



## Table of contents

<b>Identity Management</b> .....	3
Trust, but verify .....	3
What makes a reliable Identity Management system? .....	7
What does it take to implement an Identity Management solution? .....	7
How can HP meet your needs? .....	9
<b>Summary</b> .....	11
<b>For more information</b> .....	12



# HP provides collaborative technology and services that allow secure access to Identity Management solutions from the edge to the enterprise.

## Identity Management

As currently defined, Identity Management is a set of business processes working within a supporting information management infrastructure for the creation, maintenance, and use of digital identities. The use of digital identities is essential to continuing and increasing the social and economic benefits of e-business, e-government, and the Internet. Identity Management is complex and must balance the varying needs that business, government, and the individual have for security, privacy, and convenience.

As interactions between individuals and organizations—or individuals and other individuals—become less physically connected, the need to establish a trust framework for accessing benefits and services grows. In today's electronic environment, building a framework that encourages participation while complying with evolving security needs and legislation has become very complex. Pressing issues that an organization must keep in mind while considering the implementation of an Identity Management system include regulatory compliance, security, and business efficiency. But before we discuss implementation issues, it may be worth reviewing how the framework for trust has evolved over time and what makes it so complex today.

### Trust, but verify

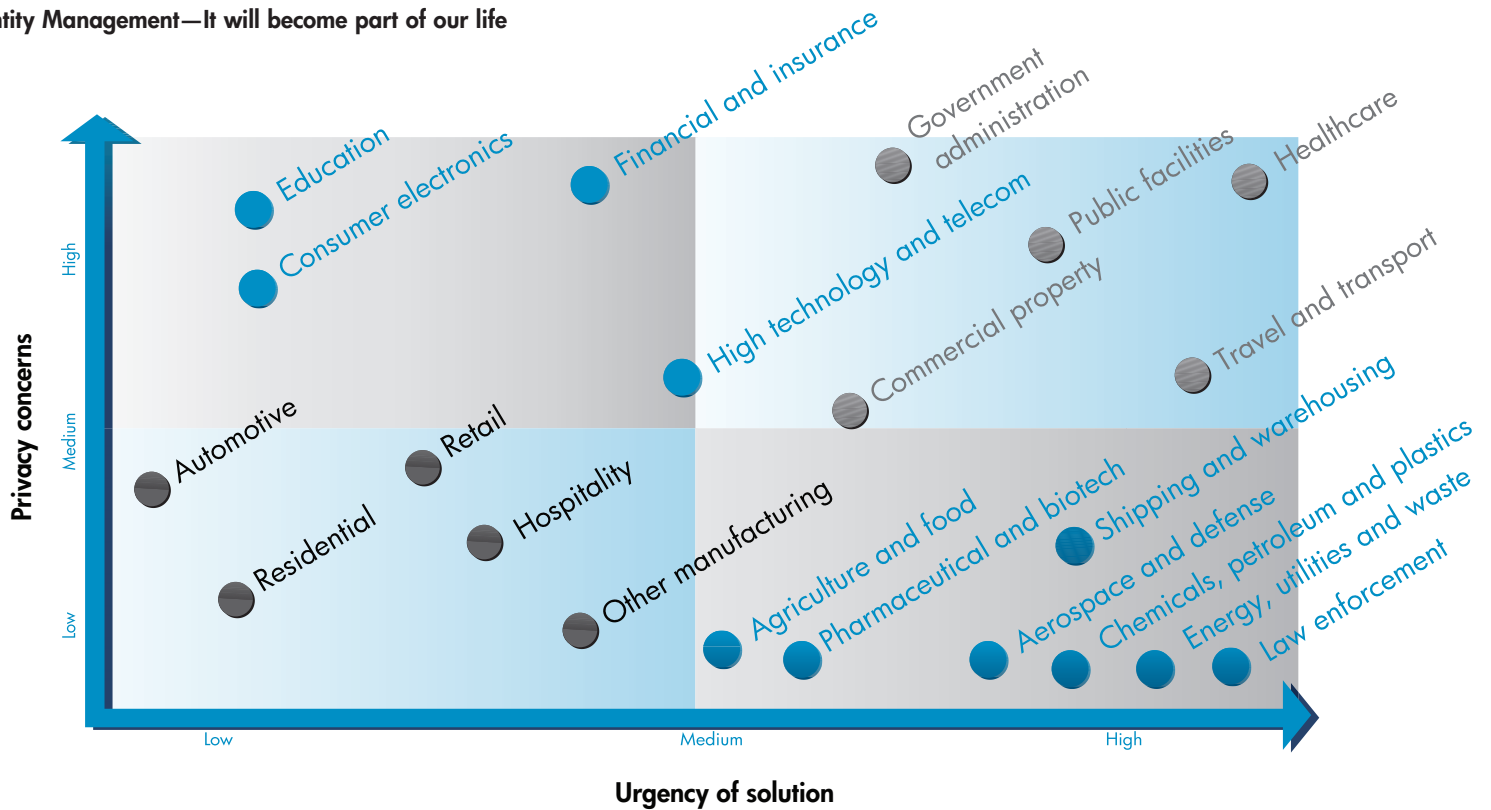
Centuries ago, trade was based on a trust that was inherently verifiable through the physical exchange of value for value—I give you my cow for your 50 chickens—and each party in the exchange typically knew one another's identity. In this exchange, the only assumption of risk that had to be made was that it was rightfully

my cow or rightfully your chickens that were exchanged. Two elements mitigated this risk: 1) knowing one another's identity, and knowing from experience the level of trustworthiness that was previously demonstrated by each party, and 2) in the end, possession was considered nine-tenths of the law.

This situation may have been more complicated if the parties did not know one another. In this case, an unknown party or parties would have needed a letter of introduction with the signature and seal of an identifiable authority. There would then be the added risk that these letters were not authentic. Ascertaining the level of trust in the letters of introduction by authenticating the signature and seal attached to the letter would have been necessary to mitigate this added risk. Clearly, being certain of the participants' identities and knowing that they have the appropriate rights and authority contribute to our ability to have trust in the execution of the exchange or transaction process.

A further evolution in trade involved the substitution of a medium of exchange, or money, on one side of the trade for valuable goods on the other side. Made of silver or gold, early forms of money had intrinsic value, and again, the trust in the exchange was inherently verifiable, and the assumption of risk remained essentially the same. The next major evolution in trade came with the substitution of a valueless certificate for the "hard" money previously used, precipitating an assumption that the certificate was authentic and represented either value, or a contractual promise of value, which could be accepted in exchange for valuable goods. This new assumption of risk was mitigated by the strength of the financial institution or country's treasury backing the inherently valueless certificate.

## Identity Management—It will become part of our life



In the early 1950s, the advent of the universal credit card substituted a promise that the bank will pay the seller—based on a separate promise that the buyer will pay the bank—for what was previously of value. More recently, with the advent of commerce over the Internet, since the exchange is no longer taking place face to face between buyer and seller, both the buyer and seller (as well as intermediaries) are now assuming (trusting, but not immediately able to verify) that the value they expect to receive will be forthcoming.

Gradually, with the evolution of information and communication technologies, electronic tokens based on similar technologies to the credit card, electronic certificates, smart cards, and radio frequency identity (RFID) tags are being introduced into personal identification solutions, first in the enterprise and later, as we see elsewhere around the world, into national identification schemes.

Thus, from the original simple trust framework of the face-to-face exchange between two parties, with only a rare possibility of interference by an outside element, both the commerce process and the associated risk to all parties have become much more complex. The exchange of value for value no longer occurs at a single point

in time, and in addition to the original two parties, it involves one or more intermediaries. Further, given that in an e-business environment, the transaction occurs electronically between diverse locations, there is potential for unanticipated adverse consequences (as from hacking, man-in-the-middle attacks, replays, etc.) affecting any or all of the parties involved. We can only expect that this will continue to be the case, and the need for solutions increases with rising privacy concerns and growing examples of process drivers as our society becomes increasingly paperless.

What is the trust framework in today's exchange process? How can trust be verified? Is trust based on the inherent reliability of the credit card or the banking institution that issues it, the security of the electronic process medium, the good intentions of all parties, or the lack of bad intentions of parties unknown? How can we know that the party claiming ownership of the credit card or other token actually owns it? And how can we be certain that once a transaction is made, one or the other party won't renege on the exchange by claiming they really didn't do it—the issue of providing non-repudiation?

Trust in each of these issues is compromised daily—and some with dramatically rising frequency and increasing impact. Key statistics from the National White Collar Crime Center, the Federal Trade Commission, and global special interest groups present a cause for concern:

- Identity theft is the No. 1 white-collar crime, and it is rising more than 50 percent per year.
- Complaints of Internet fraud rose 147 percent from 2003 to 2004.
- The UK Cabinet Office estimates the cost of identity fraud to the UK economy is at least £1.3 billion per year.
- The Interpol database of stolen passports (49 countries) contains 1.7 million entries.
- Identity fraud costs the Australian community AU\$1.1 billion per year.
- During 2004, 9.3 million Americans were victims of identity theft.
- The total U.S. annual identity fraud cost remains essentially unchanged since 2003, at \$52.6 billion, even though there has been heightened attention and increased measures of prevention and protection.

Without trust, there can be no confidence; without confidence, at the extreme, the willingness of individuals to transact business electronically also may be at risk. There are simply too many process steps, and there are

too many parties involved for an individual to be able to both trust and verify. Outside the realm of commerce, this dilemma equally applies to the access of valuable private and proprietary data, such as entitlement and benefit programs, Health Insurance Portability and Accountability Act (HIPAA) data, consumer credit data, etc.

Ultimately, we need to know who is involved in the commerce or access process and whether they have the right, privilege, and authority—which may be based on a given role—to participate in a commerce or access transaction that is likely separated by both time and distance. Being certain of the participants' identities, and knowing that they have rights and authority to participate, contributes to our ability to have trust in the execution of the transaction process. Electronic solutions to this dilemma have evolved into today's Identity Management systems. Subject matter experts, including the federal government, tell us that Identity Management must become one of the core responsibilities for any organization or institution involved in electronic transactions, whether involving access to protected data, rightful access to benefits, or involving the commercial exchange of value for value.

Recent legislation resulting from the events on September 11, 2001, and other global legislative and policy drivers have made it necessary to implement a broad range of Identity Management solutions, including some that mandate a token, badge, or card that can be carried with an individual and verified in the field.

Law/regulation	Coverage	Enacted or revised	Applies to/description
Canadian Personal Information Protection and Electronic Documents Act	Privacy	2004	Firms operating in Canada. Rules for protecting personal information collected, used, or disclosed in the course of commercial activity. Covers all personal information that enters the commercial environment.
European Data Protection Directive	Privacy	1995	Firms operating in the European Union (EU). Addresses identity theft, online fraud, and privacy issues related to consumers, employees, and citizens, harmonizing privacy laws among EU members. All member states must adopt privacy legislation or revise existing laws. Rules ensure personal data may be transferred only to non-EU countries that provide equivalent protection.
Electronic Signatures in Global and National Commerce Act	Electronic Signatures	2000	Firms operating in the U.S. Allows use of legally binding electronic signatures. The law doesn't prescribe technology, but public key cryptography qualifies and will be a leading application. Other nations have passed or are considering similar legislation.
Health Information Portability and Accountability Act (HIPAA)	Privacy	1996	U.S. health care firms. Requires controls for safeguarding protected health information (PHI) on individual patients. Establishes patient's right to control access and use of PHI. Defines who is permitted to use, disclose, or access PHI and how that information is safeguarded. Requires technical standards for access control, audit, authorization, data authentication, and network security.
Homeland Security Presidential Directive HSPD-12	Identification Standards	2004	U.S. federal government employees and contractors. Creates standards for reliable forms of identification in order to enhance security, increase government efficiency, reduce identity fraud, and protect personal privacy that can be rapidly authenticated electronically.

Law/regulation	Coverage	Enacted or revised	Applies to/description
Food & Drug Administration (FDA) Rule 21 CFR 11	Records retention, e-signatures	2000	Pharmaceutical and other firms operating in the U.S. under jurisdiction of the FDA. Defines requirements for controlling electronic records, submitting documentation in electronic form, and criteria for approved electronic signatures.
Gramm-Leach-Bliley Act	Privacy	1999	U.S. financial services firms. Requires financial institutions to establish administrative, technical, and physical safeguards to ensure the customer of record confidentiality. Prohibits firms from reusing or disclosing such information without an explicit grant from customer, and requires financial institutions to disclose their privacy policies to customers.
Sarbanes-Oxley Act	Accountability in reporting	2002	U.S. public companies. Requires annual reports to assess the effectiveness of internal controls and procedures for financial reporting.
U.S. Patriot Act	Privacy, record retention, identity verification	2001	U.S. financial services firms & transportation organizations, hazmat licenses, et al. Requires processes for risk-based identification of all new entrants; must collect identity information from customers and entrants, verify it, compare it against government-issued lists of known or suspected terrorists. Requires collection, verification, and storage of identity data. Will also affect policies for online and in-person account creation.
Securities & Exchange Commission (SEC) Rule 17a-4	Records retention	2003	U.S. securities brokers and dealers. Requires brokers and dealers to keep originals of all communications received and copies of all communications sent by a firm relating to their business. Requires 6-year record retention.
National Association of Securities Dealers (NASD) Rules 3010 & 3110	Records retention	1998	U.S. securities brokers and dealers that are NASD members. Requires correspondence retention as prescribed by SEC Rules 17a-3 and 17a-4. Records must indicate who prepared and reviewed outgoing correspondence, and must be readily available to the NASD upon request.
Fair Credit Reporting Act (FCRA)	Privacy	2002	U.S. consumers, holders and users of consumers' data. Provides rights to disclosure, requires accuracy, privacy, limits on information sharing. Requires duty to correct data.
Fair & Accurate Credit Transaction Act (FACTA)	Privacy	2003/4	U.S. consumers, holders and users of consumers' data used in transactions. Provides rights to disclosure, requires accuracy, privacy, limits on information sharing. Requires duty to correct data.
Real ID Act	Identification Standards	TBD	Requires all driver's license applicants (including U.S. citizens) to prove their legal immigration status. U.S. citizens, legal permanent residents, and refugees would receive a regular driver's license, while other immigrants would receive a different license.

Programs evolving from legislation include, for example, the Transportation Workers Identity Credential (TWIC), first responder identification, Registered Traveler Identification, and Department of Defense ID card programs. There is a definite need for highly reliable, portable identity solutions that ensure that a person working at the edge of an enterprise, administration, or agency is known to each respective domain and authorized to participate. For example, a person's authorization to provide emergency assistance, operate equipment in the transportation industry, access protected data or benefit information from remote locations, or gain access to highly effective weapons on the battlefield can be verified.

How do you know who is involved in the transaction? One function an Identity Management system must provide is authentication of the participants' identities. At the core of any Identity Management solution is the use of layered authentication technologies, from relatively weak to very strong, as the situation requires, including those which incorporate biometrics (unique physical attributes like

hand geometry, fingerprint, iris, etc.). Various combinations of what you know (ID and/or password), what you have (a card or token that is recognizable to the system), and what you are (multiple forms of biometrics) can be incorporated, along with process rules and techniques for binding the token to its rightful owner, in order to balance both optimum convenience and appropriate strength in the authentication process.

In most of the transactions today, identity is presented through something we know, and in fewer but growing numbers with something we have. However, the trust framework provided by these two levels of authentication is not enough for all types of transactions. Biometrics, either independently or in combination with the other factors, achieves the strongest form of authentication. Further, since well over half of all successful hacks to systems protecting proprietary data come from inside the enterprise rather than from outside, complete and auditable control over the entire enrollment process (for all levels of authentication, including the issuance of tokens and biometrics templates) must be implemented.

We have thus far concentrated on human identity; however, the full scope of confirming identity is not just limited to the identity of humans in the electronic (or virtual) setting. In a broader context, Identity Management encompasses determining the authenticity of documents, tokens, cards, artifacts, processes, materials, or devices in both the virtual and physical settings, particularly those that relate to the identity of humans or rightful ownership by humans. Do we know we are connected to the correct system; are we engaging in an e-dialogue with a valid website; is the e-mail requesting our proprietary information update from a valid requestor? Is the passport both a valid and an authentic document, and is the individual presenting it the rightful owner? Is the driver's license and credit card authentic and based on a credible inspection of primary identity documents? Is it a real birth certificate, diploma, piece of money, letter of introduction, or trademark—or is it a counterfeit?

#### **What makes a reliable Identity Management system?**

In the electronic environment, identity can only be trusted if it is issued and ascertained by a secure Identity Management system that comprises a complex mix of processes and technologies, including enrollment, issuance of tokens and credentials, provisioning, user administration, directory services, authentication, authorization, and audit. All are important elements of a full-function Identity Management solution, but the real business value of the Identity Management system resides in secure authentication. Each provider's Identity Management solution offers a set of capabilities. Some capabilities of Identity Management systems are required for security; others are required to support the business case for implementing Identity Management, while still others provide long-term, evolving business process efficiency. Subject matter experts define the following capabilities as necessary for a full and reliable Identity Management product-suite solution, particularly as these systems evolve in the future:

- Support identity assurance life cycle
- Provide mission-critical quality of service

- Provide flexibility of business process and business rules
- Comply with privacy policy and legislation
- Comply with standards
- Support transition management and/or minimize transition impact
- Support program evolution
- Deliver measurable business benefits
- Provide enterprise-wide, integrated authentication and authorization services, such as single sign-on
- Support for web services management and web services security
- Support interoperability and integration between trust domains
- Provide end-to-end security
- Support the ever-changing perimeter or edge
- Provide flexible support for compliance audits

#### **What does it take to implement an Identity Management solution?**

For the electronic environment, the United States' General Services Administration's (GSA) E-Authentication initiative, one of the 25 Electronic Government (E-Gov) services resulting from the President's Management Agenda (PMA), has established a highly validated process for government agencies to move into the realm of Identity Management by providing a consistent path to achieve implementation of the core Identity Management element. GSA and the Office of Management and Budget (OMB), with the technical support of National Institute of Standards and Technology (NIST), offer detailed guidance with handbooks, cookbooks, and assessment tools, as well as certified product lists, to allow an agency to understand their specific risks and requirements, to plan for migration, to select commercial-off-the-shelf (COTS) products, and to implement Identity Management leveraging the E-Authentication strategy that GSA has developed.

### Documents

- The E-Authentication Technical Architecture:  
-Technical approach for the E-Authentication Service Component:  
<http://www.cio.gov/eauthentication/documents/techApproach.pdf>
- SAML Artifact Profile as an Adopted Scheme for E-Authentication:  
<http://www.cio.gov/eauthentication/documents/SamlArtifactAdoptedScheme.pdf>
- E-Authentication Interface Specification for the SAML Artifact Profile:  
<http://www.cio.gov/eauthentication/documents/SamlSpecs.pdf>
- Trusted Credential Service Provider List:  
<http://www.cio.gov/eauthentication/documents/TCSP.pdf>
- Approved E-Authentication Technology Provider List:  
<http://www.cio.gov/eauthentication/documents/ApprovedProviders.htm>
- E-Authentication Handbook for Federal Agencies:  
<http://www.cio.gov/eauthentication/documents/GOVhandbook.pdf>

- E-Authentication Cookbook:  
<http://www.cio.gov/eauthentication/documents/Cookbook.pdf>
- E-Authentication Risk & Requirements Assessment Guide:  
<http://www.cio.gov/eauthentication/documents/eraguide.pdf>
- Credential Assessment Framework Guidance:  
<http://www.cio.gov/eauthentication/documents/CAG.pdf>
- NIST Electronic Authentication Guideline:  
[http://csrc.nist.gov/publications/nistpubs/800-63/SP800-63v6\\_3\\_3.pdf](http://csrc.nist.gov/publications/nistpubs/800-63/SP800-63v6_3_3.pdf)
- NIST Interfaces for Personal Identity Verification:  
<http://csrc.nist.gov/publications/nistpubs/800-73/SP800-73-Final.pdf>

### Tools

- E-Authentication Risk & Requirements Assessment (E-RA Tool)  
<http://www.cio.gov/eauthentication/era.htm>
- Credential Assessment Framework  
<http://www.cio.gov/eauthentication/documents/CAF.pdf>

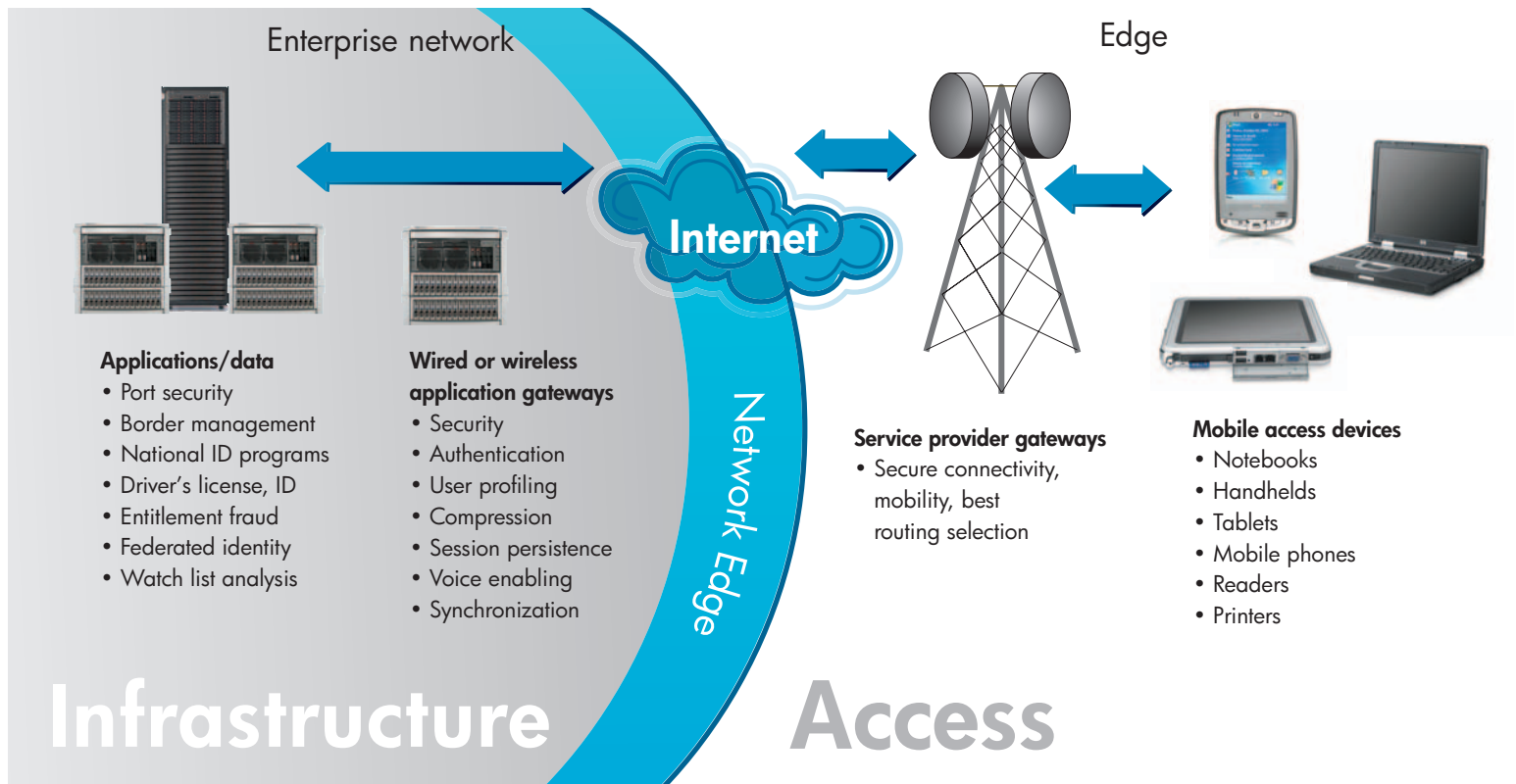
An organization's need is fundamentally based on an initial assessment of risk and requirements. Given a thorough understanding of the organization's system requirements, the agency may only need to select a single component to enhance their legacy system, or they may need to select a complete product suite. Within the agency's spectrum of need, and so long as the implementation complies with the E-Authentication specification (and OMB justification requirements), they are free to choose components or solutions that meet their needs.

The U.S. Department of Defense (DoD) has embraced the incorporation of Identity Management to secure and protect its most vital assets—people, information, and equipment. The DoD incorporates smart card technology in its Common Access Card (CAC), public key infrastructure (PKI) for network logon, digital signing, encryption of e-mail communications, and biometrics to

recognize and/or verify the identity of an individual. In January 2004, the DoD Chief Information Officer (CIO) took the first step to create an integrated, enterprise-wide approach to Identity Management when he formed the DoD Identity Protection and Management Senior Coordinating Group (IPMSCG). The CIO's vision is for the IPMSCG to "focus on department-wide interoperability standards, performance matrices, and ways to exploit Identity Management tools as means for enhancing readiness, business processes, and security, while also being cognizant of protecting entities' identifiable information."

A review of recent work accomplished by the U.S. federal government, including the policies, standards, guides, and processes, would be beneficial to any organization, government or non-government, considering implementing an Identity Management solution.

HP delivers and/or coordinates the entire solution. HP brings the Identity Management world together from the edge to the enterprise.



#### How can HP meet your needs?

The spectrum of Identity Management solutions extends from the simplest, as in incorporating a component into an existing system, to the most complex, as in a full systems integration project. HP has worldwide project experience across this entire spectrum, with all the subcomponents therein, and across the whole value chain of identity.

The Identity Management market is a growing market, one that has been rapidly consolidating. As a result, the competitive situation in the market is continuously changing, and small point-solution providers are finding it increasingly difficult to compete. Customers have also found it difficult to determine what they need and who can provide it. However, with the initial round of corporate and technology acquisitions more or less completed, technology convergence is beginning to reduce product overlap, technology redundancy, and a bloat of features, which is decreasing the confusion for customers.

HP has demonstrated strong commitment to this market with the acquisition of SelectAccess from Baltimore Technologies, which closely followed the strategic acquisition of TruLogica, a relevant player in the provisioning management space. Both of these acquisitions serve to expand existing Identity Management solutions from HP. To provide the optimum mix of expert knowledge, outstanding technology solutions, and the ability to adapt to the specific needs of the client, domain experts and proven partners are regularly engaged to provide a comprehensive solution.

In addition to the traditional worldwide partnerships with Cisco, Microsoft®, and Oracle®, full-scale Identity Management solutions from HP are being implemented with the leading secure document producers, personalization solution providers, biometric systems providers, and federated server solution providers. These acquisitions and partnerships have positioned HP as a solution suite provider with a comprehensive and first-rate offering.

For solutions implemented in the United States, particularly those involving interface with the U.S. government, Identity Management solutions from HP are compatible with standards and policy of the leading consortia in the Identity Management domain, the Liberty Alliance. A brief review of the compatibility matrices developed by the Liberty Alliance shows that with its partners' capabilities, Identity Management solutions from HP span the entire range of Liberty Alliance evaluation criteria, as well as the entire list of system capabilities that subject matter experts insist are necessary for a full and reliable Identity Management product-suite solution.

As a leading secure IT solutions provider, HP is also active in other standard-making bodies and working groups in electronic Identity Management and biometrics arena, including, for example, the BioAPI Consortium, The Open Group, the PKI Forum, the WWW Consortium, and the Trusted Computing Platform Association, as well as different working groups under the Internet Engineering Task Force (IETF). Reinforcing its commitment to IT security in general, HP has recently committed millions of dollars to accelerate its ongoing pursuit of National Information Assurance Partnership (NIAP) Common Criteria certification for its operating systems and enterprise management software, including the Identity Management solution suite.

HP has provided IT solutions and systems integration services in the Identity Management domain to government customers around the world (e.g. United States, Poland, Italy, Bulgaria, Israel, and Hong Kong).

The specific know-how and intellectual property derived from the worldwide HP project experience in this domain is concentrated within a dedicated organizational unit in HP Services Consulting and Integration—HP Center for Public Sector IT Thought Leadership. The HP Center for Public Sector IT Thought Leadership is staffed with project managers, solution architects, and technical experts that lead projects delivered throughout the world.

HP also provides multiple Managed Service models, including the formation of public-private partnerships to manage elements of customer processes. These partnerships may take either temporary or long-term responsibility for operation of IT infrastructure as desired by the customer. Public-private partnership business models can also be employed to ease the financing of complex and potentially expensive projects. HP has extensive experience with performance-based contracting, which represents another alternative contracting option that may meet the customer's needs. Depending on the actual situation, HP Financial Services will work with the customer to identify the optimum financial model, finance the initial infrastructure and solution, and share the return on investment over an extended period of time, with a broad range of ownership and operational responsibility transfer models available for consideration. HP offers many different types of utility and affordability models that are derived from both the solution building block approach and unique breadth of financial service offerings.

---

## Summary

Whether we like it or not, in the future, our identity will be much more bound to biometrics, and will be more closely integrated into the fabric of our daily lives. This is necessary in order to allow us to seamlessly move from the virtual to the physical world—in both private and business life situations—within a secure framework of trust. Some argue that implementing Identity Management to increase security can be used for the purpose of invading privacy. Rather, its intention is to enhance privacy and personal safety, as anyone who has experienced credit card fraud, Internet fraud, identity theft, or other personal violation will testify. Ensuring efficient e-commerce and e-government involves being able to trust and verify while maximizing security and minimizing expenditure of effort, cost and time—the process should make it more difficult for criminals to

perpetrate fraud, while making it easier and more secure for the rest of us to live and work. For any organization that is involved in commerce or that is providing remote access to proprietary and private data, Identity Management must be implemented as an essential coreprocess and a critical element of their IT infrastructure. Accomplishing this requires disciplined risk and requirements assessment, world-class project and systems integration management, and an all-encompassing suite of open and collaborative solutions. HP brings these benefits to its customers with reliability, dependability, and integrity.

Whether desiring to assess your Identity Management needs, replace or add Identity Management components, or initiate a full-scale Identity Management solution implementation, HP can deliver. To learn more, contact your nearest HP representative.

---

## For more information

[www.hp.com/go/IDManagement](http://www.hp.com/go/IDManagement)

© Copyright 2005 Hewlett-Packard Development Company, L.P. The information contained herein is subject to change without notice. The only warranties for HP products and services are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. HP shall not be liable for technical or editorial errors or omissions contained herein. Microsoft is a U.S. registered trademark of Microsoft Corporation. Oracle is a registered trademark of Oracle Corporation and/or its affiliates.

4AA0-0587ENUS, 05/2005

