentication, digital certificate authentication or custom authentication methods. Standards interfaces include integration include PKCS 11, SAML, Liberty Alliance and Microsoft's Cryptographic API (MS-CAPI).

6.9.3 Auditing

The provisioning system's auditing system should help ensure that all events and activities associated with identities or resources be tracked. Auditors should be able to see when an identity was created, by whom, where the identity went, what it accessed, what it touched, what it morphed into, when it was suspended, by whom and when it was terminated. It tracks all provisioning activity across the entire enterprise and extended enterprise, monitoring, collecting and filtering events, providing centralized management of organization specific audit policies, triggering alarms and alerts.

6.9.4 Provisioning Standards Support

Provisioning solutions need to interchange with other solutions including other provisioning solutions. SPML, Service Provisioning Markup Language, is a provisioning standard developed and ratified within OASIS is intended to provide a standards-based approach to provisioning and de-provisioning user accounts across heterogeneous systems. This common administration can significantly reduce IT workloads, helps ensure compliance with security policies, and provide employees with immediate access to critical resources.

Changes in human resource systems can be propagated automatically to IT applications without human intervention. As an XML-based framework, SPML allows a provisioning system's capabilities to be extended to any enterprise system or Web service with the necessary compliant interface.

6.10 Best Practices for Managing User De-provisioning

6.10.1 What triggers de-provisioning

De-provisioning should be considered very high on the list of concerns related to security and identity management. Security risks increase exponentially with valid credentials in the possession of invalid personnel, and thus require strict policies and procedures to circumvent potential invalid use.

6.10.2 Employment Status Changed

Changes in employment status could have significant implications depending on what information has changed.

End of employment, including, but not limited to:

- Resigned
- Discharged
- Deceased
- RIF (Reduction in Force)

Require deactivation of all associated credentials. Following notification of an employee's end of employment, the service provider should instruct that the employee's certificate and their assigned rights be deactivated. Status changes that reflect an end of employment have very similar de-provisioning procedures and require methods similar to the following:

- Deactivation of the certificate in the LRA: if the LRA is not on the site, by digitally signed mail from the service office concerned to the responsible LRA or to a service office
- Deactivation of all the other rights contained on the ID card, such as for example restaurant bills, physical access rights, use of company resources
- Destruction and disposal of the ID card
- Documentation

Other employment status changes such as:

- Retired
- Temporary Assignment Ended
- Contract Ended
- Promotion
- Department Move

These may affect only portions of the de-provisioning process, and are dependant on what criteria has changed. Retired personnel might have certain restrictions applied, whereas

Temporary Assignments or Expired Contracted Personnel would have similar de-provisioning procedures from “End of Employment” applied.

6.11 What changes are required when a user is de-provisioned?

6.11.1 Human Resource Systems

Human Resource systems generally retain employment criteria for a number of years after the employee’s exit. Typically the record is marked indicating the new status.

6.11.2 Access Control System

- Cardholder records are disabled, but remain in the database for a period of time i.e. 6-months, 12-months, depending on company policies.
- All access rights removed.

6.11.3 Credential Issuance System

If autonomous, user records need manual updating to reflect current status. Actual status change may not affect the Card Issuance, but depending on criteria used and policies in place, issuance of new credentials may be required.

6.11.4 IT Systems

IT related systems regarding network access including email should reflect the status of the employee and may require modifications to a number of systems including, but not limited to:

- Domain user database
- Email
- Telecommunications Systems
  - Phones, land and mobile
- PKI Certificate Authorities

6.11.5 Other Business systems unrelated to Physical and IT Security.

Other business systems using information stored on the user’s credentials should be reviewed and all the necessary steps taken to circumvent the possibility of invalid access to any system not mentioned above.

Appendix A - Attributes of a Identification Token

The following summarizes the minimum conformance requirements, and recommended best practice for intelligent identification tokens which can meet the needs of both physical and logical access control.

Contact Chip Module Attributes		
Feature	**Mandatory Attributes**	**"Best Practice"**
Protocol	ISO/IEC 7816 T=0 and/or T=1	
Memory	Sufficient to store user data	>32K bytes free
RSA Key Length	1024 bit	
Operating System	Any	VM-Compliant with JavaCard 2.1.1
Key Management	Any	Global Platform 2.0 Compliant
Physical Security	Tamper Resistant	CCEAL4, FIPS 140-1 –2 or better
Application Interface	PKCS#11 **and** MS-CAPI	
Biometric Support	Not Required	Ability to support Match on Card (MOC)

Contactless Smart Card Attributes		
Feature	**Mandatory Attributes**	**"Best Practice"**
Protocol	ISO/IEC 15693 or ISO/IEC 14443	ISO/IEC 14443 Parts 1, 2, 3 and 4
Transmit Frequency	13.56 MHz	
Key Length	64-bit diversified key structure	
Reader Output	Wiegand or RS232	Wiegand
Plastic Composition	PVC, PET or composite	
Biometric Support	Not Required	Ability to store biometric information

Multi-Technology Card
A converged solution will contain at least, both contact and contactless technology.

Table 7 – Best Practice Identification Token Attributes

