



perspective

Globally Trusted Standards for Identification Credentialing Practices and Processes

May 2006

Executive Summary

The term “security” must be redefined and expanded to address the new global realities of colliding economic, political and consumer forces that demand greater visibility and accountability from businesses and governments. From port security concerns to large-scale identity thefts, individuals, businesses and governments think differently today about what security means. Security – in a new world – is not merely about what can go wrong but what needs to go right. Security initiatives can create convenience for consumers, reduce costs for business and government, promote commerce and improve public services.

To realize such advantages, security programs must take a comprehensive view of the people, goods and assets as well as on the core systems that comprise any operation. And central to securing all these elements are trusted identity and authentication credentials. Validating one’s identity is something people do everyday, from logging on to computer networks, conducting online banking transactions, navigating airport security, and crossing borders. Yet very little global coordination exists in identity management business processes. Furthermore, when securing people’s identities, public debate has centered on privacy because sharing personal data, even to advance national security, can conflict with individual rights.

Today, the rapid convergence of security issues worldwide combined with the growing concerns around individual privacy has created an urgent need to develop global standards for identity credentialing business processes. Many organizations are doing excellent work establishing universally accepted standards around enabling technologies, functional applications or regional practices. But the global community need to come together to create a baseline for adoptable global practices that address both security and privacy requirements, allowing ID credentials to operate across international borders and encourage confidence and trust from organizations and individuals around the world.

The purpose of this paper is to encourage this debate by reviewing current challenges related to inconsistent practices and processes; discussing the benefits of credentialing procedures that have a high level of

interoperability and trust worldwide; surveying the progress already underway toward this vision; and exploring how business and government can work together toward truly global ID credential business processes.

Standards for identity and authentication credentials should promote common approaches for how organizations across different industries and regions create, use and maintain credentials within their various business and government operations. To address privacy concerns, organizations should adhere to a code of conduct in which they demonstrate the safeguards used to protect personal information (both on the credential and also in the back-end data base) and clearly define the uses of and benefits of the credential.

The key to the development of successful standards for identification credentialing is to ensure alignment with privacy and security best practices that are accepted and trusted by business, governments and individuals around the world. Therefore, standards must be developed within the context of fact-based research on consumers’ attitudes and behaviors. Otherwise, consumers may not accept nor benefit from the resulting authentication practices. As a starting point, this paper examines the formation of a consortium of public and private organizations in the areas of technology, security and privacy that can provide a forum to determine the appropriate next steps and to define and promote global standards.

Imagine It

Imagine a world where your identity credentials are recognized and accepted wherever you go because they are based on privacy and security best practices accepted and trusted by business, governments and individuals worldwide.

In this world, we move quickly through security checkpoints at airports, gain access to our office and other secure locations without having to remember entry codes, view our financial records online without having to remember passwords, and conduct commerce without worrying about lost or stolen credit cards or data.

Governments and business around the world would be part of a global federation in which they mutually trust the identity verification mechanisms contained on each other's passports, driver's licenses, employee IDs, electronic certificates, smartcards and other authentication devices. Trust is possible regardless of what organization created the device or where the individual using it comes from.

In turn, the individual would be comfortable that the type of personal data he or she provides for authentication purposes is an appropriate and necessary exchange for the goods, services or access being requested. For example, privacy-conscious citizens are questioning why they need to provide both a National ID number or Social Security number and passport if all that is needed is to authenticate that he or she is the rightful owner of a credit card or over 18 years old. In this future environment, individuals will retain more control over access to their personal information and have greater visibility and control over how their data will be used.

Why is this not the case today? Is it the lack of universal standards not just in technology but in recognized business processes to create and manage ID credentials? Is it the public's lack of confidence in the organization issuing the credential and how it will use their personal data? Is it ambivalence over having one identity credential that can be used for multiple purposes or functions? Is it lack of reliable universal document authentication mechanisms? In this paper, we explore potential solutions to these thorny issues and to other barriers that are impeding the accurate, secure and smooth identification of individuals in both digital and physical environments.

¹ 2005 Most Trusted Companies for Privacy, Ponemon Institute Report, September 16, 2005.

Identity Verification Today

Millions of people around the globe have been impacted by ineffective identity authentication practices and procedures. Current identification methods are vulnerable to human error, social engineering and other malicious attacks. Recent headlines about everything from port security (where foreign nationals from many companies have access to secure port facilities) to large-scale identity theft breaches underscore the increasing public and private demand for solutions. Heightened concerns about the safety and security of transportation systems, public places and areas vulnerable to potential terrorist attacks have resulted in identification and security practices that are inconvenient and create worries about a "big brother" government society.

These urgent issues have driven discussions about what protective measures should be used to reduce risk to both public and to business operations. At the same time, privacy advocates have encouraged new regulations and corresponding new penalties for protecting the privacy of consumer information.

In fact, many public and private organizations that hold sensitive consumer data have not waited for government to pass laws before taking steps to secure the data they collect. They have been able to make the necessary investments because laws such as the California security breach notification law, S.B. 1386, have enabled organizations to calculate the cost of security. Costs created by inefficient or inadequate identity credentialing include the following:

- **The cost to the victim of a crime.** For example, due to identity theft, the victim's assets are stolen and credit history is affected.
- **The cost to an organization**
 - In the case of a security breach, which exposes personally identifiable information, the cost to an organization may range up to \$25 per consumer notification letter.
 - In addition, there is the more intangible cost incurred due to loss of trust and confidence in the organization's ability to protect sensitive and confidential information. According to a recent study on privacy and trust, organizations that have earned the highest trust levels make security and data protection a priority.¹

– Finally, there is the cost of lost opportunities. If an organization has had its intellectual property stolen, it loses its competitive advantage.

- **The cost to public safety.** The costs can be enormous and difficult to predict when terrorists, cyber criminals and other “bad guys” are not recognized and prevented from carrying out attacks on physical locations or the Web.

Besides the need to better manage protective measures to reduce these costs, public debates also must acknowledge **the great enabling potential of effective security**. Security initiatives can create convenience for individuals, promote the flow of commerce for business, reduce costs, improve the quality of government services, and advance individual privacy. These are just a few benefits.

To both reduce risks and realize advantages, security programs must take a comprehensive view of the people, goods and assets as well as on the core systems that comprise any operation. And central to securing all these elements is the identity credential.

Yet, little coordination or consistency exists around the world in finding the right approach. As a result, business and government organizations often are uncertain of the veracity of those credentials presented to them. Questions that are often asked include, “What is the validity of any identity information associated with the credential? And, “How stringent is the identity vetting process?” Failure to get positive responses to these questions creates a barrier to acceptance of the credential – which, in turn, increases risks and decreases benefits.

To address this issue, bilateral and limited multilateral agreements are emerging that allow for the trusted exchange of electronic identity credentials between or among select organizations.

One approach is requiring a central authority to control the vetting and credentialing process for issuance of the ID. Another way to achieve a trusted exchange of ID credentials is termed the “federated approach.” This involves separate organizations or entities that issue and manage the credentialing process, each drawing upon an agreed-upon standard or generally accepted framework. One example of a federated approach is the Liberty Alliance, a consortium of more than 150 companies, nonprofit and government

organizations from around the globe. The consortium is committed to developing an open standard for federated network identity that supports all current and emerging network devices.

However, these federated approaches are limiting and only involve participating organizations. In the meantime, the public’s concern is centered on making sure personal information is kept secure and not used for purposes that go beyond the scope of the authentication program. As a consequence, there are a multitude of different protocols and processes around the world for authenticating identity, which often fail to consistently address privacy concerns and personal rights.

The Privacy Issue

How does identity management affect individual privacy rights? Authentication requires a process for using personal and sensitive data to verify identity. Therefore, the public needs to cooperate fully and accept the identity management practices and technology used. If the public considers a particular method or technology as encroaching on reasonable rights to privacy, there will be legitimate resistance to adoption.

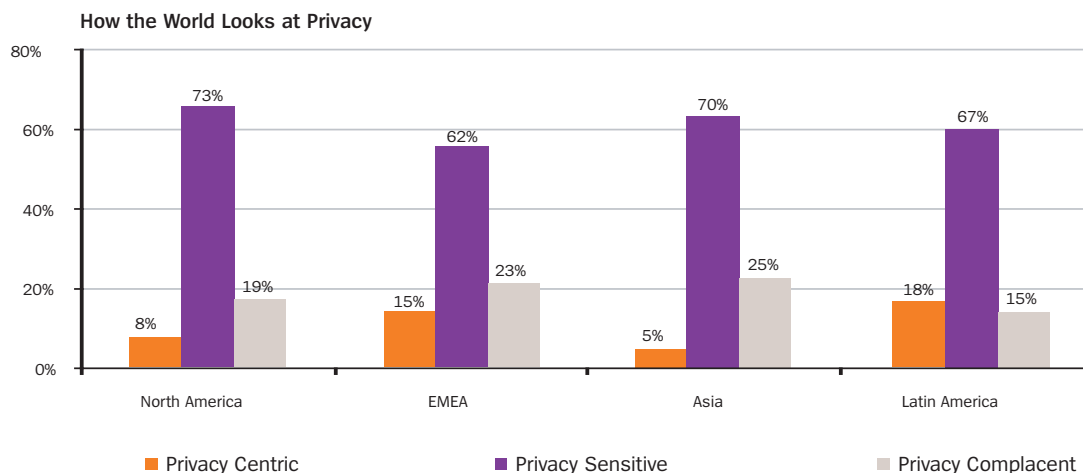
Because many organizations operate in the global economy, identity management systems need to function across national borders. Hence, it is important for businesses and governments to construct identity methods that do not violate the cultural, social or ethical sensibilities of a nation or region of the world in addition to the existing legal constraints. And that requires research into and recognition of consumer attitudes and perceptions.

For example, Ponemon Institute research indicates that citizens around the globe are becoming increasingly privacy conscious. Moreover, privacy concerns appear to vary by country or region of the world. This makes it hard for one global organization to create a unified or common approach.

Based on more than 100 studies Ponemon Institute conducted between 2003 and 2006, the following profile emerged of how adult-aged individuals in four regions of the world (21 countries) feel about their rights to privacy:

- **About 12%** of the public appear to be **privacy-centric**. Events that minimize their sense of privacy or diminish the safety of their sensitive personal information will have a significant impact on behavior.
- **About 68%** of the public appear to be **privacy-sensitive**. While they say that privacy is important to them, it will not change their behaviors or information sharing practices.
- **About 21%** of the public appear to be **privacy-complacent**. They really don't care very much about the sharing or selling of their most sensitive personal information, such as Social Security number or National ID.

The bar graph clearly shows that privacy is of consequence to most people around the world. It also suggests that people in different regions, especially EMEA (Europe + Middle East + Africa) and Latin America, are likely to be more privacy centric than individuals in other regions.



Ponemon Institute's studies on privacy show that privacy has become one of the pillars to consumer trust and confidence and is a necessary prerequisite to effective identity management. Privacy seals and posted privacy policies also make privacy one of the few observable commitments to safeguarding the consumers' security in the Internet world.

A Way Forward

To move forward, "security" must be redefined and expanded to address the new global realities of colliding economic, political and consumer forces that demand greater visibility and accountability from businesses and governments. From port security concerns to bird flu risks to large scale identity thefts and cyber breaches, individuals, businesses and governments think differently today about what security and privacy mean.

Standards for identity and authentication credentials should promote common approaches for how organizations across different industries create, use and maintain credentials within their various business and government operations. To address privacy concerns, organizations should adhere to a code of conduct in which they demonstrate the safeguards used to protect personal information (both on the credential and also in the back-end data base) and clearly define the uses of and benefits of the credential.

For example, standard global practices could include...

- Certification of the identity issuers based on degree of compliance with globally recognized identity proofing standards.
- Mandatory processes to validate input documents and possible biometric data before a credential is issued to an individual.
- Required elements to bind a certified identity issuer to a credential such as PKI technology or to associate a user to the credential such as with the use of biometrics.
- A logo to identify the credential as having met these global practice
- Interoperable global standards for reading (and writing) a credential.
- User-centric control for the release of identity attributes.

The standard practices must permit flexibility in technology architecture as well, thus allowing the ID credential to take many forms, such as an ID card, a smart chip in a cellular phone, a biometric, an RFID tag, an implantable chip and others.

Many organizations are already doing excellent work to create universally accepted standards. For instance, EPCGlobal is striving to create a set of global standards for emerging radio frequency identification devices (RFID). Other examples of standard setters that have been able to address international compliance barriers include ISO, ICAO and others.

However the relatively more niche standard setting organizations are often focused on technology issues, or on creating standards for use within countries or regions or for specific industry or functional purposes – such as national ID, driver's licenses, and so forth.

Only a very few standard setting organizations are considering a broader set of principles, including those that factor in the ethical impact of technologies on the general public. However, the focus of many of these organizations tends to be on one technology or functional application, rather than the broader spectrum of enabling business processes and consumer-focused initiatives that can advance the efficacy of the identity and authentication process.

For example, existing identity systems rely primarily on information sources such as name, home location, telephone number, National ID (or Social Security numbers), mother's maiden name, frequently asked questions and so forth. Information-based identity systems are prone to privacy and data protection issues and vulnerable to identity fraud.

Advances in new technologies, such as biometrics and electronic smart cards can improve the current state of identity management in ways that increase convenience, safety and privacy for the end user. Such technologies create the potential for true interoperability across many domains – thereby allowing the public to use an ID that services different functional needs ranging from border crossing, to airport screening to entering a secure physical location to accessing the Internet.

Despite advances in identity methods that make it possible to create more secure and convenient identity processes, some privacy advocates are still wary. For example, some

government and business organizations advocate the idea of one single identity credential that can be used for a large number of routine functions. To some, however, a single identity credential that cuts across functions, and is usable within different electronic devices, creates ethical and social risks. Credentialing mistakes and mismanagement of the identity credential could literally shutoff the individual's life. Perhaps more disconcerting, in the hands of an evil or corrupt government, the single identity credentialing system can be used as a social control weapon against the public, a.k.a. "big brother" risks.

How can global organizations create an ID that is accepted by the public and not abhorred by privacy advocates? As a starting point, there is a need to establish a governance organization or program for creating and monitoring responsible use principles, as described above. These principles should tie together selected other standards where appropriate to maximize collaboration among business and government organizations in the design, development and implementation of ID credentialing processes and procedures. In addition, these organizations must work together to address privacy issues, promote fair commerce and demonstrate value for the public.²

These principles must address the need for consumers, employees and other data subjects to have greater control over the credentialing process, possibly including control of the personal information used to establish their identity. The public must also have the ability to easily correct any errors in the authentication credential due to negligence or attempted malicious acts, in a way that does not open these correction mechanisms to fraudulent abuse.

Developing and Managing Standards

As noted above, there are many existing organizations or consortiums that have focused on the development of identity and authentication standards. Existing initiatives that have made impressive strides over the past several years include (but are not limited to) EPCGlobal (for RFID), ISO, ICAO, ITAA, and government bodies, including U.S. examples such as the National Institute of Standards and Technology (NIST), U.S. Department of Homeland Security and the National Security Agency.

Several commercial enterprises are supporting identity and authentication standards and creating de facto standards by implementing identity and authentication solutions. Among the most notable commercial enterprises promoting online worldwide identity and authentication solutions are VeriSign, IndentTrus, Microsoft, Certisign, Entrust, C&W HKT SecureNet, RSA and Cybertrust.

In order to determine the organizational structure that is needed to create and manage the responsible use of standards for identity verification, it is best to begin with the elements that the standards should address.

- Who should create electronic ID credentials?
How will the governance body or organization assess or determine the appropriate technology providers that will help design and develop credentials? This governance body must have the capability to ensure that technology providers that are part of the consortium of organizations have adopted appropriate safeguards to protect the personal and sensitive data they will receive from the general public.
- What data elements should be contained on credentials? There will be varying degrees of verification requirements ranging from one to three-factor authentication. For example, two and three factor authentication protocols require two or three independent ways to verify identity. This contrasts with traditional one-factor password authentication, which requires only one factor (knowledge of a password) in order to gain access to a system.

² Microsoft's Passport was intended to provide individuals with the ability to control their personal data. While Passport had the right intentions and objectives, its successful adoption was hampered by concerns about Microsoft collecting and storing personal information on a closed-source software platform. The new Microsoft Infocard initiative now takes an open standards approach to user centric control of identity information

- Degrees of authentication will vary with the level of sensitivity or security required in order to prevent mistakes or errors. In short, the governance body would need to create a systematic or heuristic method for identifying activities, functions or transactions that require different levels of authentication. Alternatively, the governance body may just publish standards for the level of trust to be placed in various identity credentials based on the authentication rigor and security of the credentials. Individual applications and entities could then determine the level of trust that they require in identity credentials.
- Another issue concerns the nature of data to be used. For instance, should the identity process always require one or another biometric reading? If so, which biometrics method would be accepted at different authentication levels? And, should there be a minimum accepted biometric for all IDs?
- What procedures should exist to vet and issue the ID credential? For example, how will individuals enroll, and do they need to enroll in person or can they enroll over the Internet or by phone? How will individuals provide the information to be used to authenticate them? What proof points will be accepted to allow an individual to obtain an ID? What is the process if an individual's legal identity can not be authenticated? What if the device containing the credential is lost or stolen?
- What mechanisms can be used to validate the identification credential over time or as circumstances change? For example, should digital key encryption, cert authority or other mechanisms be used? What would be the most reliable methods for ID validation purposes?

- In addition to controls over the credential vetting and issuance, there may be a need for auditing and monitoring activities by independent third-parties for the entire process. Audits and independent test labs serve as a deterrent to non-compliance with standards and, hence, may be needed to ensure transparency and stewardship of all organizations involved in the ID credentialing process. To be effective, however, organizations that fail audits should be required to remediate deficiencies or meet serious enforcement consequences.

In general, all the above questions need to be seriously considered and addressed by a governance body or consortium if business and government organizations around the globe are going to issue identity credentials that merit the public's trust and confidence.

Gaining Public Trust

As described above, the public is becoming more aware of privacy and the protection of the personal information shared with business and government. In order to gain acceptance of an identity credential, the organizations that develop and manage the credential need to understand the public's privacy concerns and take measures to reduce these worries.³ That is, standards must be developed within the context of fact-based research on consumers attitudes and behaviors.

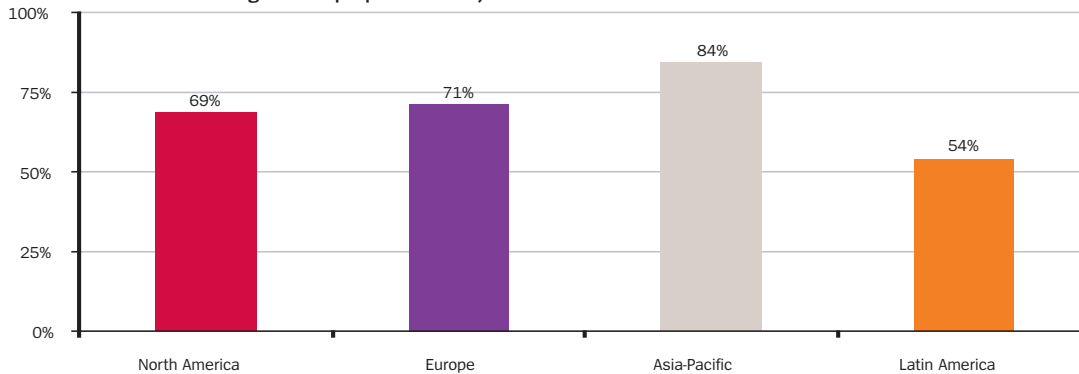
³ Unisys Global Study on the Perception of Identity Management, forthcoming May 2006.

Unisys study

A recently completed Unisys study investigated individuals' attitudes about the importance and value of different identity and authentication methods. The study looked at possible differences in the privacy or data sharing preferences of people residing in four different regions of the world, knowing identity management is essential to achieving the security goals of business and government.

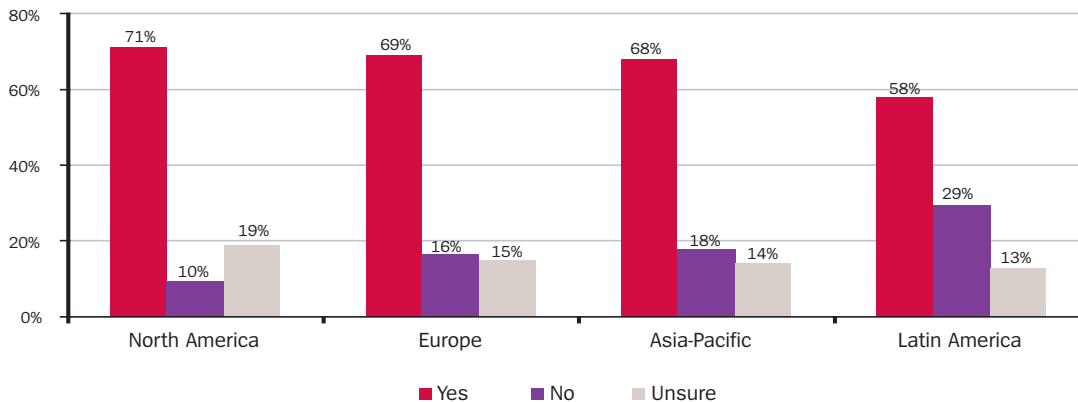
The findings suggest that individuals' propensity to share sensitive personal information with businesses and governments varies across geographic regions. However, individuals in all four regions are willing to share substantially more sensitive personal information if they perceive they are gaining real value in return (additional convenience and security). Perhaps the most important finding is that individuals in all geographic regions of the world prefer having one identity credential that can be used for multiple purposes or functions. Specifically, the survey findings show that the most important functions for a multi-purpose identity credential are to prove identity in order to access transportation channels (such as airplanes, trains, and buses), enter public locations (stadiums, airports and others), cross borders (customs) and access Internet accounts.

Bar Chart 2: Percentage of respondents in four global regions who would consider having a multi-purpose identity credential

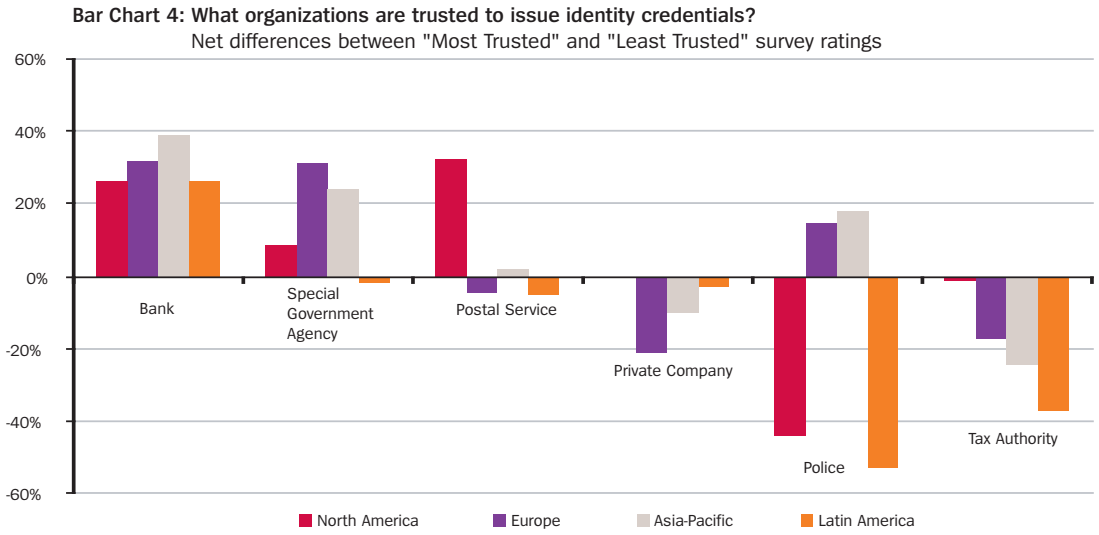


While many individuals prefer the identity credential to reside on an ID card, a large number of respondents like the idea of having it contained in a biometric, within a cellular phone, or in an article of clothing or jewelry.

Bar Chart 3: Will you consider using biometrics to prove your identity?



Who do you trust to issue the credential? On average, individuals across the globe believe that banking institutions would be the most trusted to issue and manage the identity credential. In contrast, law enforcement (police) and tax authorities are the least trusted to issue identity credentials.



Another important finding is that interoperability across national borders is critical to the success of the identity credential. That is, a majority of individuals believe it is important that the ID credential is able to operate across national borders.

In summary, the study’s results suggest that people want the identity management process to make their lives less complex and more secure.

Getting the Public On-board

As a starting point to creating global standards for identity and authentication practices, it may be important that businesses and governmental organizations develop a “bill of rights” to protect the general public from a plethora of privacy and security risks inherent in a unified or federated approach to identity verification. Framed as a credo statement, this document might contain the following attributes:

Protection: Demonstrate and make publicly known the safeguards in place to protect the individual’s data.

Benefits: Clearly define the benefits or value that the individual will experience as a result of their voluntary participation in this program.

Data collected and used: Define the personal data elements and/or biometrics required for differing “levels” of authentication and how the data will be used, managed and protected both on the device and related databases.

Secondary use: Explain how one baseline electronic credential may be added to other devices to authenticate identity.

Choice: Allow individuals to opt-in to combine or expand the use of existing ID devices. For example, a smart chip on a telephone can become an electronic authentication device (independent of its primary use for facilitating phone calls), because of the phone's typical presence in close proximity with its owner.

Redress: Provide a redress mechanism to address concerns and to respond to specific complaints or serious issues that might arise.

Another way to build trust is to make sure the public is made aware of the program, including extant privacy and data security risks that may arise as a result of their voluntarily obtaining an ID credential. Both business and government organizations involved in the vetting, issuance or management of the ID credential (a.k.a. identity industry) should be actively involved in the education and awareness process. Following are important facts that should be communicated to the general public as part of a unified, global outreach program:

- Enabling technologies like smart cards and biometrics actually decrease personal information needed for identity authentication and therefore can enhance privacy.
- Current “low tech” methods such as passwords and PIN numbers are inconvenient and open to abuse (especially because so many people can't remember their passwords).
- Stronger identity management and authentication methods actually reduce the most salient threats to privacy risk, including the theft of identity and other related frauds.
- Despite protections, the individual applying for the ID credential needs to take steps to ensure that source data is accurate and complete.

Another important step to raising the public's sense of confidence and trust is to obtain buy-in or support from leading NGO organizations such as the OECD and APEC to basic identity proposals. It may also be important to get buy-in from the United Nations, World Bank and the World Trade Organization because there is the potential to utilize this global approach to identity management as a way to harness economic opportunities for developing countries.

To enhance public confidence, ID solutions should not be overly simplistic. In other words, avoid the “one size fits all needs” syndrome. The credentialing process needs to be flexible enough to fit a wide array of different functions or purposes.

Above all, it is important to make sure ID credentialing programs are voluntary. This means that there can be no negative stigma attached to people who decide that they do not want to enroll. There also needs to be a separate set of control procedures for those people who fail the identity vetting process (e.g., because of insufficient documentation). And, as noted above, organizations issuing credentials require some degree of auditing and monitoring against responsible-use standards. Publication of these audits will enhance the program's transparency and will help to avoid program scope expansion that might occur over time.

Becoming a Trusted Enterprise

According to the Unisys Security Leadership Institute (SLI), a group of nationally recognized security experts from business and government charged with providing advice on emerging security issues, “the trusted enterprise is an organization embracing a set of corporate values and behaviors that guide all business practices. It is a highly ethical organization that treats its customers, employees, partners and shareholders with respect and stewardship. In the trusted organization, the CEO and board are deeply engaged in managing the organization's operating risk in a way that delivers maximum value in a safe and secure environment.”⁴

While security may not be a top-of-mind consideration for all senior executives, issues that impact the organization's reputation for integrity are very important to them. Confidence in the identity credentialing process that is used to verify or authenticate an organization's customers, employees and business partners is core to the integrity of the institution

relying on that credential to conduct business. Businesses or governmental entities that participate in a global standards initiative will be viewed as a more reliable and trusted partner in the global economy. Over time, the ability for an organization to adequately manage and protect the identity of key stakeholders will be essential to developing more open and collaborative relations.

Organizations that strive to become a “trusted enterprise” need to make sure that the data subject is protected. In other words, customers, consumers, employees, contractor, agent, shareholder, vendor and others feel that the organization will honor privacy- and data-protection commitments. Perhaps the adoption of a credo or “bill of rights” will be a way to convey the organization’s commitment to various data subjects.

These organizations are critical to the implementation and acceptance of globally trusted credentials. Creating secure access and safeguarding sensitive and confidential information supports the integrity of the enterprise. In this paper, we have discussed the creation of a credo or bill of rights to protect the privacy of individuals participating in a credentialing program. As with privacy policies, the credo would be posted prominently to demonstrate the trusted enterprises commitment to safeguarding individuals’ personal data.

These times are ones of increased risk and uncertainty. Institutions, both public and private, must learn how to prosper while dealing with a world encountering ever increasing threats. The trusted model is today, as it has been for many of the world’s most successful institutions in years past, the best way to see the enterprise through uncertainty.

Conclusion

The objective of this paper is to encourage global public and private sector organizations to consider universally accepted standard practices for identification and authentication credentialing. The primary focus is on what authentication business practices and processes are needed to achieve this goal. Accordingly, the discussion proposes a global standard for identity management that defines responsible uses of the identity credential as well as responsible practices in the issuance and vetting process.

As a starting point, we recommend the formation of a consortium of public and private organizations in the areas of technology, security and privacy that can provide a forum to determine the appropriate next steps. Engaging individuals, business and government in a dialogue that can address the issues raised in this paper, hear opinions that express core truths and build trust will put us all at the edge of a new frontier: the convergence of identity, technology, security and privacy.

⁴ The Trusted Enterprise is a concept developed by the Security Leadership Institute established and sponsored by Unisys Corporation. The SLI has conducted interviews of organizational leaders in North America to develop this framework.

Visit our website at: <http://www.unisys.com>

Specifications are subject to change without notice.

© 2006 Unisys Corporation.

All rights reserved.

Unisys is a registered trademark of Unisys Corporation. All other brands or products referenced herein are acknowledged to be trademarks or registered trademarks of their respective holders.

