Identity and Access Management of the Future

Realizing a “Doing More with Less” Strategy
Table of contents

4 Maximizing the ROI of IT Expenditures
4 Reducing Productivity Gaps in Implementing 21st Century Government Policies
5 Establishing National Priorities to Achieve Effective Business and Citizen Interaction
5 Determining Balanced Cybersecurity Standards and Practices
6 HPE’s Assured Identity Solution and Services Expand to Meet These Challenges
7 Conclusion
7 For more information
7 About the Author
Ongoing national-level planning and budgeting efforts highlight the critical role that information technology (IT) will play in providing government services for citizens and businesses. They encourage the wider use of technology when it can enhance effectiveness and efficiency. At the same time, however, these plans cut IT budgets for the foreseeable future. This necessitates a strategy of “doing more with less.” In this era of fiscal austerity, these key strategic activities are essential to achieving this vision:

- Maximizing the return on investment (ROI) of IT expenditures
- Reducing productivity gaps in implementing 21st century government policies
- Establishing national priorities to achieve effective business and citizen interaction
- Determining balanced cybersecurity standards and practices

A renewed emphasis on Identity and Access Management (IdAM) is one of the critical elements in achieving these strategic steps. IdAM is the primary technology for determining a) if a user is who he or she claims to be, b) which resources this user is allowed to access, and c) verification of what that user has actually attempted or accomplished while using the system. These are key questions that must be asked and answered regardless of the nature, type, and scope of any system being accessed. Access controls are applicable to every type of IT from shared service “clouds” to mission-specific systems. Let’s review the four strategic activities outlined above.
Maximizing the ROI of IT Expenditures

Ongoing strategies to consolidate data centers and increase the use of shared IT services offer the benefit of lowered costs but also require new IdAM approaches and technology. Because information may no longer reside within a specific enterprise but rather in a remotely operated and managed environment such as the cloud, new capabilities to control access to applications and information resources must be deployed by the information “owner” rather than the hosting organization.

IdAM systems must provision users in accordance with established policies and practices appropriate for a “shared” service. The IdAM system must not only manage access as defined by the policies, but also provide appropriate auditing for verification purposes. As organizations’ or users’ needs change, the IdAM technology must be flexible enough to allow those changes in a timely manner.

The use of federated identity provides a proven solution to the challenge of managing users in the cloud, as well as those within the organizations’ own environment.

Reducing Productivity Gaps in Implementing 21st Century Government Policies

As smartphones and tablets become ubiquitous and users demand more convenient access via these devices, the government has both an opportunity and a challenge to bridge the productivity gap. Mobile access allows faster response while improving agency performance and mission outcomes.

Personal Identity Verification (PIV) credentials using a smart card form factor provide proven authentication tokens for both government employees and businesses that interact with governments today. The next step in the evolution of these credentials is to develop standards for mobile devices leveraging the Public Key Infrastructure (PKI) certificates stored on a PIV card to grant a comparable level of assurance for use on a wireless device.

This capability will provide significant advancement in secure communications that support wireless access for first responders, emergency management communities, and others not tethered to a physical connection. Access to news feeds, maps, and situational awareness, as well as the ability to share information and collaborate, opens the door to new classes of applications and services.
Establishing National Priorities to Achieve Effective Business and Citizen Interaction

National priorities concerning citizen services are being considered by governments all over the world. For example, in the United States an “eBenefits Portal” provides self-service access to healthcare information for both current military members and Veterans. The credentials used to access these sites are issued by trusted third parties. This strategy encourages the development of an ecosystem of strong credentials issued by organizations with which the public may already have an established relationship. Government and business applications would then consume the credentials already in use by citizens or private businesses rather than requiring a unique credential for each application or organization. An appropriate analogy is the convenience of a single credit card accepted by most businesses rather than a unique credit card issued by each.

Citizens will no longer have multiple credentials to deal with, and organizations will no longer have to issue and manage credentials or reset passwords. A credential that allows an end user to access a variety of applications will carry with it a much higher value as compared to a credential that can only be used for a single application.

Determining Balanced Cybersecurity Standards and Practices

Standardized approaches to security assessment/access authorization using a smart card form factor, as well as continuous monitoring for cloud-based services, are key elements of many governmental strategies today. This framework will increase both the efficiency and effectiveness of providing citizen services. Moving systems and applications to a cloud-based model will still require agencies to establish IdAM-related controls. The balance associated with cybersecurity controls and accessibility must be determined in advance and “built in” to those architectural approaches. Issues over privacy and security will continue; consequently, the technology employed must accommodate a wide range of policy choices.
HPE’s Assured Identity Solution and Services Expand to Meet These Challenges

The latest release of the Hewlett Packard Enterprise Assured Identity solution adds additional capabilities to an already rich platform that has been used by U.S. Federal agencies for more than a decade. Federation, remote Identity Proofing, and Privileged User Management combine to meet the challenges of 21st century governments.

In an age of increased online interaction, the importance of identifying individuals for remote transactions has become essential to delivering fraud-resistant services. The increase in public-private collaboration and the softening of the network perimeters have resulted in the need to establish an appropriate level of identity and access in order to reduce risk to an organization’s information and assets.

HPE offers a Cloud Managed Service for identity proofing and two-factor authentication as part of Assured Identity Software as a Service (SaaS). These services can be consumed by organizations through web services via the Internet. This pay-per-transaction service allows organizations to reduce their total cost of ownership by eliminating the need for on-premise infrastructure and IT personnel. These services are compliant with U.S. government standards for Remote Identity Proofing programs. HPE has a strong partnership with a Data Mart vendor that provides reliable, current data and industry-leading data analytics.

HPE Assured Identity Federation provides a fast, deceptively simple security solution that can be delivered via a hybrid of SaaS and on-premise components, designed to seamlessly integrate into an organization’s current environment. This capability allows trusted credentials to be consumed by existing IdAM technologies.

HPE Assured Identity Federation benefits include:
- Increased security with low administrative burden
- Seamless resource access between agencies and private organizations
- Short deployment times
- Lower total cost of ownership
- Business-/mission-oriented, flexible solutions

HPE Assured Identity Privileged User Management is an enterprise administration and reporting system for privileged user and shared accounts. Using this capability, system administrators can determine fine-grained access to sensitive systems through individual, group, policy and role-based controls. Centralized auditing, reporting, and video session playback are available. HPE Assured Identity Privileged User Management permits authentication on Unix/Linux systems to the Active Directory, enabling a single repository for all users. Where shared accounts are absolutely necessary, HPE Assured Identity Privileged User Management provides for password check-out/check-in and audit back to the original user.
Conclusion

The emphasis on providing fast, accurate citizen services through mobile and cloud technologies has demanded additional risk-reducing strategies at lower costs. Identity and Access Management controls are key to meeting these challenges. HPE’s Assured Identity solutions can make these “do more with less” strategies real today and into the future.

For more information

For more information, please visit the HPE Identity and Access Management web page at www.hp.com/gov/mobility/.

About the Author

Steve Lazerowich
Lazerowich is a security solution leader on the Cybersecurity Solutioning Team within Hewlett Packard Enterprise U.S. Public Sector. In this role, he has provided detailed security architectures and solutions to public sector clients, including the U.S. Army and Air Force, FEMA, NASA, VA, the Federal Reserve, and Health & Human Services. Throughout his more than 15-year career in the federal information security space, Lazerowich has provided project management and subject matter expertise to a number of government identity management programs, including the E-Authentication Initiative, the Federal Identity Credentialing Committee (FICC), the Federal Identity, Credential, and Access Management (FICAM) Subcommittee of the CIO Council, and has provided support to the Chair of the Federal PKI Policy Authority. He holds a Bachelor of Science degree from the University of Massachusetts and is a Certified Information Security Manager (CISM) and a certified Federal IT Security Professional – Manager.