

The Three Pillars of Trust

Adopting a New Service Architecture for Trusted Transactions
with Government on the Internet

by

Mike Ozburn

ozburn_mike@bah.com

Booz | Allen | Hamilton

delivering results that endure

Table of Contents

How We Got Here 1

Toward a New Architecture of Trust..... 1

Guaranteeing Identity..... 2

Protecting Privacy 3

Improving Online Transaction Security..... 4

Conclusion..... 5

About the Author 6

About Booz Allen 7

Principal Offices Back Cover

The Three Pillars of Trust

Adopting a New Service Architecture for Trusted Transactions with Government on the Internet

Users may soon start giving more US federal agencies a “thumbs up” as additional government services begin to move online. This would represent a long-awaited yet positive change, since moving federal service delivery online with “E-Gov” has been the official policy of the US government since 2002.¹ The functional idea is similar to what private businesses have done for years: enable customers to interact with service providers and place orders online. Adapting this model to federal services offerings makes sense on many levels. E-Gov can increase the speed and reduce the cost of service delivery, which results in happier customers helps agencies improve mission performance and overall effectiveness. In this context, it can be difficult to understand why it has taken agencies more than eight years to implement this new directive. To be fair, transforming complex processes in government agencies into an online transaction format is not a simple task. Observers will point to trust-related impediments such as establishing proof of identity, ensuring privacy, and enforcing transaction security. The goal of this paper is to describe how a new architecture for trust can help agencies overcome these issues, and begin now to make E-Gov a reality.

How We Got Here

The first decades of the Internet devoted few resources to online trust. According to Internet pioneers, “early networks...were purpose-built—i.e., they were intended for, and largely restricted to, closed communities of scholars....”² There was no perceived need to engineer trust into the Internet. Today, hundreds of millions of strangers globally use the Internet, which has become an indispensable tool for business and leisure alike. Businesses now devote considerable resources to ensure the confidentiality, integrity, and availability of

Internet-based transaction systems. Consumers have growing awareness of online risks, but it is hard for them to control all online trust issues when Web sites and social networks automatically splice together a myriad of services that operate mostly “under the hood.” Despite best intentions, there are still too many stories of breaches that impede the public’s trust in using the Internet for personal business.

The organic growth of a trustless Internet resulted in efforts to bolt on security controls. Federal funds seeded early development of key security technologies, such as firewalls, intrusion detection, encryption, and authentication. Technologies like these are essential, but because of their bolt-on nature, networks and IT systems are still subject to exploits when vulnerabilities are improperly managed. Indeed, the National Academy of Sciences has long said that securing cyberspace is one of today’s “grand challenges” of engineering.³

Toward a New Architecture of Trust

Grand challenge or not, all organizations—including federal agencies—must leverage technologies that exist today to secure online transaction systems for E-Gov. Until now, fragmented silos of security technologies have been used to protect individual applications, data, or users. In a world of Web-connected smart phones and interactive social networks, however, these silos are under increasing pressure with the integration of transactional services. These pressures—combined with the rising cost of risk management, compliance, and security—present an unsustainable condition for trusted transactions.

The solution is moving to a new architecture of trust that directly addresses the need to provide secure,

¹ Office of E-Government & Information Technology in the Office of Management and Budget, www.whitehouse.gov/omb/e-gov/.

² “Birth of the Internet,” Barry M. Leiner, et al., Aug. 4, 2000, www.isoc.org/internet/history/brief.shtml.

³ “Secure cyberspace,” National Academy of Engineering, www.engineeringchallenges.org/cms/8996/9042.aspx.

convenient services that scale to hundreds of millions of users conducting billions of transactions. A transaction occurs every time a user clicks the mouse on a link, which initiates a “request/receive” process driving pieces of a particular back-end E-Gov service.

With the new architecture, online trust in these service transactions will rest upon the “Three Pillars of Trust”: identity, privacy, and security. Under this architecture, the party making the request and the party delivering the response can be known, one to the other, at sufficient levels of specificity to allow authentication and authorization. The personal data that is involved in each service transaction can be accorded appropriate protections for privacy. Finally, each transaction can be appropriately protected from end-to-end in a manner that balances security and convenience within the context of the service being used. With the three pillars in place, each E-Gov service can be provided with lower risk and, therefore, lower costs for security, compliance, and overall operations.

Guaranteeing Identity

At a human level, we each recognize the importance of being able to know who is on the other side of a transaction. It is no different online, although methods for determining the identity of the other party are changing. For many years, each service provider attempted to issue its own credentials that could be used in the context of its silo of service. The most commonly understood credential is the username and password, which are usually the minimum credentials required at each online site. A more sophisticated version of this same approach is the Public Key Infrastructure, or PKI model, which is defined for certain contained environments such as in individual enterprises, industrial groups, or federal agencies.

These controls are technically sound but they have practical constraints. Typical usernames and passwords are prone to security risks because many are easy to guess (especially with automated hacker tools). When they are “hardened” with random,

longer character strings, they become inconvenient because of the nature and scale of use within an individual’s real-world interactions. The rapid growth in an individual’s portfolio of usernames and passwords usually causes them to be written for later recall (and then be prone to discovery by an unauthorized party). Many are forgotten due to their complexity, causing users to spend time completing Web forms to recover a forgotten credential. Or users take the easiest route and reuse them in perpetuity, which creates another vulnerability. Alternatively, PKI systems have a high cost of ownership and operation due to the individual nature of their implementations and requirements for key management; many cannot be deployed on a large scale because of cost or complexity.

Borrowing from the established model of payment cards, national governments are adopting a new identity system called a Trust Framework. The objective is to enable trusted delivery of E-Gov services to citizens with a scalable, secure, low-cost, and convenient solution to the identity problem. In the US version of a Trust Framework, the user is issued a digital credential by a commercial identity provider (IdP), such as their bank, with which they already have an online relationship. This credential is used to interact online with a federal agency service provider called a Relying Party (RP). Agreements between all parties contractually enforce the technology, policy, legal, and financial aspects of the Trust Framework, which are established and managed by a Trust Framework Provider (think Visa® or MasterCard®).

Following a recommendation by President Barack Obama’s US Cyberspace Policy Review in May 2009,⁴ the Trust Framework model was adopted as part of the US Federal Enterprise Architecture in November 2009 and provides the basis for an identity solution across more than 24,000 federal agency Web sites.⁵ When adopted across a broad range of IdPs and Relying Party Web sites, the Trust Framework will provide a scalable solution for online authentication and authorization, at a lower cost and with greater convenience for users.

⁴ *Cyberspace Policy Review: Assuring a Trusted and Resilient Information and Communications Infrastructure* (May 2009), www.whitehouse.gov/assets/documents/Cyberspace_Policy_Review_final.pdf

⁵ *Federal Identity, Credential, and Access Management (FICAM) Roadmap and Implementation Guidance*, www.idmanagement.gov/documents/FICAM_Roadmap_Implementation_Guidance.pdf

The road map promises these benefits:

- Increased security
- Compliance
- Improved interoperability
- Enhanced customer service
- Elimination of redundancy
- Increase in protection of personally identifiable information (PII)

The Trust Framework has strong policy backing in the US, as well as Australia, Canada, and Great Britain. At the announcement of the National Program Office for the implementation of the National Strategy for Trusted Identities in Cyberspace (NSTIC), White House Cybersecurity Coordinator Howard Schmidt stated, "We need a vibrant marketplace that provides people with choices among multiple accredited identity providers—both private and public—and choices among multiple credentials."⁶

The Trust Framework allows US federal agencies to rely on commercial IdPs to issue credentials to the more than 250 million online users in the US. By externalizing this task, the government will considerably reduce the cost and difficulty of verifying identity for E-Gov transactions with citizens. IdPs must comply with the long-established technical and policy requirements of the federal government that are specified by the Trust Framework. With this provision, a commercial IdP can choose among several technical solutions for identity management of their own customers. Many solutions are derived from software-based "cards" that operate across any online platform.

In Great Britain, there is a similar push known as Digital by Default. The key driver is reducing operating budgets without reducing citizen-facing services. The UK seeks to move about one-third of all citizen interactions online. As in the US, the UK solution will rely on credentials issued by banks, telephone companies, and a wide range of other consumer

organizations with which citizens/customers already have an ongoing relationship.

Trust Frameworks offer the potential to solve the identity issue for citizens and federal agency service providers alike, establishing the basis for lower costs, greater security, more convenience, and a wide range of identity-based services. By building upon this first pillar of identity, agencies can now begin the move to an overall architecture of trust for delivery of E-Gov services.

Protecting Privacy

The concept of privacy includes notions of the quality or state of being apart from observation and enjoying some freedom from unauthorized intrusion into the activity of an individual or into information about that individual.

These notions could seem quaint and outdated to many in a digitally connected world where search engines like Google™ see and remember virtually anything that happens, and where information is hacked or "spilled" with alarming regularity. Today, most people would describe privacy as how "the information I care about" is being handled in any given situation. An operative definition of privacy is as much about the level of control that an individual has over a piece of information as it is about the technology or legal arrangements that are used to protect or enforce this control.

Just as the pillar of identity has its own well-developed infrastructure, there is a similarly large and complex infrastructure that has evolved for privacy. Almost every Web site boasts a privacy policy; in reality, few people read it and many are not enforceable. There have been many efforts to codify rules for privacy in laws, regulations, and self-regulated industry environments. The net result, however, has not established a general level of confidence in privacy required for online delivery of services. Skepticism abounds in the ability—and even the desire—of some institutions to protect privacy.

The architectural solution for the second pillar of privacy hinges on user control and the recognition that users

⁶ A National Program Office for Enhancing Online Trust and Privacy, The White House Blog, www.whitehouse.gov/blog/2011/01/07/national-program-office-enhancing-online-trust-and-privacy.

have been empowered to exercise this control online in new ways. Federal agencies planning delivery of services online should consider other models for successful user-based controls.

Consider that almost everyone today has some experience with establishing the rules for online service interaction. Examples include setting the recording options with a TiVo™ or other digital video recorder (DVR), or managing the information we put on Facebook™ or publish in personal blogs. Most people have experience with establishing their own choices for how their personal information is to be managed by the service provider.

As federal agencies move to a trust architecture for E-Gov, these same lessons can help establish a well-understood and well-received model for citizen privacy controls. Agencies should focus on structure, transparency, and clarity. Remember: today's online tools do not require the same one-size-fits-all approach that was typical in traditional published written privacy agreements.

A well-designed structure for privacy makes it easier for a user to understand the options that will protect certain information. Simple structures can provide users with a great deal of control. For instance, an agency can give the citizen control over the personal information that is: (a) stored for use only with that user; (b) stored for general use by the agency service provider; or (c) not stored. Similarly, by using consumer-friendly online interfaces that are optimized to a desktop or mobile device, an agency can enable transparency to dramatically improve privacy control. Finally, the use of consistent and clear communications can improve privacy controls. Even simple consumer-friendly ceremonies, such as sending an alert when information is accessed or shared can provide for greater privacy protection, certainly more than what is available in many cases today.

In the online world, privacy protection must be shared between the agency service provider and the user. Today's technologies and consumer-interaction models

can be used to architect a much greater level of privacy protection than before. By intentionally focusing on the structure, transparency, and clarity of shared online tools designed for true protection of private information, federal agencies can successfully implement the second pillar of trust and see immediate benefit from lower costs and greater customer interaction.

Improving Online Transaction Security

Security was much easier to understand—and to enforce—in a physical world measured by visible guns, gates, and guards. The location of protected assets was the basis of security in the physical world. This model served early efforts for online security, when focus on network perimeter controls such as DMZ or firewalls seemed to resonate with those grappling with the issue.

The physical model carryover also assumes that access control is all that is required for logical security. With borderless mobile computing and wide open access, however, the focus must shift to securing each online transaction. In the third pillar of an integrated trust architecture, security is designed into the entire transaction process on an end-to-end basis, whether this environment begins at a user's smartphone or ends in a virtual cloud operated by an agency service provider. The total process must be woven into a services-oriented architecture to enable convenience for and confidence by the user.

If privacy is defined by a user's perspective regarding the information that he/she cares about, then security relates to everything that the agency service provider is responsible for protecting within E-Gov systems. This is a large, but not insurmountable, requirement.

At a consumer level, it is well established that security is not a thing to be provided, but rather a condition that exists along a continuum. Security is not readily measured or quantified, but it can be understood by a user. As service models continue to evolve and expand, it will be important for service providers to integrate the third pillar of trust, which is a security architecture that can be shared with, and managed by, the user. The goal

for the agency is to achieve better security at a lower overall cost. As with privacy, the security architecture must include a clear structure, transparency, and control that includes input by citizen users.

The big challenge for federal agencies is that end-to-end security is not designed into a typical e-commerce architecture. Efforts to “bolt on” individual security solutions for individual applications or transactions have been costly, difficult to manage, and often are inconvenient for users. Yet this does not need to be the case for E-Gov, as motivated consumers have readily adopted sophisticated end-user technology (think iPhones and Droid devices) and have no problem navigating new service models (think about the many users of Facebook™ or Groupon™ accessed from these same devices). The call to federal agencies is to build the third leg of security in a trust architecture for E-Gov where each user can be positively identified, and where security is designed in at a transactional level that is inherently more user-friendly, while providing greater security at lower cost.

Some companies have built cloud-based platforms that turn an Apple iPhone into a biometric scanner able to provide voice or facial recognition. Using a security system like this is no more complicated than uploading a picture from the same device to Twitter™ or a video to YouTube™. There are security applications that provide one-time passwords or digital credentials supporting easier access to network-based resources. Federal agencies looking to provide services via the Internet need to explore similar options.

In pursuing this third pillar of trust, federal agencies should also structure individual E-Gov services within a continuum of convenience and security that is managed by each user, within boundaries set by security professionals. In this manner, agencies can design a cost-efficient architecture that provides stronger security. The key to achieving this goal is focusing on structure, transparency, and clarity when designing security into a holistic service model.

Conclusion

There is a big difference between citizens reading about services on a federal Web site versus applying for and receiving them via the same medium. The federal government has long committed to E-Gov, but making this happen in a real, personal way is the challenge facing every agency. E-gov requires agencies to transform service fulfillment from the physical world into transactions conducted via the virtual world.

In the physical world, the notions of identity, privacy, and security have always been important. These notions are no less important to virtual transactions. As we have described above, they constitute the three pillars of a trust architecture that will underpin the transformational effort of E-Gov. The operational elements of identity, privacy, and security are well-established and ready to go. By embracing the Three Pillars of Trust now, federal agencies can immediately begin moving toward a new service architecture and implement online interaction with citizens. The united effort of federal agencies will bring citizen users a more convenient and desirable experience, while controlling risk, improving privacy and security, and lowering government’s cost of fulfilling online transactions.

About the Author

Mike Ozburn is a Principal with Booz Allen Hamilton and works within the Information Technology team. He leads the firm's efforts in developing Web 3.0 Trusted Service solutions based on identity, trust management, data sharing, and cybersecurity for civil agencies and commercial enterprises. Most recently he has been actively engaged in the development of the emerging trust layer for the Internet, including the US government's adoption of Trust Frameworks. As a long-time participant in the open identity community, he serves on the boards of the OpenID Foundation, The Information Card Foundation and the Open Identity Exchange.

Contact Information:

Mike Ozburn

Principal

ozburn_mike@bah.com

703/377-6792

About Booz Allen

Booz Allen Hamilton has been at the forefront of strategy and technology consulting for nearly a century. Today, the firm is a major provider of professional services primarily to US government agencies in the defense, intelligence, and civil sectors, as well as to corporations, institutions, and not-for-profit organizations. Booz Allen offers clients deep functional knowledge spanning strategy and organization, technology, operations, and analytics—which it combines with specialized expertise in clients’ mission and domain areas to help solve their toughest problems.

The firm’s management consulting heritage is the basis for its unique collaborative culture and operating model, enabling Booz Allen to anticipate needs and opportunities, rapidly deploy talent and resources, and deliver enduring results. By combining

a consultant’s problem-solving orientation with deep technical knowledge and strong execution, Booz Allen helps clients achieve success in their most critical missions—as evidenced by the firm’s many client relationships that span decades. Booz Allen helps shape thinking and prepare for future developments in areas of national importance, including cybersecurity, homeland security, healthcare, and information technology.

Booz Allen is headquartered in McLean, Virginia, employs more than 25,000 people, and has annual revenues of over \$5 billion. Fortune has named Booz Allen one of its “100 Best Companies to Work For” for six consecutive years. Working Mother has ranked the firm among its “100 Best Companies for Working Mothers” annually since 1999. More information is available at www.boozallen.com.

To learn more about the firm and to download digital versions of this article and other Booz Allen Hamilton publications, visit www.boozallen.com.

Principal Offices

ALABAMA

Huntsville

CALIFORNIA

Los Angeles
San Diego
San Francisco

COLORADO

Colorado Springs
Denver

FLORIDA

Pensacola
Sarasota
Tampa

GEORGIA

Atlanta

HAWAII

Honolulu

ILLINOIS

O'Fallon

KANSAS

Leavenworth

MARYLAND

Aberdeen
Annapolis Junction
Lexington Park
Linthicum
Rockville

NEBRASKA

Omaha

NEW JERSEY

Eatontown

NEW YORK

Rome

OHIO

Dayton

PENNSYLVANIA

Philadelphia

SOUTH CAROLINA

Charleston

TEXAS

Houston
San Antonio

VIRGINIA

Alexandria
Arlington
Chantilly
Charlottesville
Falls Church
Herndon
McLean
Norfolk
Stafford

WASHINGTON, DC

The most complete, recent list of offices and their addresses and telephone numbers can be found on www.boozallen.com by clicking the "Offices" link under "About Booz Allen."