The Technology of Identity

A Primer

&

Resource Guide

Prepared by the eC3 Technology of Identity Workgroup

Developed by the National Electronic
Commerce Coordinating Council (eC3)

Presented at the 2006 eC3 Annual Conference,
held December 4-6, 2006, in Sacramento, California

eC3

449 Lewis Hargett Circle, Suite 290
Lexington, KY 40503
859-276-1147

www.ec3.org

Made in the United States of America

A consortium of national organizations and public & private sector leaders identifying best practices for strategic change within government

NASACT - National Association of State Auditors, Comptrollers and Treasurers
NASS - National Association of Secretaries of State
AGA – Association of Government Accountants
ALGA - Association of Local Government Auditors
ITAA - Information Technology Association of America
NACHA - National Automated Clearing House Association
NACo - National Association of Counties
NAGARA - National Association of Government Archive and Records Administrators
NAST - National Association of State Treasurers
NIGP - National Institute of Governmental Purchasing
PTI – Public Technology Institute

Introduction

Identification systems are rarely if ever constructed for their own sake. The systems are designed and the technology bought and implemented to facilitate other needs. These usually include one or more of the following: controlling access to valuable assets or space, facilitating interaction or transactions, tracking location of people or things or similar functions. Generally, the quality of the identification functions should parallel the value of the assets protected or the severity of consequences for not protecting access to a space. It is almost universally true that once deployed any such successful system will quickly be tasked with serving the needs of protecting much more valuable resources or facilitating much more valuable or riskier transactions. Planning and design of any such system should include recognition that requirements will rapidly grow to a need for higher quality identity functions.

This paper is intended to be a resource rich document on the technologies used to verify, assert and assure identity and the technologies necessary to provide identity related functions. It is the intent of this document to provide an introduction for those who are relatively new to this topic or want to dig a little deeper into specific technologies. The body of this document will discuss, generically, technology and important early considerations in brief. The appendices will provide much more detail and vendor specific information, links and documents. This paper is intended to function in concert with two other documents created this year by EC3 workgroups. The other two documents are entitled, "REAL ID is Real" and "Identity Infrastructure" and can be found at www.ec3.org.

The identities discussed herein will mostly be those of people, however, the concept of identity can be usefully extended to other entities including organizations, places virtual and real and things, especially in this case, the devices that people use to connect to the network. The endpoints of a network, after all, comprise not individual persons alone but individuals with the device they must use to attach to the network.

The Basics

One of the most ordinary examples of using the technology of identity is that of logging onto a website, desktop or network that requires a PIN or username and password. The first time one opens a browser and finds a website the screen may request that the user enter the login information or register. In the lowest level, in terms of identity verification, the user asserts his or her identity. No checking or verification is performed and the information provided by the user is accepted as is. If the user claims to be Mickey Mouse that is fine for this use. The user may also be requested to create a PIN, such as 1234, or a username, "MMOUSE", and a password, "abcd. " These are all very "weak", easily guessed or discovered by criminals or mischief-makers, and provide very little value for securing information, interaction or transactions. This level could productively be used for the convenience of users to access low value information or to begin an interaction such as filling out a form. For instance a user might need to collect information to complete a form and would want to pick up the process where it was left rather than starting over and/or the interaction or transaction may not require strong identity verification by the website because it is unnecessary or these functions are completed elsewhere.

PIN's and passwords are likely the most familiar identity technology and it is possible to make very strong PIN's and passwords to provide substantial access control and security. (Please see box below on Randomly Selected Passwords".) Often, however, the requirement to remember them leads to creation of weaker PIN's and passwords and to lesser system security. These are also used in much more secure multi-factor verification or authentication schemes as one of the factors, that of "something you know". Combining strong PIN's or passwords with other techniques, processes and technology is a standard way of protecting extremely valuable information and performing tremendously valuable transactions. These other techniques might include stronger identity verification or background checks, system created or

forced creation of PIN's or passwords to be stronger and perhaps delivered "out-of-band", by some manner other than on the computer screen during registration or refresh, possibly mailed to the user, sent in an email or delivered by phone.1 There is a vast range of technology used in conjunction with and in replacement of this approach which will be the subject of the rest of this document.

There are numerous other devices and techniques that improve upon the security of the username and password. The next step often used in creating a more secure system is to add another layer of authentication which is generally classified as "something you have". There are a variety of card systems and several different technologies used in cards such as barcodes, magnetic stripes, radio frequency devices and electronic chips. When these are employed there is a reader attached to the computer, a device that can read or sometimes "talk" or exchange information with the card. The card may be swiped, as is done with a credit card, held near to a device such as is done when entering many secure buildings or inserted into a slot. The reader discerns the information on the card and then the system performs the appropriate functions which may include requesting further information, username and password or PIN, or perhaps granting access.

Another layer of authentication can be added, this one being commonly known as "something you are" or biometrics. Those commonly used may include fingerprints, faces, corneas, retinas or voices. Some of the more exotic examples are gait and typing patterns. Employing biometrics will require a device that will "read" part of the user. This may be a touchpad or a handheld fob for fingerprints, a camera or microphone. When combined with the previous two types of authentication this is known as three-factor authentication and consists of something you have, something you know and something you are. This is currently used as a high level authentication system to protect high value assets or to mitigate high risk in transactions.

This material is excerpted from NIST 800-63, Appendix A. Please see the entire appendix at the included link above, "Estimating Password Entropy and Strength."

A.1 Randomly Selected Passwords

As we use the term here, "entropy" denotes the uncertainty in the value of a password. Entropy of passwords is conventionally expressed in bits. If a password of k bits is chosen at random there are 2^k possible values and the password is said to have k bits of entropy. If a password of length l characters is chosen at random from an alphabet of b characters (for example the 94 printable ISO characters on a typical keyboard) then the entropy of the password is b^l (for example if a password composed of 8 characters from the alphabet of 94 printable ISO characters the entropy is $94^8 \approx 6.09 \times 10^{15}$ – this is about 2^{52}, so such a password is said to have about 52 bits of entropy). For randomly chosen passwords, guessing entropy, min-entropy, and Shannon entropy are all the same value. The general formula for entropy, H is given by:

$H = \log_2(b^l)$

Table A.1 gives the entropy versus length for a randomly generated password chosen from the standard 94 keyboard characters (not including the space). Calculation of randomly selected passwords from other alphabets is straightforward.

A.2 User Selected Passwords

It is much more difficult to estimate the entropy in passwords that users choose for themselves, because they are not chosen at random and they will not have a uniform random distribution. Passwords chosen by users probably roughly reflect the patterns and character frequency distributions of ordinary English text, and are chosen by users so that they can remember them. Experience teaches us that many users, left to choose their own passwords will choose passwords that are easily guessed, and even fairly short dictionaries of a few thousand commonly chosen passwords, when they are compared to actual user chosen passwords, succeed in "cracking" a large share of those

[1] Include references to other documents and/or appendix on ID verification, etc. from this section

Some systems extend the concept of something you know. These processes are called knowledge-based authentication, KBA. There is a vast supply of information available from public records. Social Security Numbers, previous address, neighbors' names, cross street to current address, mortgage payment amount and even the color of a car owned by the user in 1990 can all be used for authentication purposes. If the user has interacted with a system previously then the knowledge may be from previous transactions. The IRS for instance uses information from previous tax filings to authenticate electronic filers.

The most basic case presented in this document, the one of a simple registration with a website, is an example of self-assertion. For instance the user "claims" the name of MMOUSE and as far as the website is concerned the user is who he or she says. This assertion is of relatively small value for the purpose of identifying the individual or of protecting resources. Improving the value of the registration often involves some other process, possibly conducted offline or "out of band" in which personal information of the registrant is collected and validated against other sources and credentials, such as username and password, a card or token, are issued to the user. The source of the information could be a personnel or human resources system if the user is an employee of an organization or could be an external information aggregator or credit bureau. A number of services are available that will provide files of information against which to verify information provided by a registrant although it is often the case that information is not entirely accurate or even available. The glossary in the appendix defines this process as "claimed identity validation." Some companies will undertake to verify identities as an outsourced or managed service or provide a score purporting to rate the likelihood that an individual is who they claim to be. In some cases these companies will verify financial account information and insure transactions based upon these processes.

The identifying information such as username, password, PIN and other associated attributes could be stored in a file or simple database. When a user attempts to access the system employing the username and password or PIN the software looks for the particular username and decides whether the password or PIN matches that established by or for the user. If it matches that stored in the system then access is granted. If no match is found or the username does not exist then usually an error message is returned that includes possible remedies such as suggestions to try again, register or use a password or username recovery option. Instead of the file or simple database there could be employed software tools developed precisely for these uses such as directories, identity management (IDM) databases, IDM tools and IDM suites. These build upon common software tools and are customized to better perform the functions of identity management including identity verification, provisioning, de-provisioning and authentication.

Sharing Technology

Extracting identity functions from individual applications provides valuable flexibility. Employing these IDM tools allows for performing identity functions across a number of applications or even throughout an enterprise. This approach allows for more efficient use of resources, greater specialization and expertise, better performance of identity functions and cost savings to the enterprise. Performing identity functions can be expensive and require substantial time, resources and expertise to conduct. Performing these functions as a shared service spreads these costs across a wider base. Extending this concept beyond the boundaries of the enterprise has led to development of identity federation.

There are a number of such identity federations under development or in operation. Some of them are as follows:

- Signatures and Authentication For Everyone (SAFE) of the BioPhRMA Association
- E-Authentication Federation
- E-Authentication Partnership

- FiXs/DCCIS
- InCommon (Shibboleth-based federations)

These federations create the infrastructure of policy, process, technology and compliance to develop a network of trust across a collection of organizations in order to share identity functions. Some participating entities will provide credentials to users to be trusted by other entities participating in the federation. Much of the documentation of the policy, process, technology and compliance are available through the websites listed above and further information is included in the appendix to this document.

Most of the discussion to this point has focused on identification of people, the system users, and vetting or assuring the identities of those users. It has been common that vetted and credentialed users will access network resources through a totally unmanaged (or unidentified) device in effect, *letting someone in, in order to determine whether or not they should be let in*. Although this approach is better than nothing, much damage can nevertheless be done immediately upon connection of a (contaminated) unmanaged device to a target network. Clearly the ability to assign an identity to a device, as well as the user, and manage access of that device to the network accordingly provides significant security benefits.

Identifying devices prior to permitting them logical access to the network allows exclusion of unknown devices. This is a significant improvement over the above described practice facilitating better access management. NIST has created documentation on device authentication in SP 800-53 and related documents. The concept of an assured identity may be further extended beyond people and devices to include validating the identity of a document, or a piece of code. This is a viable aspect of identity but is beyond the scope of this paper.

The Parts—Common Components

The first point at which a user interacts with identity technology could be when he or she registers or is registered so that the user can access protected resources. These protected resources might be a building or room, equipment, websites or networks or other assets to which access is controlled. This registration can take a variety of forms. The prospective user may have to present a birth certificate, in the case of applying for a passport or driver's license, or a passport or driver's license when becoming an employee of an organization or to receive a credential from some of the federations mentioned such as the E-Authentication Federation, E-Authentication Partnership or FiXS (more on these to follow). These documents, sometimes referred to as breeder documents, can have a variety of technologies built into them or otherwise employed to support their intended functions. Most readers will be familiar with a birth certificate. The members of the National Association of Public Health Statistics and Information Systems, NAPHSIS, have collaborated to produce guidelines for greater security of physical birth certificates and continue to work with other organizations to develop methods and systems of information capture and exchange that recognize and appropriately share data on life events of citizens such as births and deaths.

The paper birth certificates provide examples of physical document security features. These documents may be printed on special paper with particular inks, stamps and watermarks. NAPHSIS has developed guidelines for the management of the paper on which birth certificates are printed, Management of Paper. Other organizations and industries have created standards for various items special to their interests some of which are directly related to identity and its functions. The members of the American Association of Motor Vehicle Administrators, AAMVA, have worked to develop and adopt a variety of standards for drivers' licenses and identity cards and associated technology and practice. Their website, AAMVA : Standards & Technology Overview is a good resource for further information. Standardization of these components allows for easier interoperability and usefulness of these components of identity.

Included in the appendix is a list of some of the common components with explanations and links to further material.

How the Parts Can Fit Together

The following sections on PIV, ACES and FiXs demonstrate how the identity components begin to coalesce into an identity infrastructure which is the topic of another EC3 white paper for 2006. Access Certificates for Electronic Services (ACES) is a long-standing contracting vehicle for federal government personnel to obtain electronic credentials. There are other more recent programs that provide means to obtain other credentials. The E-Authentication Initiative (EAI) that became the E-Authentication Federation when incorporated in the Federal Enterprise Architecture was one of the President's E-Government Initiatives. The EAF is, "a public-private partnership that will enable citizens, businesses and government employees to access online government services using log-in IDs issued by trusted third-parties, both within and outside the government."[2] The log-in ID's are those such as issued under an ACES contract. Whatever the purpose for which an approved credential was issued it now can be used across a growing range of agencies websites for accessing protected resources through the E-Authentication Federation system.

In 2004 President Bush issued Homeland Security Presidential Directive 12(HSPD-12) "establishing a mandatory, Government-wide standard for secure and reliable forms of identification issued by the Federal Government to its employees and contractors (including contractor employees)."[3] HSPD-12 required development of a standard, Federal Information Processing Standard 201 (FIPS 201) and an implementation program Personal Identity Verification (PIV). Through the PIV credentials will be issued to all government personnel and contractors. These credentials will be used to access physical facilities and online resources in the future.

The Federal Identity Cross-Credentialing System was initiated to standardize credentialing across a group of government defense contractors to improve security while simplifying access to government and contractor physical facilities. The FiXS organizations works with the other organizations mentioned above to increase the usability of issued credentials and to reap further benefits of federation and reduce credentialing costs.

These initiatives and projects enable users to receive standardized credentials through a standardized process and then to reuse these credentials to access a widening array of physical and virtual resources. These and other systems extend similar capabilities to other levels of government and outside of government.

ACES

In the mid-90's, the General Services Administration (GSA), working with a number of other agencies, began groundwork on an identity credential that could be used by a citizen or business officer to assert their identity to any of a number of different business applications at multiple federal agencies. These credentials could also be used for digital signing of electronic documents.

In 1999 contracts were awarded for Access Certificates for Electronic Services (ACES). Three companies were authorized to authenticate citizens and businesses and issue software-based digital certificates that could be accepted by agencies. Subsequently, numerous agencies including Labor, State, SSA, Treasury, and the US House, began developing or modifying online services to accept these identity credentials.

[2] http://www.cio.gov/eauthentication/

[3] http://www.whitehouse.gov/news/releases/2004/08/20040827-8.html

The ACES identity credential is still in active use and is cross-certified with the US Federal Bridge (for PKI credentials) and is mapped into the e-Authentication initiative. For more information see www.gsa.gov/aces/.

E-Authentication Initiative (EAI) /E-Authentication Federation (EAF)

"E-Authentication is setting the standards for the identity proofing of individuals and businesses, based on risk of online services used. The initiative will focus on meeting the authentication business needs of the E-Gov initiatives, building the necessary infrastructure to support common, unified processes and systems for government-wide use. This will help build the trust that must be an inherent part of every online exchange between citizens and the Government."[4]

Homeland Security Presidential Directive 12(HSPD-12)/Federal Information Processing Standard 201(FIPS 201)/ Personal Identity Verification(PIV)

This section provides an overview of the technology required to implement Federal Information Processing Standard Publication 201 (FIPS 201) compliant solutions.

To protect their network and facilities, FIPS 201 demands federal agencies, first responders and government contractors' organizations to meet a number of security control and interoperability objectives for the identity registration, issuance and usage of PIV cards for their employees:

- Enroll employee and obtain digital identity information from available breeder documents and capture identity traits
- Register employee vetted digital identity information
- Issue to the employee a single credential for use in both logical and physical access domains
- The credential must be resistant to fraud and can be rapidly authenticated
- The credential must support multiple levels of identity assurance
- The credential interfaces must strictly implement PIV end-point specifications
- Support a number of Interoperable use cases to enable access control across federal agencies.

Several federal Government programs including the DoD Common Access Card have proven that appropriate technology such as smart card and PKI for logical access can be implemented to meet these objectives and such implementations can be deployed on a very large scale.

To specify the PIV credential, FIPS PUB 201 refers to existing technology such as smart card, PKI and biometrics and mandates the application of corresponding ISO or ANSI standards. Additional NIST Special Publications specifications are complementing FIPS201 and the base standards to meet all interoperability and security objectives.

To specify the PIV Registration and Issuance system, FIPS 201 provides the necessary requirements to ensure that the system security and privacy objectives will be consistently met. It emphasizes on the necessary protection measures to establish a vetted digital identity and issue a trusted credential. However, FIPS 201 and its companion documents leave to agencies and industry many implementation options to accommodate the system deployments.

Some technical aspects are still incomplete. For instance Interoperable system interfaces to implement shared services such as the mass production of cards are currently being defined.

[4] http://www.cio.gov/eauthentication/

A large pool of industry vendors and service providers has implemented the many pieces of the FIPS201 ecosystem. NIST and GSA have defined corresponding tools and a certification program to ensure that implementations meet the desired security and interoperability criteria and therefore can be purchased and deployed.

FIPS 201 is driving government agencies, businesses to improve identity authentication. FIPS 201 is forcing a convergence of physical and logical access with a single credential and registration that requires the adoption of new technologies such as PKI, contactless smart cards and Biometrics. The deployment of first FIPS201 certified cards is planned for October,27 2006.

FiXS

The Federation for Identity and Cross-Credentialing Systems (FiXs) anticipated the challenges that are being addressed by HSPD-12. FiXs, a coalition of government contractors, companies, and not-for-profit organizations, was formed several years ago and formalized as a not-for-profit in 2004. FiXs initially sought a means for authenticating members of the DOD contractor community to each other and to DOD installations. FiXs is today implementing an identity cross-credentialing network, by setting and maintaining standards for authentication and identity management amongst member organizations. The network has developed a secure, interoperable electronic means of authenticating an individual. FiXs can be used within and between organizations and promotes trust through a federated identity infrastructure. For more information see www.fixs.org.

Challenges

Privacy and Security

While privacy and security are different issues the means to address both lie in the same technical skills, capabilities and technology. Both require the means to control access to systems and information according to applicable policies, to record or log events when information is accessed and appropriately inform owners of systems and the information. Privacy is an issue that will continue to occupy a prominent space in public discourse and should be addressed in the design, implementation and operation of any system that will collect, use or store personally identifiable information. Similarly, security breaches and the reports of lost social security numbers[5], lost account numbers[6], and losses such as those from identity fraud[7] that have a direct impact on consumers and employees everywhere continue to flood news and information channels. Both privacy and security are important issues to address. It is beyond the scope of this paper to deal in depth with either issue. Generally conducting better identity functions will facilitate improved security and there is more extensive information included on privacy in the appendix with significant references.

Trust

Trust is often difficult to create or develop and can be very fragile. Building an infrastructure that will facilitate or enhance trust among participants, often called a system of trust or a trust infrastructure may require a lot of work and other resources as well as special skills and expertise not always readily available to an individual organization. People involved in development of identity federations often conceive of their work as that of creating a trust infrastructure.

[5] http://www.firstgov.gov/veteransinfo.shtml#happened-Aug06
[6] http://www.privacyrights.org/ar/ChronDataBreaches.htm
[7] http://www.consumer.gov/idtheft/

Many organizations choose to join with others in a federation to obtain the business benefits of belonging to a trust system without having to undertake the arduous and expensive task of developing one. This will become a more usual way of obtaining identity functions as federations expand their scope and prove their ability to provide value to participants.

Culture

Always one of the most challenging issues to address changing the culture of an organization is the subject of many articles, books and careers. Done badly it will spell disaster for any undertaking. Done well the organization will derive many direct and indirect benefits. Incorporating new technology and processes, especially ones that use personal information will undoubtedly raise concerns among the members of an organization. Careful consideration of issues related to organizational culture change will be important to the success of any effort to incorporate the use of identity technology into an organization. One organization that focuses heavily on issues of culture change and technology and those of using technology to change organizational culture is the Harvard Policy Group headed by Dr. Jerry Mechling of the Harvard Kennedy School of Government. Dr. Mechling brings together a broad range of personnel from government and non-government organizations to address a range of topics related to these issues. The website, www.lnwprogram.org , will provide an array of information on the topic and a document entitled, "Eight Imperatives for Leaders in a Networked World" is a good one with which to start.

Procurement

There are many options for procuring the technology components and services related to identity functions. Included in the appendix of this document is an article on procurement from GSA schedules. There are a number of organizations that provide worthwhile information for those addressing these issues some of which are listed here:

- National Contract Management Association
- National Institute of Governmental Purchasing
- Universal Public Purchasing Certification Council (UPPCC)
- U.S. Communities : Government Purchasing Alliance

References

There are many sources for reference material on this subject and the universe of materials is growing much more quickly than would be possible to cover in a static document. Included below are descriptions of some available reference materials and in the appendix are some of the materials that should be valuable to newcomers to the subject of identity, to those who are looking to increase their understanding on the topic and to those looking for decision support and implementation advice.

Key Terms (Glossary)

There have been a number of glossaries developed providing definitions of terms associated with identity and related functions. Included in this paper is a glossary developed by the ITAA, Information Technology Association of America, Identity Management Task Group. ITAA members cover a wide swath of the technology industry and communications, banking and financial, health and other business verticals. ITAA brings together these business participants with government personnel to address common issues related to information technology. The glossary is included in the appendix.

Standards

There is a rapidly growing world of standards related to identity and associated functions developed by various government and private sector organizations. The American National Standards Institute (ANSI) and the Better Business Bureau (BBB) in collaboration have formed the Identity Theft Prevention and Identity Management Standards Panel (IDSP). This panel brings together dozens of participating organizations, including EC3, to first catalog standards relating to identity management and those related to identity and then to identify gaps in this catalog of standards. Some existing standards that may be of interest to readers are included below. The inclusions here are by no means comprehensive, but may provide insights into the type of standards available for consideration.

National Institute of Standards and Technology (NIST)

The Computer Security Division (CSD) of NIST has produced a range of standards documents used by the Federal Government to conduct identity functions and address policy, procedure and technology. Descriptions of NIST and the CSD from the respective websites follow.

> "Founded in 1901, NIST is a non-regulatory federal agency within the U.S. Commerce Department's Technology Administration. NIST's mission is to promote U.S. innovation and industrial competitiveness by advancing measurement science, standards, and technology in ways that enhance economic security and improve our quality of life."
>
> "The Computer Security Division (CSD) - (893) is one of eight divisions within NIST's Information Technology Laboratory.
>
> The mission of NIST's Computer Security Division is to improve information systems security by:
>
> - Raising awareness of IT risks, vulnerabilities and protection requirements, particularly for new and emerging technologies;
> - Researching, studying, and advising agencies of IT vulnerabilities and devising techniques for the cost-effective security and privacy of sensitive Federal systems;
> - Developing standards, metrics, tests and validation programs:
>   - to promote, measure, and validate security in systems and services
>   - to educate consumers and
>   - to establish minimum security requirements for Federal systems
> - Developing guidance to increase secure IT planning, implementation, management and operation."

The documents produced by the CSD can be found at the Computer Security Resource Center, NIST Computer Security Division's CSRC Home page. There are numerous documents that may apply to a particular application. Consideration should be given to 800-63 Electronic Authentication Guideline, 800-73 Interfaces for Personal Identity Verification and the documents related to the Personal Identity Verification of Federal Employees/Contractors, collectively known as Federal Information Processing Standard 201 (FIPS 201) which is the result of President Bush's Homeland Security Presidential Directive-12 (HSPD-12).

Accredited[8] Standards Committee X9, Inc. – Financial Industry Standards

ASC X9 has produced and maintains a large body of standards for the financial services industry some of which deals directly with identity information and could be informative for government personnel. ASC X9, Inc. via ANSI holds the Secretariat for ISO TC68 – Financial Services and ISO TC68 SC2 – Financial Services - Security. Included below is the mission statement of this organization and a list of standards and catalog are included in the appendix.

> "Mission/Objectives of ASC X9
>
> The Accredited Standards Committee X9 (ASC X9) has the mission to develop, establish, maintain, and promote standards for the Financial Services Industry in order to facilitate delivery of financial services and products.
>
> Under this mission ASC X9 fulfills the objectives of:
>
> - Support (maintain, enhance, and promote use of) existing standards;
> - Facilitate development of new, open standards based upon consensus;
> - Incorporate nonproprietary items developed by other organizations where appropriate;
> - Provide a common source for all standards affecting the Financial Services Industry;
> - Focus on current and future standards needs of the Financial Services Industry;
> - Promote use of Financial Services Industry standards; and
> - Participate and promote the development of international standards."[9]

Document Security Alliance

> "The Document Security Alliance is dedicated to improving security documents and related security procedures by drawing upon the knowledge and detailed technical disciplines of its members."[10]

The Document Security Alliance brings together personnel from Government agencies, private sector organizations and academia to address the issues of document security.

> "Currently, the government agencies that have been active in the DSA include: U.S. Secret Service, Department of Homeland Security, U.S. Food and Drug Administration, Transportation Security Agency, Social Security Administration, U.S. Postal Service, State Department, Government Services Administration, Federal Bureau of Investigation, The White House, U.S. Treasury Department, Government Printing Operations, U.S. Treasury Inspector General for Tax Administration, Central Intelligence Agency and Immigration and Naturalization Services. In addition, volunteers from over eighty worldwide companies and have organized committees within the meetings and have worked diligently to provide the group with recommendations on processes, methods, techniques and technologies that could be used to improve the forensic tracing of fraudulent documents. Participants at these gatherings have continued to include a broad representation from the credentialing industry

[8] Accredited as a national standards developer by the American National Standards Institute.

[9] From X9, Inc. website: http://www.x9.org/mission.shtml

[10] Document Security Alliance website: Document Security Alliance

including system integrators, card manufacturers, secure printing companies, printer manufacturers; security features producers, encryption organizations, biometric providers and security industry associations."[11]

[11] IBID

Appendix

Industry Information

Included in this section of the appendix is information from industry participants who have helped to provide information and support for this effort and who provide solutions and services to government for identity management and related functions. We at EC3 thank them for their contributions.

For easier navigation included here are links to the various materials included below:

Accenture Security Practice – Overview

The primary focus of Accenture's global Security Practice is to provide solutions which address the critical issues of risk, trust, privacy, access, governance and compliance. Accenture's 1000 plus global security partners and consultants are highly trained, certified professionals who possess considerable knowledge, strategic acumen, strong execution capabilities and an in-depth understanding of the security applications which are critical to every High Performance organization.

Experience has proven that an integrated, embedded security infrastructure which is tied to strategic objectives and underlies all business functions across an extended enterprise is fundamental to an organization's ability to limit exposure to both internal and external threats and protect proprietary processes, thought leadership and intellectual capital. Accenture's Security Practice offerings range from solutions which address specific applications to providing holistic, integrated end-to-end solutions to managing outsourced services

Dr. Alastair MacWillson is the Partner in charge of Accenture's global Security Practice. Alastair and his team work closely with business and government leaders around the world on critical issues such as security strategy, risk, trust, privacy and compliance. Alastair brings global security experience, expertise and insights in identifying and delivering work for NHS, QinetiQ, London Stock Exchange, Banca Intesa (Italy), BP, Shell, Dupont, Ericsson, UK Home Office and Department of Immigration, US Departments for Education and Defense, Homeland Security… He has also recently launched a new Security capability in the India Delivery Centre and will soon announce a new Enterprise Security Outsourcing offering.

Solution Offerings

1. **Security Risk Management -** Provides an integrated enterprise, scalable, standards-based approach to risk in an operational, continuous process improvement infrastructure. Security is embedded into the organization's strategy, enterprise risk management frameworks and software development lifecycles that drives organizational design, governance, privacy and compliance.

2. **Enterprise Application Security** – Provides a roadmap for discrete strategic investments aligned for technological advancements and regulatory needs. Offers a holistic approach to SAP security; encompassing technology, controls, processes, and management which is integrated with Enterprise-wide Identity Management standardized roles and authorizations.

3. **Identity and Access Management** – Design and implementation of a single identity which is shared across applications and resources through the implementation of processes and technologies to manage identities and attributes in a consistent manner.

4. **Infrastructure Security** – Provides technology frameworks which manage access to the organization anytime and anywhere while maintaining the right level of asset protection through authentication and authorization programs, combined with granular access control.

5. **Business Continuity Management** – Integrates of all lines of business into a disaster recovery and continuity program to provide end-to-end availability and protection of business processes across the organization. Identification, implementation and test recoverable, highly available and secure solutions to support and protect against treats and violations.

Security Domain Contacts:

Alastair MacWillson, Global Security Practice Lead, Alastair.Macwillson@Accenture.Com
Stephen A. Barlock, North America Security Practice Lead, Stephen.A.Barlock@Accenture.Com
Robert W. Dyson, Sun Security Initiative Lead, Robert.W.Dyson@Accenture.Com
Jesse W. Bowen, Symantec Security Initiative Lead, Jesse.W.Bowen@Accenture.Com
http://www.accenture.com/security

ActivIdentity

industry brief

ActivIdentity Solutions for Business and Government

Smart Employee ID

For organizations seeking to deploy a single and secure intelligent ID badge allowing employees, contractors, customers and business partners to access corporate facilities and IT resources, ActivIdentity provides a Smart Employee ID solution that enables secure access, communications and transactions while reducing administration costs and improving user convenience.

Business benefits

Compliance, brand and liability protection

A security or privacy breach can result in high remediation costs and permanent damage to the image of any organization. ActivIdentity Smart Employee ID solutions reduce the risk of such events by strengthening proof of identity and securing access to information.

Accountability

When a security incident occurs, the organization must be able to identify who broke the rules. Strong proof of identity and tight integration between security audits are the keys to providing legally enforceable proof of access to facilities, IT systems and information.

Cost reduction

Separate processes for issuance and administration of facility access badges and IT security tokens leads to high costs, duplicated administrative efforts, and increased security risk. With ActivIdentity Smart Employee ID solution, smart cards for facility and IT access can be issued directly from the facility access control system, therefore increasing security and reducing operating costs.

Productivity

In a typical organization, users login with user names and static passwords multiple times per day. With smart card authentication, the login experience is fast with an ATM-like experience and enables access to any enterprise application for a true single sign on.

Employee education

Frustrated users tend to work around security policies to make login to computers easier. With ActivIdentity Smart Employee ID solutions, convenience and security are tied together.

Organizational efficiency

As recent regulations have increased the accountability of executives, many organizations are merging their facility and IT security teams into a single group. ActivIdentity Smart Employee ID solution enables alignment of processes and technology to reinforce this.

Highlights

- A single smart card enables proof of identity for strong authentication to IT resources, secure communications and transactions, and secure access to facilities.
- Consolidate processes for issuance and management of smart cards for facility and IT security.
- Enable auditing and reporting of physical and logical access events.

Customer quote

"With the ActivIdentity Smart Employee ID, Sun Microsystems' personnel will be able to use one smart card for both secure IT and facilities access. We are consolidating our processes for issuance and management of these cards, in conjunction with our own identity management products, to streamline and gain greater efficiency throughout our global infrastructure. Smart Employee IDs help to enhance security, while increasing employee productivity, accountability and mobility."

Bob Worrall, Chief Information Officer of Sun Microsystems

Moving from existing solutions

Why replace passwords?

Passwords are insecure: A password can be used by anyone who knows it and there is no way to be sure that password-authenticated users are really who they say they are.

Passwords are inconvenient: End-users typically choose weak passwords to make them easier to remember. Strong password policies can reduce this risk, but passwords then become too complex to remember, so end-users write them down on sticky notes under the keyboard or other trivial locations. In either case, the end-result is similar: weak proof of identity and compromises in security policy.

Why migrate from tokens to smart cards?

Functionality: One-time password tokens provide a higher degree of security than password authentication, but their usage is limited to authentication. By itself, a token cannot be used to sign a document or encrypt a file. A smart card or USB token, on the other hand, can be used for secure communications and transactions.

Limited usability: Users read the one time password from the token display and then type it on their workstation keyboard. This can be time consuming, and typing mistakes can lead to multiple authentication attempts. A smart card or USB token only requires the user to insert the device and type in a simple PIN code.

No integration with facility security: One-time password tokens do not replace facility access badges, and cannot be issued or administered directly from the physical access control system console.

ActivIdentity Solutions for Business and Government

Technical benefits

Complete solution

The Smart Employee ID solution enables two-factor security across the IT infrastructure, including secure remote access, workstation access, network access, application access (single sign on), as well as secure information and transactions through signed and encrypted e-mail, documents, files and transactions, secure auditing, and data protection.

Increased security compliance

Address IT and facility security compliance requirements (Sarbanes-Oxley, Basel II, Gramm-Leach-Bliley, HIPAA, HSPD-12) by establishing strong proof of identity, preventing unauthorized access to resources and information, and providing comprehensive audit logs. ActivIdentity solutions link users to online activities with a strong proof of identity.

Ease of deployment

ActivIdentity solutions integrate with existing IT and facility security environments for cost-efficient deployment and operation, through extensive support for a variety of smart cards, directories, certificate authorities, identity management and user provisioning systems, facility security systems.

Government-approved security

ActivIdentity Smart Employee ID solutions are used by many government agencies around the world and comply with multiple security standards such as FIPS 140 and FIPS 201.

Extensibility

Open APIs and SDKs allow easy integration with more environments such as additional identity management and user provisioning systems, certificate authorities, and facility access control systems.

Future-proof

ActivIdentity Smart Employee ID solution is an integrated and modular suite of products that allows organizations to easily deploy smart cards for their immediate business needs (such as replacing expiring tokens used for VPN access), and adding functionality later as their needs grow, such as increasing security for LAN access.

Standards Support

- Card management: GlobalPlatform
- Java Card™
- ActivIdentity CMS and ActivClient received PIV / FIPS 201 certification
- PIV / FIPS 201 cards and applications
- FIPS 140-2 cards and applications
- FIPS 140-2 Hardware Security Modules
- Directory interface: LDAP v3.0
- Web communications: SSL 3.0
- Accessibility: Section 508
- PKI: PKCS#7, PKCS#10, PKCS#11, X509, CRMF / CMMF / CRM
- U.S. DoD GSC-IS and CAC

ActivIdentity offers

Products

- ActivID™ Card Management System (CMS)
- ActivClient®
- ActivIdentity Readers
- SecureLogin® SSO
- 4TRESS™ AAA Server

Technology solutions

- Strong Authentication
- Enterprise Single Sign On
- Secure Information and Transactions
- Device and Credential Management

Industry solutions

- Smart Employee ID
- Smart Employee ID for PIV
- Strong Authentication for Banking
- Single Sign On for Healthcare

Partner solutions

- Novell Identity Assurance solution
- Smart Employee ID for Sun Java System Identity Manager
- Smart Employee ID with Lenel OnGuard
- Smart Employee ID for PIV with Lenel IdentityDefender

About ActivIdentity

ActivIdentity, Inc. is the trusted provider of identity assurance solutions for business and government worldwide.

ActivIdentity provides the only fully integrated platform that allows organizations to issue, manage and use trusted digital identities for secure access, secure communications, and legally binding digital transactions.

ActivIdentity customers experience multiple business benefits including protection of resources and information, enhanced workforce productivity and regulatory compliance.

Partners

Adobe
Microsoft Gold Certified Partner
CyberTrust
Novell
Entrust
Sun microsystems
Honeywell
Lenel
VeriSign

www.actividentity.com

Americas	+1 (510) 574 0100
US Federal	+1 (571) 522 1000
Europe	+33 (0) 1 42 04 84 00
Asia Pacific	+61 (0) 2 6208 4888
Email	info@actividentity.com

ActivIdentity

NORTEL
Government Solutions

Solution Brief

Security Services

Identity Management Services

Secure System Center, IAED, EGIS

The Secure System Center (SSC), a center within Information Assurance and Engineering Division (IAED), has provided full lifecycle Identity Management solutions to Federal Government agencies for almost a decade. IAED is a component of the EGIS business sector.

Identity Management Functional Overview

Identity Management is an aggregate of policies, procedures, people, and technology. Nortel Government Solutions' Identity Management Solutions (IdM) Set is predicated upon its extensive experience in: Public Key Infrastructure (PKI) and global directory services design, implementation, and support; Government regulation development, policy development. IAED has been developing an IdM Service offering that is vendor independent. Nortel Government Solutions has an in-depth knowledge of the leading standards-based Identity Management solutions and is able to select the proper blend to facilitate secure information sharing intra- and inter-organization. We have focused its reach and development on building a service offering that includes PKI, Directory Services, Smartcard/Token-based Services, Web Enablement, User Provisioning, Auditing, and Identity Lifecycle Management.

Identity Management Technologies

The following table details the major Identity Management components and benefits.

Identity Management and Related Technologies

Key Components	Benefits
User Provisioning and Compliance	Workflow Automation, User Lifecycle Management, Auditing & Compliance
Federated Identity	Ability for identities and entitlements to be propagated across security domains. Secure information sharing.
Directory Services	Certificate Revocation List (CRL) repository. Central user repository. Facilitate administration, references to other directories and existing repository stores.
Strong Authentication	Includes support for PKI credentials, smartcards for key storage, and biometric for authentication to smartcard contents.
Web Services	Supports deployment of SOA, centrally define policies that govern Web services.
Toolkits	Supports Enablement of Web services.
Identity Administration	Administering users/entities and their privileges.
Single/Reduced Sign On (SSO, RSO)	Help Desk, Administration, User Experience (fewer username/passwords).

Identity Management Related Directives and Legislation		
Directive	**Description**	**Impact**
Homeland Security Personal Directive 12 HSPD-12	> Issued August 27, 2004 > Directed the creation of a common identification standard for all Federal employees, contractors, and affiliates.	> Citing the risks of wide variations in identity proofing and identity management, the directive mandated that NIST promulgate standards for identity-proofing personnel as well as technical requirements for a common smart-card-based Personal Identity Verification (PIV) system. > NIST developed the FIPS 201 document, which establishes identification standards for all Federal employees and contractors who require physical access to Federal facilities and logical access to Federal information systems. > NIST provides further related technical implementation guidance for smart-card architecture and interfaces, in SP 800-73 (Interfaces for PIV), and for biometric interfaces in SP 800-76 (Biometric Data Specification for PIV).
Real-ID	> Passed May 11, 2005 > The intent of this Act is to allow DHS to set minimum issuance standards for state-issued driver's licenses and identification documents.	> Specifies that the cards be read by a common machine-readable technology. > While the Act does not require individual States to adhere to the Department of Transportation's driver's license specifications, the fact that citizens will be unable to use non-compliant licenses for Federal purposes (including air travel, opening a bank account, or collecting social security payments) provides incentives for the individual States to comply.

Identity Management Activities	
Current Identity Management Initiatives	**Initiative Description**
Nortel Government Solutions Identity Management Solutions Set	> Nortel Government Solutions is in the process of establishing an Identity Management Solutions Set. > Creation of an Identity Management Test/Demo Environment to test and evaluate leading IdM product sets, special focus on HSDP12/FIP 201-1 approved solutions.
GSA HSPD12 Qualified Integrator	> The Nortel Government Solutions Identity Management Team is in the process of preparing a submission to GSA to become a qualified HSPD12 with the focus on integration services. Anticipate qualified status before the end of calendar year 2006.
Nortel Technical Journal Article	> Dr. Alan Harbitter, Margaret Leary, and Thomas Casey contributed to the latest Nortel technical journal: Title Co-Author "Secure Information Sharing for U.S. Government," Nortel Technical Journal, Issue 3, March 23, 2006.
Nortel Networks R&D	> Nortel is in the process of testing and developing new software products that integrate the management and control of identities that exist at the network and application levels of an enterprise. > Nortel calls this more complete federation of identity: Unified Federated Identity Management. We believe that unified identity management is necessary to deliver the full benefit of FIdM. For instance, without unified identity management, true single sign on can not be achieved--a user will always have to authenticate first to the network and then to applications of interest. Further, network identity can include, among other things, a user's geographic location. > This information is useful to applications in tailoring information delivered to a user. We believe that unified identity management is an important and necessary concept as the network plays an increasing role in delivering information applications to geographically dispersed and mobile users. Nortel is leading the way in advances in federated identity research. > Nortel is developing new products that implement unified identity management and provide a more complete profile of the user. Unified Federated Identity Management increases the scope of functions that can be delivered and improves security and privacy.

Nortel Government Solutions' Identity Management Experience Summary

Customer	Experience Description
Social Security Administration (SSA)	> Provided support to SSA for its pilot program developing a federated model of the SSA's direct deposit application and allowing access to the application using a third party credential from Fidelity investments. > Worked with members of both the public and private sector from SSA, General Services Administration (GSA), and Fidelity Investments.
Department of Justice (DOJ)	> Developed U.S. Department of Justice supported information security framework for secure information sharing between Federal, state, and local law enforcement and criminal intelligence organizations. Federated identity management is a key component of the overall security framework.
DEA Diversion E-Commerce System (PKI)	> We have been working with the DEA's Office of Diversion Control for almost a decade supporting the implementation of a successful PKI system to support the electronic digitally-signed transmission of controlled substances and the electronic validation of these orders. This system has been in production since August of 2005 and has saved the industry over $5 Million and over 150,000 orders have been processed. This effort also included supporting an updated Ruling to permit electronic orders. This rule became final in April of 2005.
Department of Justice and Federal Bureau of Investigations Public Key Infrastructure (PKI)	> We were a key member of the team providing full life cycle services to the FBI and DOJ PKI efforts. These architectures were established to facilitate inter- and intra-agency information sharing. The FBI PKI has been deployed and is now operational. We have been recognized by Director Muller for our efforts.
DHS Transportation Security Administration (TSA) Airport Screeners	> Provide secure mobile solution for fingerprint processing via FBI Integrated Automated Fingerprint Identification System (IAFIS). > Authenticate candidates at each step of the hiring process and perform background checks (Recruitment).
U.S. Department of Justice Joint Automated Booking System (JABS)	> Standard infrastructure to share booking information among law enforcement (FBI, DEA, INS (former), USMS and BOP). > Conduit to FBI IAFIS. Criminal Background checks on detainees; share fingerprints and mug shot information across DOJ components (Law enforcement). > Booking system solution set (processing 45,000+ transactions per month). > Integration (1,000 + biometric capture suites deployed).

Nortel Government Solutions' Identity Management and Supporting Security Services Experience Matrix

Experience	DOJ JABS	DOJ PKI	DEA Diversion E-Commerce	SSA	FBI
PKI Design		●	●		●
PKI Development		●	●		●
PKI Integration		●	●		●
PKI Operations			●		●
SmartCards and SmartCard Management System			●		●
Security Policy Development, Implementation, and Enforcement			●		
Knowledge Based Authentication				●	
Consolidated Authentication				●	
Directory Services		●	●		●
Registration Authority Services			●		
System Administration			●		
Customer Relationship Management System Design, Development, and Operations			●		
Intrusion Detection			●		

Nortel Government Solutions' Identity Management and Supporting Security Services Experience Matrix					
Experience	**DOJ JABS**	**DOJ PKI**	**DEA Diversion E-Commerce**	**SSA**	**FBI**
Web Services, Web Development	●				
Electronic Workflow			●		
Biometrics	●		●		
Facility Access Control			●		
FISMA Compliance			●		
NIST Compliance		●	●	●	●
Continuity of Operations, Disaster Recovery			●		●
Incident Response			●		
WebTrust/Third-Party Certification			●		

For additional information

Larry Jurcich, IAED Vice President, larry.jurcich@nortelgov.com
Dick Thelen, SSC Center Director, dick.thelen@nortelgov.com
Thomas J. Casey, Identity Management Department Manager, thomas.casey@nortelgov.com
Theresa Nguyen, SSC Identity Management Senior Engineer, theresa.nguyen@nortelgov.com
Stuart Saiki, SSC Identity Management Senior Engineer/Developer, stuart.saiki@nortelgov.com
Steve Skordinski, SSC Identity Management Engineer/Developer, stephen.skordinski@nortelgov.com

Nortel Government Solutions, a network-centric integrator, is a trusted partner for government to support the livelihood, security, and well-being of its citizens. We deliver a comprehensive portfolio of technology and high-end services capable of meeting the demands of the most complex and important systems in the world. Headquartered in Fairfax, Virginia, Nortel Government Solutions engineers, deploys and manages mission-critical solutions for government, including homeland security, criminal justice and intelligence, defense and civilian agencies within the U.S. Federal Government and at state and local levels.

Nortel Government Solutions
12730 Fair Lakes Circle
Fairfax, VA 22033
877-NORTEL7
(703) 653-8000 phone
(703) 653-8001 fax

www.nortelgov.com

NORTEL
Government Solutions

Key Terms (Glossary)

There have been a number of glossaries developed providing definitions of terms associated with identity and related functions. This glossary was developed by ITAA, Information Technology Association of America, Identity Management Task Group. The Group is comprised of over 60 companies that are responsible for producing the majority of government credentialing and identity management programs at the federal, state, and local levels. Our members include those firms that specialize in the production of state-issued driver's licenses and identification cards; federal, state, and local smart card and identity credentialing programs; biometric device, algorithm, and middleware providers, RF technology, and background checking and identity proofing companies with expertise in all the facets of establishing and maintaining identity. The website link is included here ITAA Home.

Identity Management Task Group
Definitions

Glossary of Terms:

Access Control: The process of granting or denying specific requests: 1) obtain and use information and related information processing services; and 2) enter specific physical facilities (e.g., Federal buildings, military establishments, border crossing entrances).
Acquisition device: The hardware/sensors used to acquire biometric samples.
These would include finger sensors or readers, iris scanning devices, facial recognition cameras.
Algorithm: A sequence of instructions that tells a system how to accomplish some task. Cryptographic algorithms are used to encrypt sensitive data files, to encrypt and decrypt messages, and to digitally sign documents. In biometric systems, it is used to determine whether a sample and a template are a match.
Application Program Interface (API): Modular computer code that defines how a software application interacts with an application or device. For example, when used with biometric systems, it provides an interface between the application and the biometric device.
Authentication: The process of validating an identity (ensuring someone is who they say they are)
Authentication is generally done through the presentation of a credential (unique id, logon id) or token (SecureID, Smartcard). Primary authentication methods are:

- Access passwords (something the user knows)
- Access tokens (something the user owns)
- Biometrics (something the user is)

Authorization: Once an identity has been authenticated, the process of ensuring the identity has the proper access to a set of privileges. "Now that you know I am who I claim to be, can I get access to the systems for which I am authorized."
Automated Fingerprint Identification System (AFIS): A system originally developed for use by law enforcement agencies, which compares one or more fingerprints from an individual with a database of fingerprint images.
BioAPI: The API specification developed by BioAPI Consortium designed as a standard for serving various biometric technologies. BioAPI is a specification used to facilitate the use of different proprietary biometric products within the same application. It does not ensure interoperability between different proprietary biometrics.
Biometric: A measurable, physical characteristic or personal behavior trait used to recognize the identity, or verify the claimed identity, of an applicant. Facial images, fingerprints, and handwriting samples are all examples.
Biometric Template: A highly compressed and digitally encoded mathematical representation of fingerprint features stored for future verification purposes. Templates require less space to store than images, offer quicker matches, and are nearly impossible to reverse engineer.
Certificate Authority: A system that issues and manages digital certificates to individuals generally used in PKI.
Certificate Revocation List (CRL): In a system where digital certificates are being used to authenticate identity of users, the CRL is the list of certificates that have been revoked or expired. Certificates are checked against the CRL before access to a system is granted.
Claimed Identity Validation: The process of validating that a person is who they claim to be. May involve checks against public databases and biometric databases, authentication of breeder documents, and background checks.
Credential: An object that authoritatively binds an identity. In the cyber world it is the certificate or biometric, that binds you to the computer system; in the physical world it is a generally a card.
Contact & Contactless: In regard to Smart Cards, there are two ways for systems to read the computer chips on the card.
__ Contact – requires the user to insert the card into a reader where the smart chip has direct physical contact with the reader.
__ Contactless – requires the user to initiate a card read by holding it up in very close proximity to the reader. Contactless smart cards should not be confused with RFID technology that allows RFID chips to be read from a significant distance.
Digital Certificate: an electronic means of establishing your credentials. A digital certificate systematically binds an authenticated individual to a particular encryption key. That key can then be used to identify the individual online or in person. Digital Certificates are generally issued by a certificate authority (CA) and are a key component of PKI.
Encryption: The process of encoding or decoding information so people will be unable to read it. Generally a password or key is required to encrypt or decrypt the information.
Enrollment: The process of capturing an individual's biographic and biometric data for entry into an identification system.
False Accept Rate (FAR): is the probability of a random user, who is not enrolled, being falsely accepted by a specific system. Sometimes referred to as a false positive or false match rate.
False Reject Rate (FRR): The frequency (usually expressed as a percentage) at which enrolled persons are incorrectly rejected as unidentified or unverified persons by an authentication system.
FIPS 201: A standard published by NIST in response to Homeland Security

Presidential Directive 12 (HSPD-12) that establishes a uniform federal standard for Personal Identity Verification (PIV) of Federal employees and contractors.

Hash: the process used in encryption used to take raw data that needs to be encrypted and use an algorithm to turn it into encrypted data. Hash functions by their nature are one-way functions that are irreversible.

Identification: The process of recognizing the true identity (i.e. origin, initial history) of a person or item from the entire collection of similar persons or items.

Identity Management: The general practice of establishing, verifying, and managing the privileges associated with an individual's identity. Identity management involves the use of various technologies (i.e., biometrics, smart cards, digital certificates, PKI, etc.), and encapsulates the process of using identity traits to interact with systems or services.

Identity Proofing: The process of providing sufficient information (e.g., identity history, credentials, documents) when attempting to establish an identity.

Identity Verification: The process of confirming or denying that a claimed identity is correct by comparing the credentials (something you know, something you have, something you are) of a person requesting access with those previously proven and stored in a system and associated with the identity being claimed.

Logical Access Control: An automated system that controls an individual's ability to access one or more computer system resources such as a workstation, a network, an application, or a database, including systems which make use of encryption keys and/or digital certificates.

Match/Matching: The process of comparing biometric information against a previously stored biometric data and scoring the level of similarity.

Minutiae Points: Unique characteristics or identity points of a biometric. In a finger biometric unique lines, called ridges, occur on the fingerprint surface. The finger minutiae are the points where these ridgelines terminate or intersect one another.

Personal Identity Verification (PIV): The standard for identification mandated by HSPD-12 and formalized by NIST in FIPS 201 to establish a Government-wide standard for secure and reliable forms of identification issued by the Federal Government to its employees and contractors.

"Secure and reliable forms of identification" means identification that (a) is issued based on sound criteria for verifying an individual employee's identity; (b) is strongly resistant to identity fraud, tampering, counterfeiting, and terrorist exploitation; (c) can be rapidly authenticated electronically; and (d) is issued only by providers whose reliability has been established by an official accreditation process.

Physical Access Control: Refers to an automated system that controls an individual's ability to access a physical location such as a building, parking lot, office, or other designated physical space.

Public Key Infrastructure (PKI): The policy and procedures for establishing a secure method for verifying the authenticity of identities and exchanging information with in an organization, an industry or worldwide. PKI includes the use of certificate authority and digital certificates as well as all the hardware and software used to manage the process. For online transactions it is widely considered the most secure means of authentication the validity of an entity and the data contained in a transaction.

Response Time/Processing Time: The time period for an authentication system to return a decision on identification or verification of a biometric sample or other presented authentication data.

Smart Card: "A computer on a card" – a smart card is a card or token that contains a computer processor chip. Smart cards are unique among card technologies in that they have the ability not just to store large quantities of information, but also to execute complex processes directly on the card. In Identity Management systems, smart cards are used to store information related to identity and privileges, and to generate encryption keys for secure transactions. Smart cards are used in a wide range of applications globally such as: identification, health care, mobile telephony and banking. They have emerged as the card platform of choice for government ID projects, where a single card can carry information to support multiple applications, including: biometrics, digital

signatures, electronic keys, medical information and PIN validation. Data on smart cards can be fire walled off from other card applications to ensure that only authorized users can access the information.
Validation: The process of determining whether a credential that is presented is valid.
Verification: The process of comparing characteristics of a valid identity to those presented to the claimant in order to establish whether or not the identity is valid and can be bound to the identity claimant. When used with biometric systems, it is the process of establishing identity validity through the comparison of the verification with the enrollment template. Verification answers the question, "Am I who I claim to be?"

Common Components—definitions, explanations and links.

802.1x – 802.1x is an authentication standard for wired and wireless LANs, used to identify users before allowing their traffic onto the network. It can be used in wireless environments to authenticate users for more secure WEP, Wi-Fi Protected Access or 802.11i deployments. (http://www.networkworld.com/reviews/2004/1004wirelessgloss.html)

Cookies – Cookies are information stored on a user's computer by a Web Browser at the request of software at a web site. Web sites use cookies to recognize users who have previously visited them. The next time the user accesses that site, the information in the cookie is sent back to the user so the information displayed can vary depending on the user's preferences. (http://www.ask-edi.com/glossary.htm)

Digital Signature – A digital signature is like a paper signature, but it is electronic. A digital signature cannot be forged. A digital signature provides verification to the recipient that the file came from the person who sent it, and it has not been altered since it was signed. (http://sig.nfc.usda.gov/pki/glossary/glossary.html)

Digital Watermark – A digital watermark is an identification code carrying information about the copyright owner, the creator of the work, authorised consumers and so on. The watermark is invisible and permanently embedded into digital data for copyright protection and for checking if the data has been corrupted. By means of watermarking the work is still accessible, but permanently marked. (http://www.dig-mar.com/Commentaries/glossary.html)

FIPS (199-201) – [FIPS (Federal Information Processing Standards) are a set of standards] published by the U.S. National Institute of Standards and Technology, after approval by the Dept. of Commerce; used as a guideline for federal procurements. (http://www.orafaq.com/glossary/faqglosf.htm)

- **FIPS 199: February 2004**, Standards for Security Categorization of Federal Information and Information Systems
- **FIPS 200: March 2006**, Minimum Security Requirements for Federal Information and Information Systems
- **FIPS 201: March 2006**, Personal Identity Verification (PIV) of Federal Employees and Contractors

Higgin's Trust Framework -- Higgins is a software development framework that will enable users and enterprises to integrate identity, profile, and relationship information across multiple systems. Using service adapters, existing and new systems such as directories, collaboration spaces, and communications technologies (e.g. Microsoft/IBM WS-*, LDAP, email, IM, etc.) can be plugged into the Higgins framework. Applications written to the Higgins API can virtually integrate the identity, profile, and relationship information across these heterogeneous systems. A design goal is that Higgins be useful in the development of applications accessed through browsers and rich clients. [The] intent is to define Higgins in terms of service descriptions, messages and port types consistent with an SOA model and to develop a Java binding and implementation as an initial reference. (http://www.eclipse.org/higgins/faq.php)

HTTP – HyperText Transfer Protocol, the underlying protocol used by the World Wide Web. HTTP defines how messages are formatted and transmitted, and what action Web servers and browsers should take in response to various commands. For example, when you enter a URL in your browser, this actually sends an HTTP command to the Web server directing it to fetch and transmit the requested Web page. (http://www.saol.com/glossary.asp)

HTTPS – The HTTPS is the HyperText Transfer Protocol (HTTP) with the added option of SSL security. (http://www.saol.com/glossary.asp)

IEEE – The IEEE (Institute of Electrical and Electronics Engineers) is an organization of engineers, scientists and students involved in electrical, electronics, and related fields. It also functions as a publishing house and standards-making body. (http://www.orafaq.com/glossary/faqglosi.htm)

Kerberos – Kerberos is a network authentication protocol that was created by MIT. It is designed to provide strong authentication for client/server applications by using secret-key cryptography. The Kerberos protocol uses **strong cryptography** so that a client can prove its identity to a server (and vice versa) across an insecure network connection. After a client and server has used Kerberos to prove their identity, they can also encrypt all of their communications to assure privacy and data integrity as they go about their business. (http://web.mit.edu/Kerberos/)

LID (lightweight identity) Light-Weight Identity (LID) is a set of protocols and software implementations created by Johannes Ernst of NetMesh Inc. for representing and using digital identities on the Internet without relying on any central authority. LID supports digital identities for humans, human organizations and non-humans (e.g. software agents, things, websites, etc.) (http://en.wikipedia.org/wiki/Light-Weight_Identity)

LDAP – Light Weight Directory Access Protocol (LDAP) is an open network protocol standard designed to provide access to distributed directories. LDAP provides a mechanism for querying and modifying information that resides in a directory information tree (DIT). A directory information tree typically contains a broad range of information about different types of network objects including users, printers, applications, and other network resources. (http://www.microsoft.com/windows2000/techinfo/howitworks/activedirectory/ldap.asp)

Microsoft Identity Metasystem – The Identity Metasystem is an interoperable architecture for digital identity that assumes people will have several digital identities based on multiple underlying technologies, implementations, and providers. Using this approach, customers will be able to continue to use their existing identity infrastructure investments, choose the identity technology that works best for them, and more easily migrate from old technologies to new technologies without sacrificing interoperability with others. (http://msdn.microsoft.com/webservices/webservices/understanding/advancedwebservices/default.aspx?pull=/library/en-us/dnwebsrv/html/identitymetasystem.asp)

Microsoft Windows Communications Foundation (WCF) – The WCF is an incremental, yet evolutionary technology that brings all the formerly distinct and separate Microsoft connectivity technologies together under a single umbrella within the System.ServiceModel namespace. Included in WCF are Web services (ASMX), the Web service Extensions (WS*), Microsoft Message Queuing (MSMQ), Enterprise Services, COM+, and .NET Remoting. Having a single namespace that subsumes all of these into a coherent package is

enormously useful, and makes designing, developing, and deploying applications that require connectivity far simpler. (http://www.devx.com/dotnet/Article/29414)

PGP – PGP ("Pretty Good Privacy") is a powerful, free cryptography package. PGP lets people exchange files in a private, encrypted format, and also provides message authentication. PGP is called a public key system. Each person using PGP has two keys, a public and a private key. The keys are actually a digital signature, a small file with a stream of uniquely generated characters. The public key is widely distributed to any correspondents, and the private key is guarded with secrecy. An encrypted message in PGP is scrambled in a complex way to make it unreadable to anyone other than the intended recipient. You can use your private key and the recipient's public key to generate a message that can only be unscrambled by the recipient who has your public key as well as a personal private key. This allows you to easily exchange encrypted messages with anyone with whom you have exchanged public keys. (http://kb.iu.edu/data/afkr.html)

Public Key Encryption – Public Key Encryption is a type of cryptography also known as asymmetric cryptography. It uses a unique Public/Private Key Pair of mathematically related numbers. The Public Key can be made available to anyone who wishes to use it, while its holder keeps the Private Key secret. Either key can be used to encrypt information or generate a Digital Signature, but only the corresponding key can decrypt that information or verify that Digital Signature. The public key enables the encrypted document, file, e-mail or data stream to be deciphered using the related private key. Public-key encryption requires more computing power than symmetric-key encryption. To improve throughput, many systems use a public key to protect a symmetric key that, in turn, is used to protect the material. **(**http://isb.wa.gov/policies/definitions.aspx#IndexPQ)

Public Key Infrastructure (PKI) is the software and/or hardware components necessary to manage and enable the effective use of public key encryption technology, particularly on a large scale. (http://isb.wa.gov/policies/definitions.aspx#IndexPQ)

SAML – SAML (Security Assertions Markup Language) is a vendor-neutral, XML-based framework for exchanging security-related information, called "assertions," between business partners over the Internet. SAML is designed to deliver much-needed interoperability between compliant Web access management and security products. The result: Users should be able to sign on at one Web site and have their security credentials transferred automatically to partner sites, enabling them to authenticate once to access airline, hotel and rental car reservations systems through Web sites maintained by associated business partners, for example. (http://www.computerworld.com/developmenttopics/development/webdev/story/0,10801,73712,00.html)

SFTP – SFTP, or secure FTP, is a program that uses SSH to transfer files. Unlike standard FTP, it encrypts both commands and data, preventing passwords and sensitive information from being transmitted in the clear over the network. (https://kb.iu.edu/data/akqg.html)

Single Sign-on – Single sign-on (SSO) is mechanism whereby a single action of user authentication and authorization can permit a user to access all computers and systems where he has access permission, without the need to enter multiple passwords. Single sign-on reduces human error, a major component of systems failure and is therefore highly desirable but difficult to implement. (http://www.opengroup.org/security/sso/)

SSH (Secure Shell) – Secure Shell (SSH) is a secure way of transmitting data over TCP/IP networks from one computer to another. It utilizes strong encryption and authentication to ensure confidentiality, integrity, and authenticity of the transferred data. (http://www.ssh.com/products/ssh_secure_shell/)

SSL (Secure Sockets Layer) – SSL (Secure Sockets Layer) is the standard security technology for establishing an encrypted link between a web server and a browser. This link ensures that all data passed between the web server and browsers remain private and integral. SSL is an industry standard and is used by millions of websites in the protection of their online transactions with their customers. (http://info.ssl.com/Article.aspx?id=10241)

Strong Authentication – Strong authentication refers to systems that require multiple factors to identify users when they access private networks and applications. These authentication systems use advanced technology, such as token-generated one-time passcodes, to verify (authenticate) a user's identity. (http://www.securecomputing.com/index.cfm?skey=647)

WEP – WEP is short for Wired Equivalency Privacy and it is a security protocol for Wi-Fi networks. Many base stations have WEP turned off by default but users can change that setting. WEP, however, has known flaws that skilled hackers can exploit. (http://edition.cnn.com/2004/TECH/internet/10/25/glossary/)

WPA – WPA (Wi-Fi Protected Access) is a security protocol designed to create secure wireless (Wi-Fi) networks. It is similar to the WEP protocol, but offers improvements in the way it handles security keys and the way users are authorized. For an encrypted data transfer to work, both systems on the beginning and end of a data transfer must use the same encryption/decryption key. While WEP provides each authorized system with the same key, WPA uses the temporal key integrity protocol (TKIP), which dynamically changes the key that the systems use. This prevents intruders from creating their own encryption key to match the one used by the secure network. (http://www.iwebtool.com/what_is_wpa.html)

Standards

Mission/Objectives of ASC X9

The Accredited Standards Committee X9 (ASC X9) has the mission to develop, establish, maintain, and promote standards for the Financial Services Industry in order to facilitate delivery of financial services and products.

Under this mission ASC X9 fulfills the objectives of:

- Support (maintain, enhance, and promote use of) existing standards;
- Facilitate development of new, open standards based upon consensus;
- Incorporate nonproprietary items developed by other organizations where appropriate;
- Provide a common source for all standards affecting the Financial Services Industry;
- Focus on current and future standards needs of the Financial Services Industry;
- Promote use of Financial Services Industry standards; and
- Participate and promote the development of international standards.

X9 National standards:

Included here is a link to the ASC X9 Current Catalog and following is a list of standards available from the catalog.

X9 National Standards

TG-3 Retail Financial Services Compliance Guideline – Part 1: Online PIN Security and Symmetric Key Management

TG-4 Recommended Notation for DEA Key Management in Retail Financial Networks

TG-7 Initial DEA Key Distribution for PIN Entry and Transaction Originating Devices

TG-9 Abstract Syntax Notation and Encoding Rules for Financial Industry Standards

TG-19-1 Triple DES Validation System Procedures

TG-19-4 Secure Hash Algorithm Validation System (SHAVS): Requirements and Procedures

TR-31 Interoperable Secure Key Exchange Key Block Specification for Symmetric Algorithms

X9.8-1 Personal Identification Number Management and Security – Part 1: PIN Protection Principles and Techniques for Online PIN Verification in ATM & POS Systems

X9.24-1 Retail Financial Services Symmetric Key Management Part 1: Using Symmetric Techniques

X9.24-2 Retail Financial Services Symmetric Key Management Part 2: Using Asymmetric Techniques for the Distribution of Symmetric Keys

X9.30:1 Public Key Cryptography, The Digital Signature Algorithm

X9.30:2 Public Key Cryptography, The Secure Hash Algorithm

X9.31 Digital Signatures Using Reversible Public Key Cryptography for the Financial Services Industry

X9.32 Financial Institution Data Compression (Wholesale)

X9.42 Public Key Cryptography For The Financial Services Industry: Agreement of Symmetric Keys Using Discrete Logarithm Cryptography

X9.45 Enhanced Management Controls Using Digital Signatures

X9.49 Secure Remote Access to Financial Services for the Financial Industry

X9.52 Triple Data Encryption Algorithm Modes of Operation

X9.55 Public Key Cryptography: Extensions to Public Key Certificates and Certificate Revocation Lists

X9.57 Public Key Cryptography for the Financial Services Industry, Certificate Management

X9.62 Public Key Cryptography for the Financial Services ECDSA

X9.63 Public Key Cryptography for the Financial Services Industry: Key Agreement and Key Transport Using Elliptic Curve Cryptography

X9.65 Triple Data Encryption Algorithm (TDEA) Implementation

X9.68:2 Digital Certificates for Mobile/Wireless and High Transaction Volume Financial Systems

X9.69 Key Management Extensions

X9.73 Cryptographic Message Syntax

X9.79 Financial Services PKI Policy and Practices Framework PUBLISHED MARCH 2006 4 X9.80 Prime Number Generation Primality Testing, and Primality Certificate

X9.84 Biometric Information Management and Security for the Financial Services Industry

X9.95 Trusted Time Stamp Management and Security

X9.96 XML Cryptographic Message Syntax (XCMS)

ISO TC68 SC 2 Security management and general banking operations

ISO 9564-1:2002 1996

Banking—Personal Identification Number (PIN) management and security—Part 1: Basic principles and requirements for online PIN handling in ATM and POS systems

ISO 9564-2:2005 2001

Banking—Personal Identification Number management and security—Part 2: Approved algorithms for PIN encipherment

ISO 9564-3:2003 2000

Banking—Personal Identification Number management and security—Part 3: Requirements for offline PIN handling in ATM and POS systems

ISO/TR 9564-4:2004

Banking—Personal Identification Number (PIN) management and security—Part 4: Guidelines for PIN handling in open networks

ISO 10126-1:1991

Banking—Procedures for message encipherment (wholesale)—Part 1: General Principles

ISO 10126-2:1991

Banking—Procedures for message encipherment (wholesale)—Part 2: DEA algorithm

ISO 10202-1:1991/Cor 1:1999

Financial transaction cards—Security architecture of financial transaction systems using integrated circuit cards—Part 1: Card life cycle—Technical Corrigendum 1

ISO TC68 SC 2 Security management and general banking operations

ISO 10202-4:1996/Cor 1:1999

Financial transaction cards—Security architecture of financial transaction systems using integrated circuit cards—Part 4: Secure application modules—Technical Corrigendum 1

ISO 11131:1992

Banking and related financial services—Sign-on authentication

ISO 11568-1:2005

Banking—Key Management (retail)—Part 1: Principles

ISO 11568-2:2005

Banking—Key management (retail)—Part 2: Management techniques using symmetric ciphers

ISO 11568-4:1998

Banking—Key management (retail)—Part 4: Management techniques using public key cryptosystems

ISO/DIS 11568-4

Banking—Key management (retail)—Part 4: Management techniques using public key cryptosystems

ISO 11568-5:1998 WG12

Banking—Key management—Part 5: Life cycle for public key cryptosystems

ISO 13491-1:1998

Banking—Secure cryptographic devices (retail)—Part 1: Concepts, requirements and evaluation

ISO/DIS 1349-1: 2004

Banking—Secure cryptographic devices (retail)—Part 1: Concepts requirements and evaluation

ISO 13491-2:2005 Banking—Secure cryptographic devices (retail)—Part 2: Security compliance checklists for devices

ISO 13492:1998 Banking—Key management related data element

ISO/DIS 13492 Financial services—Key management related data—Application and usage of ISO 8385 (Revision of ISO 13492:1998)

ISO/TR 13569:2005 Financial services--Information security

ISO 15668:1999 Banking—Secure file transfer (retail)

ISO 15782-1:2003 Banking—Certificate management for financial services—Part 1: Public key certificates

ISO/NP 15782-1Banking—Certificate management for financial services—Part 1: Public key certificates (Revision of ISO 15782-1:2003)

ISO 15782-2:2001Banking—Certificate management—Part 2: Certificate extensions

ISO 16609:2004

ISO/NP TR 19039-1 (type3) Banking and related financial services—Part 1: Modes of operation validation system for the triple data encryption algorithm (TMOVS) requirements and procedures

ISO/FDIS 19092-1: 2003 Financial Services—Biometrics—Part1: Security Services

ISO 21188:2006 Public key infrastructure for financial services

ISO/CD 22895:2004 Cryptographic syntax scheme for financial services

STATE & LOCAL GOVERNMENT PROCUREMENT
Use of GSA Multiple Award Schedules

September 12, 2006

By Richard Pennington, McKenna Long & Aldridge LLP, Denver CO

This supplement to the September 12, 2006, NCMA Web seminar provides a state and local government perspective on the use of GSA Schedules. For vendors moving to or already in state and local government markets, GSA Schedules provide competitive opportunities. This supplement also highlights for state and local government members resources concerning cooperative procurements and the use of GSA Schedules to meet state and local requirements.

State and Local Indefinite Quantity Contracting

GSA Schedules are a type of indefinite quantity contracting. Indefinite quantity contracting is commonly used in public procurement by state and local governments.

State and Local Governments Use Blanket Purchase Agreements

Individual local governments or state departments sometimes establish open-ended purchase orders that do not commit to any quantity of purchase. They streamline the ordering process for individuals in local government offices or state departments.

But states also establish multiple award contracts: the California Multiple Award Schedule program is one of the best known. State contracts often are permissive in nature, meaning that departments or agencies have the discretion to not use the contracts. The contracts usually do not contain a minimum quantity either, another way (along with a "requirements contract") of establishing a contractual commitment with a vendor that may lead to more favorable pricing. Colorado calls these agreements "price agreements." Other states call them "state contracts." They all are a type of "blanket purchase agreement" as that term is used in the Federal Acquisition Regulations. The advantage to state departments is the ability to satisfy requirements above small purchase thresholds without having to use formal competitive processes like invitations for bids.

Local Governments Use State Contracts

Within states, local governments use the state contracts or price agreements established by the central purchasing office. Often local ordinances permit orders from the statewide agreements without having to otherwise conduct competitive procurements.

Authority to Conduct Cooperative Procurements

Procurement Statutes/Rules Vary Among State and Local Governments

The National Institute of Governmental Purchasing (NIGP) teaches public procurement practices that are familiar even to federal procurement professionals. Yet, each of the governmental entities has different rules. The most common core of law comes from the American Bar Association Model Procurement Code, but only about half of the States have adopted the MPC. Even in those states, the local governments and institutions of higher education may not be covered by the Code.

Cooperative Procurement Authority Varies Also

Outside of the cooperation between a state and its local governments, a threshold question is their authority to engage at all in cooperative procurements on a broader scale. GSA procurements would fit into this category. The states differ in their ability to conduct cooperative purchasing.[12] For states that have adopted it, the MPC grants states the authority to conduct cooperative procurements in the traditional sense of up-front cooperation. In other cases, state and local governments may have the express authority to conduct "piggyback" cooperative purchasing, meaning they can order from another public entity's contract if that entity permits it.

In a comprehensive 2006 whitepaper published by the National Association of State Procurement Officials about cooperative procurement,[13] NASPO found that a few states have no cooperative procurement authority at all.

State and Local Governments Cooperate on a National Level

NASPO's Western States Contracting Alliance is a consortium of chief procurement officials in the Western states that has developed a process for doing cooperative procurements in ways that meet the legal requirements in each of the participating states. Other organizations like U.S Communities (affiliated with NIGP) and Educational & Institutional Cooperatives Services, Inc. (affiliated with the National Association of Educational Procurement) have developed similar approaches to cooperative procurements to meet the legal and purchasing requirements of their members.

Authority to Use GSA Schedules

The Federal Government Allows Use of GSA Schedule 70

Section 211 of the e-Government Act of 2002 amended the Federal Property and Administrative Services Act to allow for cooperative purchasing for specified goods and services. This legislative change authorized state and local governments to use Schedule 70 to buy firmware, software, supplies, support equipment and services. But state and local governments still must comply with their own procurement laws. GSA's regulations permit negotiation of terms and conditions with state and local agencies that are necessary to comply with their laws. The

---

[12] National Association of State Procurement Officials, *2003 Survey of State Government Purchasing Practices*, available at www.naspo.org.

[13] National Association of State Procurement Officials, *Strength in Numbers: An Introduction to Cooperative Procurements*, February 2006, available at www.naspo.org, hyperlink to Whitepapers.

legislation made vendor participation optional, that is, they do not have to accept orders from state and local governments.

The Federal 1122 Program permits use of GSA Schedules

Previously, Congress had authorized the use of some GSA Schedules for the counter drug program, known as the Section 1122 Program. Each state participating in the 1122 Program designates a State Point-of-Contact[14] to administer the state's activities under the program. The state's point-of-contact under the program usually is the central state purchasing organization or a state law enforcement department. GSA has approved certain GSA Schedule equipment and the purchase of motor vehicles under the program. The states' points-of-contact are responsible for receiving orders from state and local law enforcement entities, and for determining that the items will be used for counter drug activities.

Not All State and Local Governments Can Use GSA Schedules

States having only traditional cooperative procurement authority – i.e. meaningful up-front cooperation – may not be able to use GSA Schedules without express statutory authority. The GSA as a practical matter cannot engage state and local governments in the up-front solicitation planning that is the hallmark of effective cooperative procurement. Some states solve the authority problem by passing express statutory authority to use GSA Schedules. Colorado used a different approach that illustrates the policy considerations in use of GSA Schedules. In 2004, Colorado amended its procurement code to permit "other procurement methods." The resulting regulations permit approval of use of a GSA Schedule after submission of a request for approval to the State Purchasing Director. The approval criteria include, among other things, the presence of competition and the effect on the local vendor community.

On the other hand, state and local governments already having "piggyback" authority can use GSA contracts. But the authority to use them, and whether their use is in the best interests of the state or local government, are different questions.

Whether to Use GSA Schedules

Will GSA Pricing and Terms Be More Favorable?

The whitepaper published by the National Association of State Procurement Officials discussed the use of GSA Schedules by the states. NASPO noted that GSA charges a fee, the Industry Funding Fee (IFF) that must be factored into the value analysis. Further, NASPO highlighted the need to analyze terms and conditions, because separately negotiated provisions may be needed to comply with state or local law. Finally, as in any blanket purchase agreement, sometimes aggregated purchases and traditional competitive solicitation methods may lead to more favorable rates and prices.[15]

GSA Schedules May Not Comply With State and Local Law

GSA Schedules often do not have the terms and conditions required by state and local law. Nonappropriation provisions, for example, are different for state and local governments. State and local law may require specific clauses regarding liability allocation. And disadvantaged business and other socioeconomic requirements often are different. The need to add these provisions may affect the willingness of vendors to make their Schedule pricing and terms available to state and local governments.

---

[14] For example, South Dakota's site is at www.state.sd.us/boa/opm/section_1122_program.htm.

[15] For an industry perspective on multiple award contracts, vendor willingness to participate, and the potential impact on pricing, see Jim Hiles, *Riding the Ramps of the Multiple Award Freeway,* CONTRACT MANAGEMENT (NCMA: September 2006).

Additional Resources

The General Services Administration provides information about the availability of GSA Schedules to state and local governments.[16] The National Institute of Governmental Purchasing offers training in the use of GSA Schedules by state and local governments.[17]

Key Points

- Know the limitations on authority to use GSA Schedules.
- The effective use of GSA Schedules and other cooperative procurements by state and local governments involve considerations that balance efficiency, equity, and potential for cost reduction.
- Know what terms and conditions would be required to make the GSA order comply with state or local law.
- Vendors and public procurement professionals must be sensitive to the issues involved in deciding whether use of GSA Schedules is in the best interests of state or local governments.

[16] At www.gsa.gov, hyperlink to GSA Schedules, then to Cooperative Purchasing.

[17] National Institute of Governmental Purchasing, *Federal Supply Schedule Contracting*, course available from www.nigp.org.

Case Study

United States Department of Defense (DoD) Common Access Card: Case Study and Technology Lessons Learned

Introduction

Increasingly Government organizations are facing the challenge of improving identity management within their mission areas through the use of more secure emerging technologies. The implementation of a smart card based secure identity system is one of these choices. This section of the paper provides a case study of the implementation of a smart card based identity program in the Department of Defense and addresses, at a high level, the issue areas that will commonly need to be addressed for a successful implementation. Many of these issue areas are shared with those facing private sector implementers but they are particularly cogent for those in the public sector. Programs in this sector can involve a range of implementations that are either government to citizen implementations or government to employee/contractor/trading partner implementations. Government to citizen implementations can be very large and visible programs involving a national identity card or a more limited scope program that may involve entitlements, benefits delivery or privilege verification (e.g. a driver's license) or a combination of these. Governments to employee applications involve secure physical and logical access and authentication for a department or agency – usually as part of a larger identity management capability. Public confidence, or employee confidence in the case of an employee program, is key to success. The successful navigation of the challenges results in building confidence in the program both by the participants and by the leadership of the agency required to do the implementation.

Background on US Department of Defense Program

In 1999, the US Department of Defense (DoD) began work on a program to issue a smart, common-access identification card to 3.5 million Active Duty, Selected Reserve, DoD civilian and eligible Contractor personnel. The Common Access Card, or CAC, as it is referred to, is a smart card program designed to serve as a standard DoD ID card, enabling physical access to buildings and controlled spaces, and for logical access to the Department's computer networks and systems. The driving factors for the development of this project involved issues of information assurance and the reduction of fraud associated with the existing Armed Forces ID card. A smart card would improve the security of physical and logical access and enable e-commerce to become a possibility. The subsequent reduction in paperwork and decreased transaction and business process time would lead to an increase in efficiency and, overall, reduce costs. .One challenge was to design an interoperable and secure multi-application smart card that would function as a military ID card and ensure it complied with the Geneva Conventions. Cost was also a consideration while addressing this challenge and while the DoD considered creating a proprietary government specific approach, they eventually decided to adopt best commercial off-the-shelf (COTS) products adapted to the DoD environment. The ultimate goal was to be able to use a CAC anywhere that the cards are accepted, regardless of which DoD component issued it. The 1,500 workstations issuing the military ID cards would need to be upgraded to issue the more secure smart cards and up to 200 additional registration workstations included to provide issuance to the military as well as the DoD civilian and contractor personnel that had not been served by the existing card issuance work stations. .Approximately 3.5 million participants are involved in the DoD's CAC program Active Duty Military personnel, Select Reserve personnel, DoD civilian employees and approved contractors are the initial recipients while the potential population is approximately eleven million – if the CAC is issued to retired military members and family members. The first Beta site was established at Quantico, Virginia, USA on October 2nd,

2000. By mid-2001, the CAC card was operational at 70 Beta sites. An accelerated rollout began. All work stations and sites were deployed by the end of May2003. As of August 2006, more than 11 million CAC cards have been issued at a rate of approximately10K cards per day. The cards have been issued on a decentralized basis at over 1,000 sites in 27 countries and 2,000 workstations.

Initial Technology Choices

Early in the program it was decided that the CAC would contain an integrated circuit chip – that is be a smart card. After assessing the token technologies and standards, the DoD decided to employ smart cards to obtain increased security. By combining such a large number of security features on one piece of plastic, the CAC would become one of the most versatile ID and access cards in the world. The decision to use smart cards over other token technologies was based on industry interoperability, commercial industry direction, economic considerations, multi-application capability, dynamic loading of applications, and post issuance capability. Smart cards provide the most comprehensive solution to a variety of applications and address the functional and technical requirements identified through the token strategy. Additionally, smart cards enable strong identification, digital signature, storage of demographic data, and Service specific applications. A final benefit offered by the smart card was that because of format, the card functions as an ID card as well as a physical and logical access card. The multiple technologies, such as ICC, bar codes and magnetic stripes, which are included on the card platform, also facilitated integration with the legacy systems providing a strong economic business case. So although alternative technologies were explored, the decision was that there must be a card form factor to satisfy the Geneva Convention requirements and that the smart card adequately provided the functionality envisioned for logical access and improved business process. In fact, the DoD had been experimenting with smart cards in personnel applications for many years. Other technology choices followed on from the smart card decision. It was quickly decided that the functionality requirements and the unforeseen requirements that could materialize based on the availability of the smart card platform dictated a multi-function smart card with a capable operating system that would allow additional functions to be added to the card, even post-issuance. At the beginning of the CAC program there were three operating system choices that were considered non-proprietary. The non-proprietary nature of the operating system was considered key to the vision of providing a capability that could be “any card, any reader, any where”. The choices were JavaCard from Sun Microsystems; Windows Powered Smartcard from Microsoft and Multos from Master Card. These three system provided a wide range of capability and acceptance. DoD settled on JavaCard simply because it provided the largest installed based, most mature specification, and was most widely implemented across card manufacturers. Additionally, JavaCard had the largest resource pool for programming talent. This choice was pivotal in providing functionality and lowering risk for the new card. With this choice work could begin on the development needed to run the DoD required functions on the card.

Of equal importance was the decision on the secure issuance of the card. Since the card would be carried by military members all over the world and would be used for logical access and Public Key Infrastructure (PKI) implementation, secure issuance and protection of the data on the card was a high priority. Unlike the choice of card operating systems, the choice was between building a capability for secure loading of the card or utilizing a member organization maintained specification. Global Platform had a widely adopted specification that would allow the payload for the CAC to be securely loaded from the card management system directly onto the card. The Global Platform specification proved to be a very good choice for the DoD. It provided a widely adopted and vetted specification, one that card manufacturers understood and had implemented on a variety of cards. In addition, the specification worked very well with the card management system which was developed by ActivIdentity. The secure loading of the card directly from the secure issuance server proved to be a very workable and secure method for personalizing the card and implementing the PKI. In

addition, the Global Platform specification continues to be well maintained and continually evolving to ensure the security of the card.

Card Content and Card Edge Standards

The first challenge in the design and implementation of secure identity solutions is the identification and integration of standards into the design of the program. Historically, the introduction of smart card based identification card programs have been hampered by the choices that had to be made between competing mainly proprietary based solutions. The smart card manufacturers used to vertically integrate their offerings so that their cards, card applets, network and client software, and card readers all worked with their cards – but not with anyone else's. This worked when smart card solutions were fielded within one company but were particularly poorly suited to government applications. Government applications were suited to standards based implementations and the number of standards in this area is growing quickly. When initial decisions were being made on the CAC, card edge standards that were applicable to a government program of this size did not exist. But since the power of standards was widely recognized, the DoD along with the General Services Administration (GSA) and industry partners came together to develop the first Government Smart Card Interoperability Specification (GSCIS). This initial specification set the stage and began the process of standards being an integral part of government smart card programs. The government manager can now specify a number of recognized standards which will result in a much abbreviated and more precise procurement cycle. Standards can be formal, blessed by a US or international standards body; vendor based, for example the Sun Microsystems specification for a Javacard; or contributor or consortium based, for example the Global Platform specification. Using a combination of these standard specifications allow the government manager to have more control over the technology, more competition, and the ability to go for best of breed solutions in the parts of the identity infrastructure knowing that the parts will work together once assembled.

For implementations in the US, a first point of departure is a review of Federal Information Processing Standard (FIPS) 201, which is the recently released standard that addresses a whole range of issues surrounding the design and implementation of a smart card based secure identity system. FIPS 201 is especially useful because it details a business process that would be part of the secure identity program. It is not just the issuance of the card that matters, but the entire process of identity vetting and identity management that makes the system secure. FIPS 201 was developed by the National Institute of Standards and Technology (NIST). NIST has supplemented FIPS 201 with a number of technical standards that provide the detail on the technical standards that must be met to be fully compliant with the standard. For example, NIST Special Publication 800-73 addresses Interfaces for Personal Identity Verification**;** NIST Special Publication 800-76 specifies technical acquisition and formatting requirements for the biometric credentials for FIPS 201.

Distributed versus Centralized Issuance

An additional technology decision which is important to the design of the security of the system and integral to the customer service aspects of the system involves the decision on the business process associated with issuing the card. The issuance of high security identity card requires a face to face authentication of the individual and the proofs of identity needed to ensure a high degree of confidence in the identity of the applicant. The business process and the nature of the card may dictate whether the individual leaves the face to face interaction with a card, must come back again later to receive the card, or will receive the card in the mail. In the case of DoD, the decision was made initially that the ideal situation, given the wide dispersion of our workforce, was to have the card issued in real time and provide it to the individual in a single visit. This decision rested on the fact that all potential recipients for the card had been vetted prior to showing up for the card and that an independent confirming record existed in the enterprise "enrollment" database and this record was available at the time that an applicant applied for a card. Of course, in the case of individuals who

already have a card, the enrollment database also contains confirming biometric information that can assure that a card that is being reissued because it was lost or had expired, is being issued to the same person. The distributed issuance decision brings with it a more complex and challenging technology requirement. Secure issuance must extend remotely over wide are networks and high capability card printers and encoders must exist at each issuing location. For DoD this meant about 1000 locations in 27 countries. But since the need for the card was immediate, and physically getting a card to some locations required time and logistical planning, the distributed option was the only practical one. One additional factor was to engineer the card management software to provide the needed payload to the card in a reasonable time. This was complicated by the interaction needed to generate keys and certificates for three PKI keypairs in a real time interaction with DoD's Certificate Authority. In fact this model work well with the data collection, identity confirmation and card issuance taking about 15 minutes.

Later on in the program, DoD added a central issuance facility to the program. This approach is used only in situations where a mass issuance is needed for lots in individuals located in relatively few locations. The classic application for the centralized model is for recruits who show up in large numbers for basic training. The DoD experience provides many lessons learned on both approaches and the fact that both central and distributed processes exist in the same program is unique.

Linking to the Existing Infrastructure

Most organizations do not start a secure identity program with a "clean slate", they have existing systems in place to do some of the functions that are needed for an end-to end identity system, and, in fact, these legacy systems do many more functions as well that are integral to the business process. The option of ripping these systems out and replacing or reengineering them is not either practical or smart. This was the case for DoD as well, DoD had already built an effective infrastructure for managing employees: the Defense Enrolment Eligibility Reporting System (DEERS), a massive database of benefits and other personnel information for 23 million active and retired DoD employees. This database would serve a dual function in the new system – it would be modified to become smart card "aware" and could be used to track the card content and related data; second, the DEERS database would serve as the enrollment database and store all information related to the person and the card. In the DoD model, this central database would also store biometric information. In addition, this database would be linked to the underlying personnel databases that would update it in the case of any changes in the affiliation of the individual with the DoD. Based on these updates, the identification card and its associated privileges could be revoked. The DoD also had a system that linked to the DEERS database and was used for identity card issuance. This system was called the Real-time Automated Personnel Identification System (RAPIDS) and it was used for updating the DEERS database and issuing laminated paper IDs with bar codes for military personnel, retired military members and family members of those groups.

The challenge was to interface the new smart card issuance infrastructure to these existing systems with out impacting the production systems and without extensive reengineering. The solution for DoD was the insertion of a card management and issuance system and its integration with the RAPIDS system. The new system allowed for the continued issuance of the existing card to certain populations (retirees and family members) who were not scheduled to get the new smart card. In practice, this strategy worked very well and minimized the impact on the existing production system while inserting a secure smart card issuance in the middle of the existing suite of software. Once integrated, the entire end-to-end system was evaluated to ensure that it met security requirements. Of particular interest is the security surrounding the handling, initializing, and personalizing of the smart card chip. The provisioning of PKI was also very closely scrutinized to ensure that the key generation occurred on the card for the non-escrowed key pairs, and that the private key was securely injected into the card in the case of the escrowed key pairs.

Status of the Program

The DoD Common Access Card program remains the largest and most comprehensive secure identity program in the US. As of September 2006, more than 11 million cards have been issued under the program and at any one time almost 4 million people carry valid Common Access Cards. Use of the card continues to grow, as the power of this vast infrastructure gets further exploited by DoD leadership. Most recently, and because of the maturity of the CAC program, the entire Department was ordered to move to mandatory PKI authentication for logical access and web access. Mindful of the success of the DoD program, Homeland Security Presidential Directive 12 mandated a secure identity program for the entire Federal establishment. While the technical standards for HSPD-12 differ in detail from the DoD implementation, DoD will continue to push ahead to evolve their program to provide more functionality and greater security. At the same time, DoD will manage its program to bring it closer to the HSPD-12 standard so that interoperability will be assured. DoD aims to preserve the functionality of the CAC and its innovative use of permissions and biometrics while at the same time achieving FIPS 201 compliance.

Additional Lessons Learned

Some key lessons learned from the implementation experience stem from decentralized issuance. In circumstances where cards are issued through a number of sites, a good roadmap identifying different communication types involved and maintaining control over firewalls are critical factors to make integration more seamless. The DoD identified a need to improve the speed and reliability of the DEERS/RAPIDS issuance portal. Maintaining connectivity between the RAPIDS workstations and issuance portals is vital to streamline the issuance process. When connectivity failed, stations were unable to issue CAC's, and at times, congestion at the portal significantly slowed down the issuance process. User acceptance and "buy-in" is another critical success factor. To ensure the migration to the new CAC card was smooth, it was essential that users were educated about PKI, card functionalities and the goals of the program. Implementation displayed the need to provide greater training and help desk assistance to users. Some end users reported they were not aware when they were performing PKI functions properly. A comprehensive public relations effort to ensure that the users of the smart cards are aware of their issuance ahead of time to facilitate the transition process would permit all system users to fully capitalize on the enhancements provided by the ICC technology. The implications for this program are already spreading beyond the DoD. Private industry is adopting a similar model to provide an improved cyber identification credential for commercial and industrial e-commerce applications.

Privacy

The technical implementation of privacy requires the same skills and technical means as security. It requires the ability to control information and access to that information and plays an integral role in technical implementations of online and offline identity systems. Citizens expect, regulations require, and prudence demands that identity systems meet the requirements of privacy for those subject to the systems. Still, failures occur. What is the concept of privacy and why is it so important in identity systems?

Ari Schwartz, Deputy Director from the Center for Democracy & Technology in testimony before the House Committee on Government Reform Subcommittee on Government Management, Information and Technology on April 12, 2000, stated, "a starting point for thinking about privacy online should be individuals' long-held expectations of autonomy, fairness, and confidentiality". As a starting point, this very concept carries well into the world of identity.

In the book "Identity Crisis", Jim Harper advocates lowering the amount of identity data divulged by individuals and collected by institutions[18]. This one fairly simplistic approach could produce tangible benefits to identity system users and providers. While by no means a panacea, this concept enables the identity providers to begin not just thinking about mitigating the risk, but lowering the overall amount of information *requiring* mitigation.

- Collect and maintain less information in identity systems.

The Office of Management and Budget provides salient information on a number of different privacy points as they relate to protecting personal privacy in interconnected systems. Actions such as performing Privacy Impact Assessments and gaining consumer consent can go a long way towards privacy security.

- Perform privacy impact assessments.
- Explain usage and gain consent.

Effective control systems internal and external to the identity system can prove invaluable to reducing the impact of certain types of losses. Separations of duties, logically or physically, provide a robust mechanism for thwarting a considerable threat to privacy, insider fraud. While more appropriate to the enrollment and verification process requiring different authorizations to complete a component process in an identity system reduces the potential for fraud, by simply requiring the collaboration of more individuals inclined to fraud.

- Separation of duties.

This document does not endeavor and cannot provide an answer to every issue concerning privacy that might arise in specific implementations of identity systems. There is however, a wide range of government, private sector, and citizen based groups providing a wealth of opinions on privacy. While this list is by no means comprehensive, it provides a starting point for researching the implications for identity systems with respect to individual privacy.

- http://www.nist.gov/
- CSPRA.ORG
- http://www.whitehouse.gov/omb/privacy/personal.html
- http://www.whitehouse.gov/omb/privacy/website_privacy.html
- http://www.aclu.org/privacy/
- http://www.cdt.org/

[18] Harper, Jim. Identity Crisis: How Identification Is Overused and Misunderstood. Cato Institute: Washington D.C., 2006.

- http://www.cpsr.org/
- http://www.eff.org/
- http://www.epic.org/
- http://www.privacyrights.org/
- http://www.privacy.ca.gov/recommendations/recomend.htm

This partial list should provide the reader with again, a starting point for delving deeper into the privacy issue and in determining the best process, people and technology solution to mediate the privacy issue.

The Platform for Privacy Preferences offers several links to implementations that deliver on privacy solutions. More information can be found at http://www.w3.org/P3P/implementations.html.

Specific implementations of technology provide the tools for helping solve the privacy problem. Tools such as:

http://www-306.ibm.com/software/tivoli/products/privacy-mgr-e-bus/