Testimony of Dr. Peter Alterman

Assistant Chief Information Officer, E-Authentication

National Institutes of Health

and

Chair, Federal PKI Policy Authority

Before the

American Health Information Community

Confidentiality, Privacy & Security Workgroup

September 29, 2006

Background

I am Dr. Peter Alterman, Assistant Chief Information Officer of the National Institutes of Health for Electronic Authentication. I am also the current Chair of the U.S. Federal Public Key Infrastructure (PKI) Policy Authority, an interagency committee chartered by the Federal CIO Council. In this role, I am responsible for drafting, modifying and implementing policies controlling the Public Key Infrastructure Architecture of the U.S. Government. All Federal Agencies that issue digital certificates are required by the Office of Management and Budget to cross-certify their Public Key Infrastructures with the Policy Authority or to buy their digital certificates from a vendor who operates its PKI under the U.S. Federal Common Policy Framework, overseen by the Policy Authority. Additionally, I work closely with the Federal E-Authentication Program Management Office and I am responsible to them for reviewing and approving PKI credential providers.

My purpose in testifying to the AHIC Confidentiality, Privacy, & Security Workgroup is to give you background information about the policies, procedures and guidelines being followed by U.S. government Agencies and affiliated entities. The Federal government has been working for years to develop standards, procedures and guidelines for implementing electronic identity management services that can ensure trusted, secure transactions over the Internet. I would like to summarize briefly our experience for you in the hope that our experiences will help you analyze, plan and implement the appropriate strategies for ensuring secure, trusted electronic transactions among citizens, caregivers, allied services providers and the Federal government.

Basic Principles of Electronic Authentication Architecture

There are many credential providers in the electronic identity business. Every application that generates and issues user ID/password pairs is a credential provider. In fact, historically, every electronic application has been its own credential provider. If you log on to an Internet Service Provider, that provider is a credential provider. If you log on to a network at the office, that network is a credential provider. There are so many credential providers of user IDs and passwords that many companies market password management software products.

The foundation of the US government's E-Authentication approach is that software applications should not issue credentials; rather, they should trust and use existing credentials issued by other providers. It has been the avowed goal of the US government to minimize the number of user IDs and password or digital certificates a user needs to authenticate to government applications and websites. Imagine walking around with only one or two credit cards in your pocket instead of fifteen. Rather than add to the glut of electronic identity credentials most people must manage, the US government has built an identity authentication infrastructure that helps a software application recognize and trust – at a known Level of Assurance, or LOA – electronic identity credentials issued by other entities.

In order for this to work, an application needs to know two things: how assured it can be that the electronic identity credential presented is actually being used by the person who

it claims to be from (generally called the "Level of Assurance") and second, what level of assurance of identity does the application require in order to guarantee sufficient privacy for and security of the information being passed and stored?

Risk and Risk Management

The procedure for satisfying these requirements begins with a standardized risk assessment of the software application or business process. The E-Authentication Program Management Office has a very good risk assessment tool available for free on its website (references at the end) but several others exist and are in use generally. In addition to identifying the risks your system or process is vulnerable to (and the list might surprise you), this exercise will identify the Level of Assurance of Identity (LOA) required by the software application in order to ensure sufficient risk mitigation. The National Institute of Standards and Technology Special Publication 800-63 maps risk levels to particular technologies for ensuring the required LOA.

All Federal Agencies that field electronic applications on the Internet are required to implement this process by the Office of Management and Budget. Included in this list are the Drug Enforcement Administration Controlled Substance Ordering System, which allows for secure electronic transmission of Schedule IV controlled substance orders from manufacturer and distributor to pharmacist. Indeed, DEA plans to issue high assurance digital certificates to every single practitioner who prescribe controlled substances in the USA. These electronic identity credentials will be trusted by other Federal Agency applications online at a known Level of Assurance, since the DEA issues

its digital certificates under policies and procedures that are mapped and published by the Federal PKI Policy Authority and which are recognized internationally.

Trusting External Credentials

Both the E-Authentication Program Management Office and the Federal PKI Policy Authority have extensive, published procedures for determining the trustworthiness of electronic identity credentials issued by a wide variety of credential providers, government, commercial and academic. For assertion-based credentials such as user ID/password pairs, the E-Authentication program has a procedure called the Credential Assessment Framework. Assessors go out to a candidate credential provider and evaluate their identity proofing, operations and technology implementations using a published, standardized process for assessing the trustworthiness of the credentials issued by that provider. Credential providers that satisfy the E-Authentication requirements may join the government's identity federation and their credentials may be trusted by all government applications at their stated levels of assurance.

At substantially higher levels of assurance cryptographically-based credentials are required. The Federal PKI Policy Authority has an extensive assessment process called "cross-certification" that assess the trustworthiness and security of digital certificates issued by providers. In addition to a dozen Federal Agencies, the State of Illinois, MIT Lincoln Lab, Wells Fargo Bank, CertiPath (the aerospace industry international PKI bridge), and the European Telecommunications Standards Institute have mapped their policies and procedures against the Federal PKI Policy Authority's policies and

procedures. Cross certification is currently under way with many other entities including SAFE, the pharmaceutical industry international PKI bridge that services almost two dozen corporate PKIs issuing digital certificates to thousands of staff. Public Key Infrastructures that are cross-certified with the US Federal PKI Architecture issue digital certificates that may be trusted by applications that require higher, known Levels of Assurance of Identity.

Identity Proofing

Mandated by HSPD-12, the National Institute of Standards and Technology has promulgated a Federal Information Processing Standard – FIPS 201-1, which describes the required procedures for identity proofing for issuing high assurance electronic identity credentials for Federal employees and contractors. This process for identity proofing is targeted at guaranteeing assurance of identity for issuing digital certificates at high LOA, but the principles embodied in the Standard are generally applicable for issuing all sorts of electronic identity credentials.

Summary

The US government has developed and has implemented widely a standardized method of identifying the risks that must be planned for and mitigated when designing and fielding online applications providing services to citizens and businesses. We have developed and implemented standards, policies, procedures and an architectural approach that stress trusting external electronic identity credentials rather than adding to the current glut of user IDs, passwords and digital certificates. The US government has

implemented a robust architecture for identifying, evaluating and validating electronic identity credentials issued by a wide variety of providers using varying technologies at known Levels of Assurance of Identity that are directly related to the risks of operating electronic software applications on the Internet. A list of references and resources that may be helpful to you follows. My colleagues and I stand ready to advise you and support your efforts.

Resources and References

Government Paperwork Elimination Act of 1998,
http://www.whitehouse.gov/omb/egov/e-1-legislation.html

E-Government Act of 2002, http://www.whitehouse.gov/omb/egov/e-1-legislation.html\

Office of Management and Budget Memorandum 04-04,
http://www.whitehouse.gov/omb/memoranda/fy04/m04-04.pdf

Office of Management and Budget Memorandum 04-24,
http://www.whitehouse.gov/omb/memoranda/fy04/m04-24.html

Office of Management and Budget Memorandum 05-05,
http://www.whitehouse.gov/omb/memoranda/fy2005/m05-05.pdf

Office of Management and Budget Memorandum 05-24,
http://www.whitehouse.gov/omb/memoranda/fy2005/m05-24.pdf

National Institute of Standards and Technology Special Publication 800-63,
http://csrc.nist.gov/publications/nistpubs/800-63/SP800-63V1_0_2.pdf

Federal Information Processing Standard 201-1,
http://csrc.nist.gov/publications/fips/fips201-1/FIPS-201-1-chng1.pdf

Office of Management and Budget Common Policy Framework,
http://www.cio.gov/ficc/documents/FICCframework.pdf

Criteria and Methodology for Cross-Certifying With The
U.S. Federal PKI Architecture,
http://www.cio.gov/fbca/documents/crosscert_method_criteria.pdf

E-Authentication Credential Assessment Framework,
http://www.cio.gov/eauthentication/documents/CAF.pdf

Drug Enforcement Administration, Controlled Substance Ordering System,
http://www.deaecom.gov/csosmain.html