

Identity and Access Management Supports Governments Worldwide

Author

Steve Hutchens, CISSP
EDS Global Government

Governments around the world share a common need to provide a variety of services, including the protection of citizens and of critical infrastructures such as finance, healthcare, transportation, public safety and utilities. The proper identification of individuals and beneficiaries of services is essential to effective government service delivery and operations. In the areas of government healthcare and human services, for example, proper identification of beneficiaries is necessary to ensure that those who are eligible for services do, in fact, receive the appropriate levels of service. Incidences of fraud and abuse within a social services context can cost governments several hundred million dollars per year. Identity management technology can provide an effective solution to minimize fraud and provide more efficient service delivery.

Similarly, governments today must deal with increasing threats from criminals and terrorists who pose risks to citizens and critical infrastructures. To help counter such threats, countries around the globe are implementing electronic credentials to support border and immigration security, citizen identification, government services (such as welfare, healthcare and education), and armed forces membership. These credentials present outstanding opportunities for supporting service delivery, while also creating a situation that begs for greater cooperation between agencies within a government to minimize duplication and waste of precious public resources. The idea that a single citizen card would facilitate disparate uses – for example, serving as personal identification, driver’s license, passport, healthcare card, educational identification, and even an electronic purse – presents the possibility of tremendous savings while providing identification accuracy with much stronger authentication. As governments struggle to address these concerns, solutions are emerging in

the form of information technology-enabled identity management.

“An ‘open door’ world in which federations interoperate without friction is a pipe dream. Trust among relying parties in any federation is built on agreement regarding process and controls for identity verification, credential issuance and use, back-end transaction integrity, and anomaly detection.”

Kreizman, et al., “Findings from the Gartner 2006 Global Research Meeting”¹

Establishing “positive identification” of individuals is clearly a significant mission of most countries today. Government agencies require some form of identification from all citizens who receive services. Each agency has unique requirements, but they share a need for common and basic information, such as an individual’s name, social security number (or equivalent unique identifier),

address, date of birth, phone numbers and account numbers. Today, each agency works independently to verify and store this kind of information about individuals in an agency database. Imagine the potential value that would be created by government if agencies would agree among themselves upon common identification elements and accept the same credential.

The concept of a “federated” identity credential provides a point of convergence based upon recognized standards and interoperable capabilities. Ultimately, trust must be established between cooperating agencies for a true federated identity credential to be successful.

Citizen concerns over personal privacy and security create unique challenges that must be met if both government and citizen are to benefit from identity management programs. These topics will be addressed as part of a multifaceted review of social, business, technology and process considerations for identity and access management systems.

This journal represents a collection of articles that are intended to be thought-provoking and which address many of the real-world challenges of identity management for global governments. Relevant business contexts and social interpretations of the role of identity management in society and government will be explored. There are no simple answers to these challenges, but advances in information technology and, in particular, identity management do offer hope toward a more integrated and effective solution. Each article in this journal provides a unique perspective into government applications of identity management to improve service delivery.

Incidentally, based upon recent legislation that drives the demand for and security of stronger identity and access management systems, the United States serves as a central example in some of the articles. Topic selection for the journal has to some extent been guided by the pressing nature of these very near-term implementation deadlines and challenges currently faced by the United States federal government, as well as the individual state and local governments. Other countries may be considering (or may already have in place) comparable legislation to address similar concerns. Globally, governments are trying to address the increasing flow of people across borders for visit or immigration. As populations grow, the increased demand for government services will require a more secure and efficient system for personal identity verification.

In the United States, recent legislation has established that digital identity credentials are not just desired but will be absolutely required for citizens to board airliners or gain entry to federal government buildings. The passage of U.S. legislation such as the Homeland Security Presidential Directive 12 (HSPD-12), the Real ID Act and the Privacy

Act illustrates how the U.S. government is attempting to establish the value of electronic identity credentials to support essential services. Similar legislation from the Department of Homeland Security for both the Transportation Worker Identification Credential (TWIC) and the U.S. Registered Traveler program specifically requires individuals involved in commercial transportation to have stronger identity credentials supported by appropriate background investigations. David Troy's paper explores some of the implications of HSPD-12 and the opportunities it creates.

The United States Real ID Act provides a unique opportunity for state governments to establish one common identification credential that will both meet the requirements of the Real ID Act and offer tremendous cost savings to every other agency that agrees to accept the same identification card. The article "Real ID is Identity Management," by Paul Mrochinski, provides an overview of the legislation and offers insights about what the Real ID Act means for states. This article will also address how the Real ID Act can save the taxpayers both money and time.

Governments provide significant social and healthcare services to citizens based upon established individual needs. The process of identifying and verifying that eligible individuals do, in fact, receive the appropriate services presents significant challenges. Fraud attributed to the exploitation of government social services causes financial loss to taxpayers while preventing those in need from receiving necessary care. Can identity management make a positive impact in the areas of eligibility determination and verification? John Petraborg and Diane Scott's article explores the challenges and recommendations of identity management applications to improve service delivery while reducing

the potential for fraud and abuse of government services.

The judicial system, including law enforcement, exists to protect citizens, deter crime and arrest criminals, and to provide a judicial process leading to incarceration of convicted criminals. Offender management systems must support all the judicial processes that are required to maintain control of those incarcerated. The offender management system provides a more streamlined and coordinated approach, from arrest to incarceration to parole and reform. Ensuring that the correct individual is managed and monitored through this process is vital to successful criminal justice systems. Jim Pauli's article will explore the use of identity management in offender management and present a case study of a successful implementation.

This journal and the articles it contains provide a unique and timely perspective on the value of integrated identity and access management systems. The articles selected represent some of the most complex and challenging areas of government where identity verification and identity management actually drive the services delivered. As governments worldwide consider recent advances in information technology, security and identity management, these articles offer insight, experience, lessons learned and practical case studies that illustrate demonstrated benefits. Consider these articles – particularly their perspectives on identity management's role in establishing true savings of time and resources and in producing real benefits for citizens – our latest contribution to the thought leadership of identity management. It is our hope that these articles will provide true value to governments and the people they represent as we all work to improve communications, enhance service delivery and provide safer communities for our citizens.

The Basics and Beyond: A Primer on Identity Management Technology

This paper will explore enabling technologies, such as username/passwords, smart cards, and biometrics, and will discuss how these elements can be applied to build a robust identity management system. A stronger identity management system can help counter many of the real world challenges and concerns discussed in the introductory portions of this journal. A wide range of technical concepts relate to identity and access management, and while a complete technical overview is beyond the scope of this paper, a brief review is necessary.

In short, this paper will provide a review of basic concepts, terminology and applications of identity and access management. This review is intended to provide a common base of reference as we explore identity and access management technology and principles. In addition, this paper will also present various aspects of the business processes, technologies and applications that are necessary to support an identity and access management system. Those who already have a good working knowledge of identity management principles and technologies may find this section useful as a review; otherwise, they may wish to proceed to the next article.

Author

Steve Hutchens, CISSP
EDS Global Government

Identity management (IdM), or identity and access management (IAM), includes the relevant business processes, procedures, standards and technology to establish an individual's "digital identity" to support electronic applications. Technologies such as smart cards, biometrics (including fingerprint recognition, facial recognition, hand geometry and iris recognition), security tokens, and access control devices are integrated in accordance with industry-recognized standards to support the operation of identity management systems. The essential functions of an identity management system include the basic operations of individual pre-enrollment, enrollment, credential issuance, credential maintenance and credential revocation. Nevertheless, the important point to remember is that identity management is a security concept supported by identification and authentication tools that may range from very basic identification cards – that is, non-smart cards that may feature only the card-holder's photograph and name – to very advanced, multi-factor (also called "strong") security credentials.

The specific standards, processes and technologies needed to implement an identity management system will depend upon the business context in which the digital credentials will be used. Some business contexts may require nothing more than a basic identification card, while others will require the combination of smart card, biometrics and passwords or personal identification numbers (PINs).

There are many terms associated with identity management that may not be entirely familiar to technology professionals. Identity management represents a subset of information security principles and processes that support authentication, authorization and non-repudiation, which are described in detail below. A well designed and implemented identity

management system will provide an integrated solution to address all three principles. Beyond authentication, authorization and non-repudiation, we will consider smart cards and biometrics in more detail to explain why these technologies work better together than they do separately. Next, we will explore the importance of risk management in establishing the correct approach and levels of security that will address the appropriate threats or vulnerabilities. Finally, no discussion of identity management would be complete without a review of the security versus privacy concerns of citizens.

AUTHENTICATION, AUTHORIZATION AND NON-REPUDIATION

Authentication is the process by which an automated system can verify – with certainty – that the individual is the person he or she claims to be. Consider as an illustration a scenario in which John Smith is registered as a valid user of a computer system. When John begins access to the computer system, he may be prompted to enter a username (a name by which the system can recognize him) and a password or PIN (a unique word or phrase that should be known only by John). The simple username and password are the most common methods of authentication to computers around the world.

Authentication is the process by which an automated system can verify – with certainty – that the individual is the person he or she claims to be.

Once the authentication process is completed, users may gain access to system resources and privileges for which they have been "authorized" by a systems administrator. The authorization process depends upon proper authentication to determine which resources and applications an individual user may access on a given system. To prevent unauthorized access to system resources, a strong authentication system must be considered and implemented.

Authorized users may engage in a variety of electronic activities, including sending e-mail, conducting online transactions, maintaining databases and supporting software applications. In practice, non-repudiation is analogous to an electronic audit trail through which an individual's actions cannot be denied. To return to our earlier scenario, let's say that John Smith sends an e-mail to his staff about an upcoming corporate meeting. The authorized user – John – of a corporate e-mail system sent a message that was recorded with date, time and other identifying information, and thus it cannot be denied that John sent the message. Non-repudiation forms the basis for audit and control and is an essential information security principle.

Achieving authentication through the use of a username and password combination alone is called "single factor" authentication. A factor is based upon a unique combination of elements that can be attributed to an individual user. "Something you know" – in this case, a password – is unique and therefore can be used to validate that John is who he claims to be and that he is also a valid user of the computer system.

The introduction of smart cards and electronic tokens add a second factor to support authentication processes. Smart card technology allows a system to electronically store a significant amount of information that may be used to support

the authentication process and improve the overall security of an information system. Two-factor authentication is possible with the addition of “something you have” – that is, a smart card or token (an electronic key that has limited storage but can support a unique number generator – often synchronized to a known computer server source). With the username/password combination (something you know) and the addition of a smart card or token (something you have), security authentication is supported by a two-factor process. An individual attempting to masquerade as an authorized user must now have both the username/password and the token belonging to a legitimate user to gain access.

With the addition of biometrics stored on a smart card (which have sufficient storage to store biometric data files) the authentication process is even stronger. The combination of “something you are” – such as a fingerprint, a facial image or an iris image – establishes a much higher level of verification that an individual is who he or she claims to be. This additional element, that of a biometric combined with the smart card, establishes a “three-factor” authentication process and substantially improves the overall security of a system. An individual attempting to masquerade as an authorized user must now have the username/password, a token and the physical characteristic represented by the legitimate user’s biometric to gain access. Consequently, access by unauthorized users becomes very difficult indeed.

The security of single-factor authentication is limited. Simply by observing an individual enter his or her username and password, an unauthorized user can compromise the system by masquerading as that individual and entering the same information to gain access. Therefore, single factor authentication is not as secure as the other

two methods. Two-factor authentication improves security because to masquerade as an authorized user, the individual would need to know the username/password combination in addition to having possession of the token or smart card. To obtain both of these elements is more difficult to do and

Standards have improved significantly over the past five years, and interoperability is becoming better each year. Currently, industry standards are driving the way to improved interoperability and more competitive costs per card.

would require that the token be removed from the possession of the valid user. A three-factor authentication system requires that the username/password combination, the token or smart card, and the exact duplicate of the individual biometric be compromised before a masquerade could occur. While someone who intends to breach system security may manage to observe another person’s username/password and may also be able to steal the corresponding token or smart card, creating an exact duplicate of another’s physical biometric is virtually impossible.

By establishing stronger authentication of the individual through three-factor authentication, the corresponding strength of the identity management system can mitigate the occurrence of imposters. The combination of smart cards or tokens with passwords or personal identification numbers along with biometrics (fingerprint,

iris scan or facial recognition) can significantly improve both speed and accuracy for positive identification of individuals. The choices for strong or weak authentication are driven by business or mission requirements and the value of the access in support of information sensitivity.

Next, we will review the role of smart cards in an identity management program. Smart cards provide a very flexible and effective storage medium that can improve the level of security and access control. Using well-recognized standards, smart cards can be applied in a variety of business processes, providing a very cost-effective solution. Smart cards represent the essential medium to a strong authentication system with the ability to store multiple biometrics and to support the processing of identity information.

SMART CARD TECHNOLOGY

Smart card technology has been around for a number of years, but was not widely used due to the relatively high cost per card. In addition, proprietary vendor technology (involving cards, readers and storage mechanisms) has proven challenging for governments that require a fully interoperable smart card system that will be shared among various departments or agencies. However, standards have improved significantly over the past five years, and interoperability is becoming better each year. Currently, industry standards are driving the way to improved interoperability and more competitive costs per card.

The selection of specific smart card technology is driven by user requirements and the amount of storage that is required on each card. Identity card systems that utilize a biometric stored on the card will have greater storage requirements than a smart

card with limited information, such as user account numbers or similar text information. As a government agency explores smart card technology and its uses, consideration must be given to the differences between “contact” and “contactless” smart cards. The major difference is the ability to simply pass a card in close proximity to a reader device (contactless) where the information is transmitted in a wireless mode to the reader. This type of technology is also referred to as a “proximity” card because the user only needs to swipe the card past the reader or very close to the reader surface, usually within about four to six inches.

A contact smart card must be physically inserted into a card reader and thus requires a bit more time to place the card into the reader and to have the reader retrieve the necessary information. The contact card is considered to be more secure since no information is transmitted in a wireless mode and is thus not vulnerable to a remote reader that could attempt to hijack the authentication information in transit.

BIOMETRIC TECHNOLOGY

The parallel introduction of biometric technology with smart card technology is a perfect fit to address identity management system security challenges. The smart card is a medium that is capable of storing multiple biometric information files, or signatures. Biometrics are obtained by taking a measurement or image of some common physical attributes of an individual. For example, fingerprint biometrics involve capturing an image (one that is similar to a fingerprint image taken by security or police departments) that can be converted into an electronic signature file. The exact science behind biometric technology devices is beyond the scope of this article. In brief, however, a fingerprint image can be converted into a digital image and then stored on an electronic device such as a

smart card, disk or other digital medium. Once the image is captured, a mathematical algorithm is used to process a reference to the fingerprint image and a resulting “signature” is established. Just as an individual’s fingerprint is unique, so too is the resulting signature file that is calculated based upon that unique image.

The principles of taking a biometric – taken typically from a fingerprint, iris, retina, face or hand – and converting this physical attribute into an electronic signature file are fairly similar. The science and the exact algorithms are technically different, but that again lies beyond the scope of this article and is more relevant to the type of biometric selected to support the identity management system. Simply consider that a unique signature file can be established in reference to an individual and thus can be used to improve the overall security system. Why, then, doesn’t every computer system require a biometric to validate an authorized user? There is no single answer, but certainly cost, accuracy and application integration are important factors.

Users of computer systems that require biometrics often share a common concern, or even fear, regarding the use of technology and the resulting use of biometric information. There may be a fear of the biometric capture process, concern about the potential uses of this biometric information, or an impression of intrusion of privacy. Many individuals fear “intrusive” biometric technology, such as retinal scanning, but accept “non-intrusive” technology such as facial recognition. Retinal scanning requires the individual to place his or her eye close to a camera that will shine a light and capture a digital image of the retina. This causes concern for some individuals who fear the physical effects of using this capture process (for example, the effects of shining light in the eye or of placing one’s eye on the same reader used by others).

“Non-intrusive” technology, such as facial recognition, involves using a digital camera to capture a facial image at a distance (often three to ten feet) under fairly benign lighting conditions. Fingerprint biometrics are considered one of the most acceptable and least intrusive technologies for common identity management systems.

The speed and accuracy of each type of biometric technology create trade-offs in efficiency and risk. Security processes must take risk into account as an element of exposure that could result if an unauthorized user is mistakenly allowed access to sensitive information because of failures in the identity management system.

RISK MANAGEMENT

Risk management involves the statistical evaluation of the identity and access management system’s capability to accurately identify authorized users. Risk management for identity credential recognition must address the issues of “false positives” and “false negatives” with regard to preventing or allowing access by an authorized user. A false positive may occur, for example, when an access management system recognizes as an authorized user someone who is not, in fact, an authorized user. Similarly, a false negative occurs when an authorized user is denied access.

Tradeoffs in security system characteristics must be addressed as part of the overall security risk management program development. Risk management considerations for identity management are driven by security policies and procedures that are, in turn, based upon business or mission requirements. The level of security and the sensitivity of information establish the requirements and challenges that must be addressed through proper selection of authentication mechanisms. Multiple biometrics offer significant improvements

in overall system performance and risk management, with the proper combination of smart cards with multiple biometrics offering the most secure and effective identity and access management system.

SECURITY VERSUS PRIVACY CHALLENGES

The concept that strong security policy can succeed through the implementation of equally strong authentication processes is commonly accepted among government agencies that deal with national security information. The individual is often the subject of the debate over security versus privacy, where perceptions of information technology, smart cards and biometrics can often be seen as contributing to the exploitation of individual privacy. In an identity management context, can these two concepts coexist, and can systems be implemented in a way that protects individual privacy of information while also improving information security?

Information security is fundamentally a process whereby sensitive information is maintained in a confidential manner through the implementation of appropriate security policy, processes and technology. However, most citizens and government employees are concerned that their “sensitive information” can be compromised when too much of this kind of information is collected and is then analyzed beyond its intended scope. When data such as name, address, date of birth, social security number (or equivalent identifying numbers), and employer information are stored together or associated with other equally sensitive information, the potential for privacy violations can occur. In the United States, legislators have moved to ensure that citizen privacy concerns are addressed through laws that impact the healthcare and financial industries; the Health

Insurance Portability and Accountability Act (HIPAA) and Graham-Leach-Bliley (GLB) are two such examples.

Citizen concerns about privacy must be addressed with enhanced government policy and resulting procedures to ensure that sensitive private information is not exploited and individual privacy is not impacted in a negative way.

Citizen concerns about privacy must be addressed with enhanced government policy and resulting procedures to ensure that sensitive private information is not exploited and individual privacy is not impacted in a negative way. While governments must be able to capture the necessary information to perform vital public services, the processing or analysis of information beyond its intended scope can pose a liability for the individual citizen, as well as the government agency, if a compromise should occur.

Privacy fears over too much integration of information will, in many cases, prevent the true value of identity credentials from being highly leveraged and the ultimate savings realized. Much of this fear stems from misunderstandings about the specific identity technology itself, combined with a lack of trust in how the information will be used and protected.

Can citizens have one card that establishes identity and still have peace of mind over how the information will be used? The answer is “yes,” but in many regards it is a matter of perspective. Governments currently already hold personal information on individuals across many functions and services, such as driver’s license, passport, tax, healthcare and education. The potential that this information may be commingled is the real concern. Using digital credentials for citizen identification will require that practical choices be made that remain technically sound while also meeting socially accepted standards.

NOTE

- 1 Gregg Kreizman, Avivah Litan, Neil MacDonald, Eric Ouellet, and Ray Wagner, “Findings from the Gartner 2006 Global Research Meeting: Low-trust world suits identity federation providers.” Gartner Research, 9 February 2006, 2.