



**Considerations and Lessons Learned for Federal Agency
Implementation of DNS Security Extensions and E-mail
Authentication**

**Supporting the Adoption of the National Strategy for Trusted Identities in
Cyberspace for Public-Facing, Non-Person Entities**

**Information Security and Identity Management Committee (ISIMC)
Network and Infrastructure Security Subcommittee (NISSC)
Web 2.0 Security Working Group (W20SWG)**

November 2011

CONSIDERATIONS AND LESSONS LEARNED FOR FEDERAL AGENCY IMPLEMENTATION OF DNS SECURITY EXTENSIONS AND E-MAIL AUTHENTICATION

Federal CIO Council

Copyright 2011 Carnegie Mellon University.

This material is based upon work funded and supported by the United States Department of Homeland Security under Contract No. FA8721-05-C-0003 with Carnegie Mellon University for the operation of the Software Engineering Institute, a Federally funded research and development center sponsored by the United States Department of Defense.

Any opinions, findings and conclusions or recommendations expressed in this material are those of the author(s) and do not necessarily reflect the views of the United States Department of Homeland Security or the United States Department of Defense.

This report was prepared for the

SEI Administrative Agent
ESC/XPK
5 Eglin Street
Hanscom AFB, MA 01731-2100

NO WARRANTY

THIS CARNEGIE MELLON UNIVERSITY AND SOFTWARE ENGINEERING INSTITUTE MATERIAL IS FURNISHED ON AN "AS-IS" BASIS. CARNEGIE MELLON UNIVERSITY MAKES NO WARRANTIES OF ANY KIND, EITHER EXPRESSED OR IMPLIED, AS TO ANY MATTER INCLUDING, BUT NOT LIMITED TO, WARRANTY OF FITNESS FOR PURPOSE OR MERCHANTABILITY, EXCLUSIVITY, OR RESULTS OBTAINED FROM USE OF THE MATERIAL. CARNEGIE MELLON UNIVERSITY DOES NOT MAKE ANY WARRANTY OF ANY KIND WITH RESPECT TO FREEDOM FROM PATENT, TRADEMARK, OR COPYRIGHT INFRINGEMENT.

This material has been approved for public release and unlimited distribution except as restricted below.

Internal use:* Permission to reproduce this material and to prepare derivative works from this material for internal use is granted, provided the copyright and "No Warranty" statements are included with all reproductions and derivative works.

External use:* This material may be reproduced in its entirety, without modification, and freely distributed in written or electronic form without requesting formal permission. Permission is required for any other external and/or commercial use. Requests for permission should be directed to the Software Engineering Institute at permission@sei.cmu.edu.

* These restrictions do not apply to U.S. Government entities.

Intended Audience

This document is intended for Federal Government CIOs, CISOs, designated Authorizing Officials (AO), security managers, and program managers who have the responsibility to assess, plan for, and implement identity management technologies on the information systems under their purview.

This document is intended, in conjunction with other appropriate Federal CIO Council and NIST documents, to help Federal officials identify and overcome technical and administrative barriers to the adoption of Domain Name System Security Extensions (DNSSEC) and e-mail authentication as part of an identity management strategy.

Note: The Federal CIO Council does not endorse the use of or imply a preference for any vendor's commercial products or services mentioned in this document.

Acknowledgements

The Federal CIO Council would like to thank the following people for contributing lessons from implementing DNSSEC, DKIM, and SPF: Scott Rose , Dan Sheehan, Jim Boissonnault, Edward Rhyne, and Carl Beaudry. Additionally, we are grateful to Earl Crane, Roger Seeholzer, and Marilyn Rose for their feedback and support during the development of this document.

TABLE OF CONTENTS

Executive Summary	6
The Importance of Identity Management.....	7
The Role of DNSSEC in the Federal Enterprise.....	9
E-mail Authentication in the Federal Enterprise.....	12
Considerations for Implementation of DNSSEC, DKIM, and SPF.....	15
Management Considerations.....	15
1. Develop a Comprehensive Concept of Operations for the dotgov.gov DNSSEC Program.....	15
2. Establish a Forum for Federal Network Operators and Technicians	15
3. Consider Executive-Level Endorsement for e-mail Authentication	15
4. Take the Opportunity to Update Existing Executive Policy	16
5. Improve Documentation of DNS Policies and Procedures within Agencies.....	16
6. Establish and Expand Communities of Interest	17
Operational Considerations.....	17
1. Update Implementation Guidance	17
2. Understand Operational Challenges of Key Management.....	17
3. Standardize DNSSEC Validation Criteria	17
4. Maintain Communications with Registrar	18
5. Maintain Ability to Perform DNS Testing.....	18
6. Manage the Decommissioning and Retirement of Government Domains.....	18
7. Conduct Training	18
Technical Considerations.....	19
1. DNSSEC Requirement.....	19
2. DNS Vulnerability to Caching Resolvers (Implementation)	19
3. Challenges of Complexity.....	19
4. Lack of Major Vendor Support for DKIM and SPF	20
5. Replay and Message Content Protection	21
6. Reputation Policy.....	21
Conclusion	22
Appendix A: Training and Resources for DKIM, SPF, and DNSSEC.....	1

Executive Summary

Federal information infrastructure modernization programs have enabled development of innovative electronic Government services. Agencies providing such services must identify and manage associated risks. One challenge is to manage access to assets in a manner that meets Federal security requirements. As Government sensitivity to unauthorized use of information continues to increase, agencies must increase their investment in resources to verify the identity of users and control their access.

To establish an environment that encourages trusted electronic transactions, the Government needs to create and support conditions that build confidence. Efforts are underway to establish and maintain confidence in the identity of public-facing, non-person entities in the Federal information infrastructure. Two such efforts are Domain Name System Security Extensions (DNSSEC) and e-mail authentication.

This paper outlines the original case for DNSSEC and e-mail authentication as important components of a trusted Government cyber environment; highlights some technical considerations that Federal agencies need to appreciate when deploying these components; and identifies lessons learned by early adopters.

The Importance of Identity Management

Federal information infrastructure modernization programs have enabled development of innovative electronic Government services. Agencies providing these services must identify and manage the associated risks. One challenge is to manage access to assets in a manner that meets Federal security requirements. In cases of increased sensitivity to unauthorized use of information, agencies must increase their investment in verifying the identity of users and in access control. In essence, agencies must establish who in their organization is trusted to utilize what resources and data, and make available a way to validate and verify that trust.

According to the National Institute for Standards and Technology (NIST) Special Publication SP 800-53, *Recommended Security Controls for Federal Information Systems* trust must be understood as a chain, particularly when operating in interconnected environments, for which the agency establishes and retains “a level of confidence that each participating service provider in the potentially complex consumer-provider relationship provides adequate protection for the services rendered to the organization.”¹ Increased trust enables agencies to confidently provide increased access to their assets, and increased assurance of the identity of the users accessing that data.

The Federal Government has made identity management a priority of cyber security strategy for most of the last decade. In 2003, the Department of Homeland Security published the *National Strategy to Secure Cyberspace* which recognized the vulnerability of cyberspace to denial-of-service attacks and stated that “lack of address verification and accountability makes filtering and contacting the sources of an attack impossible.”² In her 2009 60-day cyberspace policy review, Melissa Hathaway, then acting senior director for cyberspace for the National Security and Homeland Security Councils, renewed the call to improve identity management:

*With the systems available today for most Internet transactions, the electronic equivalent of cues people use to establish trust might be absent, incomplete, or difficult to understand and act upon. Identity management has the potential to help individuals and organizations form trusted communities based on varying degrees of identity exposure and mutually agreed accountability, while helping exclude unwanted intruders or inappropriate membership. Identity management also has the potential to enhance privacy through additional protection against the inappropriate release of personal identifiable information.*³

On April 15, 2011, the White House released the *National Strategy for Trusted Identities in Cyberspace* (NSTIC),⁴ envisioning an identity ecosystem as a component of an overall cyber security. This ecosystem would result from an effort by the private sector facilitated by the Government-and lasting several years. The NSTIC emphasizes the need for building the identity ecosystem through a collaborative relationship, and suggests the role of the Government is to “support and enable the private sector, [and to] lead by example.”⁵

¹ NIST Special Publication SP 800-53 *Recommended Security Controls for Federal Information Systems*.

http://csrc.nist.gov/publications/nistpubs/800-53-Rev3/sp800-53-rev3-final_updated-errata_05-01-2010.pdf

² *The National Strategy to Secure Cyberspace*. http://www.us-cert.gov/reading_room/cyberspace_strategy.pdf

³ *Cyberspace Policy Review: Assuring a Trusted and Resilient Information and Communications Infrastructure*. http://www.whitehouse.gov/assets/documents/Cyberspace_Policy_Review_final.pdf

⁴ <http://www.nist.gov/nstic/>

⁵ http://www.whitehouse.gov/sites/default/files/rss_viewer/NSTICstrategy_041511.pdf

The NSTIC envisions that the identity ecosystem will facilitate a new type of operating environment where “individuals and organizations utilize secure, efficient, easy-to-use, and interoperable identity solutions to access online services in a manner that promotes confidence, privacy, choice, and innovation.”

Recent evidence indicates a rising tide of data theft.⁶ Some observers suggest that malicious actors are scaling back their efforts to steal information via misleading e-mails (phishing) not because of resistance, but because phishing is so easy they can achieve sufficient results with reduced effort.⁷ If this criminal activity is to be curtailed, Federal civilian agencies must implement effective identity management technologies as outlined in the NSTIC.

Regardless of the presence or absence of policy or compliance requirements, there are good business reasons to position an organization for participation in a trusted identity ecosystem. However, no matter the level of trust an organization has in its identity ecosystem, two primary identity problems remain, which require improvements in identity management:

1. Passwords are inconvenient and insecure.
2. Individuals are unable to prove their true identity online.⁸

The NIST NSTIC fact sheet⁹ that identifies these two problems provides several examples of the costs and issues associated with current password and identity management practices.

This paper focuses on a small part of the identity ecosystem envisioned by the NSTIC: public-facing, non-person entities operated by Federal civilian agencies. In practice, this part of the identity ecosystem is realized by applying security protocols to the Domain Name System (DNS) and by e-mail authentication. DNS security requires the implementation of DNS Security Extensions (DNSSEC). Agency level E-mail authentication can be achieved by a combination of DomainKeys Identified Mail (DKIM) and Sender Policy Framework (SPF).

⁶ *RISK Team 2010 Data Breach Investigations Report*. http://www.verizonbusiness.com/resources/reports/rp_2010-data-breach-report_en_xg.pdf

⁷ http://www.antiphishing.org/reports/APWG_GlobalPhishingSurvey_1H2010.pdf

⁸ *The National Strategy for Trusted Identities in Cyberspace: Why We Need It*. <http://www.nist.gov/nstic/NSTIC-Why-We-Need-It.pdf>

⁹ <http://www.nist.gov/nstic/NSTIC-Why-We-Need-It.pdf>

The Role of DNSSEC in the Federal Enterprise

In August 2008, the Office of Management and Budget (OMB) issued Memorandum M-08-23, “Securing the Federal Government’s Domain Name Systems Infrastructure,” establishing the policy that the Federal Government would deploy DNSSEC to the top-level .gov domain by January 2009 and all Federal agencies must deploy DNSSEC by December 2009.¹⁰ Subsequently, in February 2009, the .gov domain was digitally signed, with DNSSEC deployed.¹¹ The annual Federal Information Systems Management Act (FISMA) Report coordinated by the Department of Homeland Security (DHS) tracks compliance with this mandate.^{12 13}

The Department of Homeland Security’s Federal Network Security (FNS) Branch¹⁴, performs scans to check for DNSSEC implementation in the Federal .gov namespace for second level domains. As of May 1, 2011, scans showed approximately 10 percent DNSSEC compliance.¹⁵ Since that time, FNS has been sending weekly and monthly compliance reports to Federal departments and agencies in order to inform them of their DNSSEC compliance status. As of October 24, 2011 DNSSEC compliance rates had risen to approximately 30%, the increase showing that on-going monitoring can significantly increase awareness of potential vulnerabilities.

The intent of DNSSEC is to address a number of vulnerabilities in the design of the DNS protocol, which translates easy to remember domain names into Internet Protocol (IP) addresses. DNS saves human users from needing to remember an IP address like “10.0.0.181,” and allows them to use a name easier to recall such as “www.whitehouse.gov” Several critical machine-to-machine, Internet-wide processes also use DNS.¹⁶ The technology supporting DNS is not without vulnerabilities¹⁷ that continue to affect the trust and confidence users should have in online transactions. Among those vulnerabilities is lack of assurance that a response to a DNS request delivers the accurate and authentic IP address desired. DNS cache poisoning, a type of malicious attack on DNS servers, changes DNS record information and redirects users to a new address. DNSSEC is designed to mitigate this type of vulnerability, among others.

DNSSEC is a set of modifications to the DNS protocol intended to provide DNS data integrity, authenticated denial of existence, and a trusted path of authentication for DNS data.¹⁸ In short, DNSSEC increases confidence the information returned in a DNS request is the information desired and is not corrupted. When

¹⁰ <http://www.whitehouse.gov/sites/default/files/omb/memoranda/fy2008/m08-23.pdf>

¹¹ Jackson, W. (2009, March 5). *Government Implements DNSSEC on the .gov Domain*. Retrieved May 11, 2011, from <http://gcn.com/Articles/2009/03/05/DNSSEC-on-dot-gov.aspx>

¹² http://www.whitehouse.gov/sites/default/files/omb/assets/memoranda_2010/m10-15.pdf

¹³ http://www.whitehouse.gov/sites/default/files/omb/assets/memoranda_2010/m10-28.pdf

¹⁴ FNS is a branch of the National Cyber Security Division (NCS), Office of Cybersecurity & Communications (CS&C) of the National Protection & Programs Directorate (NPPD), a Component of DHS.

¹⁵ [http://max.omb.gov/community/display/DHS/\(a+.mil+or+.gov+e-mail+address+is+required+for+access\)](http://max.omb.gov/community/display/DHS/(a+.mil+or+.gov+e-mail+address+is+required+for+access))

¹⁶ Computers also do their own address resolution. Also see, for example, Request for Comments (RFC) numbers 2782 (service location), 3568 (request routing), 4398 (storing public key certificates), 5782 (DNS white and black lists), and 5864 (AFS file location). It is also necessary to implement DKIM and SPF.

¹⁷ See RFC 3833 for an overview of the technical vulnerabilities that DNSSEC is designed to address (<http://www.rfc-archive.org/getrfc.php?rfc=3833>).

¹⁸ Arends, R., Austein, R., Larson, M., Massey, D., & Rose, S. (2005, March). *RFC 4033*. Retrieved June 2011, from Internet Engineering Task Force: <http://www.ietf.org/rfc/rfc4033.txt>

people type “www.whitehouse.gov” into a browser, they can have a measure of assurance the Web site they are directed to is the one they wanted to reach.

According to DHS, agencies are experiencing challenges in deploying DNSSEC. These challenges range from a lack of available commercial solutions to funding issues and technical problems. A 2010 presentation by DHS listed the following obstacles:¹⁹

- Vendor support capabilities or vendor solutions not ready
- Technical problems with signing software and key exchanges
- Lack of managed DNSSEC solutions
- Infrastructure upgrades needed
- Insufficient funding and resources
- Contractual barriers between vendors and agency subcomponents
- Personnel management and training required
- Communication of standards and governance guidance is inadequate

Similarly, NIST has surveyed agencies to understand obstacles to DNSSEC deployment. They have made these observations:

- Deployment of DNSSEC is an exercise in content management because existing agency practices in data management will guide deployment decisions for DNSSEC.
- Agencies may find key management to be difficult, and the logistics of key re-signing can be particularly challenging.
- Interagency communication about DNS management, including information about points of contact for DNS information, is challenging because many agencies have not maintained DNS registrar information with the General Services Administration (GSA).
- The difference in equipment age and capabilities in the Federal computing environment means that not all agencies need to purchase new equipment to implement DNSSEC; upgrading technology may be a viable option for the majority of agencies. In some cases, budget issues can slow agency deployment.
- Agencies need to protect DNS data to the same degree that they protect encryption keys. The DNS database is just as important to DNSSEC as the keys are.
- Documenting agency processes and policies is important, as is management of changes in personnel who have logins for dotgov.gov or are otherwise important to DNS management.²⁰

¹⁹ Department of Homeland Security. (2010, March 24). *Getting DNSSEC into Trusted Internet Connections (TIC)*. Retrieved May 13, 2011, from https://www.dnssec-deployment.org/wp-content/uploads/2010/03/Donelan_Logistics_free-ed.pdf

²⁰ Rose, S., & NIST. (2011). “DNS Security Extensions (DNSSEC) Briefing.” *DBSSEC Tiger Team*.

Some of these challenges can be overcome only through administrative changes, including restructuring of vendor agreements to require DNSSEC; financial allocations for infrastructure upgrades; and policy changes. One example of how policies are being changed to support DNSSEC adoption is Trusted Internet Architecture, a component of the Trusted Internet Connection (TIC) initiative from the Comprehensive National Cybersecurity Initiative of 2008.²¹ Plans for the next version of the TIC architecture include a requirement for DNSSEC. Another example is found in the Federal Risk and Authorization Management Program (FedRAMP), which requires DNSSEC. In October 6 2011, John Curran, President & CEO of the American Registry for Internet Numbers (ARIN) provided testimony before the House Subcommittee on Cybersecurity, Infrastructure Protection, and Security Technologies. Mr. Curran discussed security implications for the Government when using cloud computing, noting the importance of the FedRAMP program. He also spoke to the importance of the Government's adoption of standards regarding IPv6 and DNSSEC, and how their adoption can shape the Internet at large. He noted:

"These new standards are quite important in protecting the global Internet from cybercrime, in that they insure that Internet users reach the actual web site that they intended to, and that their communication is protected in the process. When it comes to agency use of cloud computing services, these protections are equally important, since these services are reached over the public Internet."²²

Other challenges can be met by other means. For example, Federal agencies would benefit from adding resources for DNSSEC technical training. Two later sections of this paper will address the training challenge. The first section presents a small set of lessons learned for technicians working to deploy DNSSEC. These considerations, intended to ease the transition to DNSSEC, may not be readily apparent to people having no experience with such a deployment. The second section lists available educational resources for DNSSEC. An opportunity exists to develop a training program addressing the technical deployment of DNSSEC for Federal employees.

²¹ <http://www.whitehouse.gov/cybersecurity/comprehensive-national-cybersecurity-initiative>

²² <http://homeland.house.gov/sites/homeland.house.gov/files/Testimony%20Curran.pdf>

E-mail Authentication in the Federal Enterprise

Configuration management efforts like the Federal Desktop Core Configuration,²³ the Federal Server Core Configuration, and NIST Special Publication 800-53²⁴ promote systems configuration that reduces overall system attack surface and serve as a foundation for trust because consumers can make better decisions about risk when working with systems of a known configuration. E-mail authentication can provide both of these benefits to the Federal Government. To assist Agencies in their configuration management efforts, DHS has published the E-mail Gateway Reference Architecture on the OMB MAX portal.²⁵

*Homeland Security Presidential Directive 12: Policy for a Common Identification Standard for Federal Employees and Contractors (HSPD-12)*²⁶ established the requirement for a common, secure identity standard across the Federal Government. That policy provided the foundation for a number of trust services. E-mail is one technology that has been in desperate need of a restoration of user confidence. Like many technologies used today on the Internet, e-mail was not designed with any integrated requirements for trust or confidence. One consequence is that because of the many vulnerabilities found in its supporting technologies, common e-mail cannot be trusted to be authentic or unmodified.²⁷ A number of known e-mail vulnerabilities allow malefactors to alter the information in an e-mail message so as to dupe the unsuspecting reader; these vulnerabilities also enable malicious activities such as spamming and phishing.²⁸ The Federal Trade Commission noted that the conceptually simple act of ensuring accurate attribution of e-mail senders could reduce spam:

*“If the cloak of anonymity were removed, however, spammers could not operate with impunity. ISPs and domain holders could filter spam more effectively, and the government and ISPs could more effectively identify and prosecute spammers who violate the Controlling the Assault of Non-Solicited Pornography and Marketing Act of 2003 (the “CAN–SPAM Act”), 15 14335U.S.C. 7708, or other statutes.”*²⁹

The digital certificate(s) stored on the Personal Identity Verification (PIV) Card is one important way to authenticate e-mail messages and is a significant weapon in the battle against spam and other malicious e-mail activities. In Memorandum M-04-04, “E-Authentication Guidance for Federal Agencies” (2003), OMB stated that “authentication focuses on confirming a person’s identity, based on the reliability of his or her credential.”³⁰ The PIV Card is intended to establish a reliable credential for user access. Extending this

²³ http://nvd.nist.gov/fdcc/download_fdcc.cfm

²⁴ <http://csrc.nist.gov/publications/PubsSPs.html>

²⁵ <http://max.omb.gov/community/display/DHS/e-mail+Gateway> (a .mil or .gov e-mail address is required for access)

²⁶ http://www.dhs.gov/xabout/laws/gc_1217616624097.shtm

²⁷ A search of NIST’s National Vulnerability database in May 2011 (<http://nvd.nist.gov/home.cfm>) for the text string “SMTP” resulted in 217 hits.

²⁸ More information on e-mail scams can be found at http://www.us-cert.gov/reading_room/e-mailscams_0905.pdf.

²⁹ Federal Trade Commission. (2004, September 14). *www.ftc.gov*. Retrieved May 9, 2011, from <http://www.ftc.gov/os/2004/09/040915e-mailauthfrn.pdf>

³⁰ <http://www.whitehouse.gov/sites/default/files/omb/memoranda/fy04/m04-04.pdf>

reliability to e-mail between Government agencies should allow agencies to establish trusted communications with each other as well as more reliable e-mail communications between the Government and citizens.

When coupled with DNSSEC, e-mail authentication solutions provide badly needed integrity to the e-mail communication chain in a manner relatively transparent to the end user, and very little additional end-user education is necessary.

The two foundational technologies for e-mail authentication chosen for implementation by the Federal government are the Sender Policy Framework (SPF) and DomainKeys Identified Mail (DKIM). The Sender Policy Framework is a DNS based method for validating that a mail server that sends a message on behalf of an internet domain is authorized to do so. An internet domain may establish a policy defining which internet hosts may act as mail senders for that domain. This policy is established by the publication of a DNS policy record hosted by domain's authoritative DNS servers. SPF Policy records contain a domain specific language which specifies a list of internet hosts that are authorized to send mail on behalf of the domain, and how strict the enforcement of that list must be.

When a mail server receives an e-mail from an internet host, it extracts the domain from the sender's e-mail address and queries the authoritative DNS server for that domain for that domain's SPF policy record. It then matches the address or domain name of the sending host against the SPF policy record to determine if the sending host is allowed to send mail on behalf of that domain. The result of that policy check determines what the receiving mail server does with the received message (i.e. accept or reject).

DomainKeys Identified Mail is a protocol designed to allow the validation of the integrity and authenticity of e-mail received by an internet mail server. In the DKIM paradigm, all mail messages sent by or through a mail server are signed using the private portion of a public/private key pair unique to that mail server. This signature is intended to provide an undeniable proof that the mail was processed by a specific mail server, and that the message has not been modified in transit. The exact signature type and the information it covers in the e-mail header varies with the policy adopted by the implementer of the DKIM signing mail server. Verification of these signatures is performed by retrieving a DNS record containing the sending domain's public key, using information contained in the mail message header to locate the domain name server that contains the key.

Technically, e-mail authentication can be achieved through implementation of DomainKeys Identified Mail (DKIM), Sender Policy Framework (SPF), or both of them together. There are currently no policy requirements for implementation of e-mail authentication, but implementation is being tracked by FISMA reports. During the FY10 FISMA audits, the 24 large agencies reported a widely varying degree of e-mail authentication implementation. Only seven agencies reported close to 100% implementation, while others reported partial or no implementation³¹ DHS FNS is developing additional tools for trusted third party validation of e-mail authentication technologies across the Federal enterprise. These tools will provide the same degree of feedback and reporting currently available for DNSSEC deployments and help to provide continuous monitoring and improvement of e-mail authentication throughout the Federal enterprise.

³¹ http://www.whitehouse.gov/sites/default/files/omb/assets/egov_docs/FY10_FISMA.pdf

**CONSIDERATIONS AND LESSONS LEARNED FOR FEDERAL
AGENCY IMPLEMENTATION OF DNS SECURITY
EXTENSIONS AND E-MAIL AUTHENTICATION**

Federal CIO Council

DKIM and SPF are necessary first steps in a larger deployment of secure messaging standards for the Federal enterprise. The NSTIC clearly envisions a more formal method of e-mail authentication that uses HSPD-12 PIV cards to enable each Federal system user to digitally sign their electronic messages. Digital signatures would be easily verified through common validation mechanisms using the Federal Bridge as the root of trust for the Federal enterprise.

The Identity, Credential, and Access Management (ICAM) subcommittee of the Federal CIO Council's Information Security and Identity Management Committee (ISIMC) coordinates working groups to align the Government's identity management activities. ICAM administers Public Key Infrastructure (PKI) policies and enforces digital certificate standards in communications both within the Government and between the Government and external entities. This coordination is essential to ensure that all digitally signed messages originating from the Federal Government are independently verifiable by every recipient, regardless of the recipient's mail service provider.

Considerations for Implementation of DNSSEC, DKIM, and SPF

The FY10 FISMA reports indicate less than optimal adoption of DKIM, SPF, and DNSSEC authentication technologies. In light of these results, the Federal Network Security (FNS) branch of DHS chartered a tiger team to specifically address the implementation of DNSSEC and e-mail authentication. The Information Security and Identity Management Committee (ISIMC), under the Federal CIO Council structure, chaired the tiger team in conjunction with FNS and NIST. One of the tiger team's objectives is to foster sharing information about best practices, technical implementation hurdles, and lessons learned in overcoming them.

Department and agency implementation of authentication technologies falls short for several reasons, some social or political and some technological. These sometimes create disagreement between technical personnel and policy makers that are difficult to resolve; technical solutions do not always conform to policy constraints. To help alleviate such difficulties, the following sections identify common administrative and technical hurdles so that agencies can prepare to overcome them.

Management Considerations

1. Develop a Comprehensive Concept of Operations for the dotgov.gov DNSSEC Program

The concept of operations (CONOPS) would include information about deployment of DNSSEC, e-mail authentication, and other identity management technology. At least one agency has noted a substantial lack of guidance related to key management on the dotgov.gov portal.

2. Establish a Forum for Federal Network Operators and Technicians

A forum similar to the North American Network Operators' Group (NANOG) would improve communication for technicians in the Federal enterprise. Existing security-oriented forums could serve as models.

3. Consider Executive-Level Endorsement for e-mail Authentication

Previously this paper noted OMB Memorandum M-08-23, "Securing the Federal Government's Domain Name Systems Infrastructure," as a driver in the adoption of DNSSEC. Currently, there is no equivalent executive-level endorsement of the adoption of e-mail authentication technologies, though it has been a priority in a number of executive branch programs. The FY11 FISMA survey examined e-mail authentication, concluding that agencies must:

- "Provide the percentage of Agency e-mail systems that implement sender verification (anti-spoofing) technologies when sending messages to Government agencies or the public such as DKIM, SPF, or other.

- Provide the percentage of Agency e-mail systems that check sender verification (anti-spoofing technologies) to detect possibly forged messages from Government agencies known to send e-mail with sender verification such as DKIM or SPF or other.”³²

A second Federal initiative directly encouraging agencies to adopt e-mail authentication is the Trusted Internet Connection (TIC). Version 2 of the TIC architecture integrates Federal policies, such as OMB M-08-23, and requires e-mail authentication.³³

Some additional FISMA metrics could be considered:

- The number of unsigned agency domains
- Whether or not the agency has identified one or more points of contact for DNS
- The number of agency domains for which DNSSEC errors are reported

4. Take the Opportunity to Update Existing Executive Policy

Policy documents that mandate e-mail authentication are out of date. Policy can be improved by following the example set by DNSSEC mandates such as OMB M-08-23, which establishes implementation guidelines whose deadlines have now passed. Furthermore, Federal IT staffs have assumed that the policy applies to externally-facing DNS servers, with an additional requirement for agencies to develop roadmaps for internal deployment. This guidance should be reintegrated into the official policy to ensure a common understanding.

Lesson Learned

Since the original publication of this report, OMB has reaffirmed that M-08-23 applies to externally-facing DNS servers. *Domain Name System (DNS) Security Reference Architecture Version 1.0*, published by DHS on OMB Max, reinforces this policy.

5. Improve Documentation of DNS Policies and Procedures within Agencies

Agencies have reported difficulty in communicating with the GSA about DNS administration, due partially to outdated record keeping by agencies and the GSA. In many cases, DNS registrar information has not been kept current with personnel changes. Obsolete registrar POC information has become a barrier to DNSSEC deployment because GSA can no longer contact appropriate agency personnel to manage important DNS issues. Verisign serves as the name server operator for .gov. To enable effective zone maintenance and error correction capability, the GSA needs to keep its whois data up to date with agency contact information. Deployment of DNSSEC increases this need. Agencies need to examine their policies and procedures for maintenance of DNS registrar information and ensure that the GSA has up-to-date contact information for all agency DNS registrars.

³² FY 2011 Chief Information Officer Federal Information Security Management Act Reporting Metrics, Version 1.0, June 1, 2011. <http://max.omb.gov/community/display/DHS/e-mail+Gateway> (a .mil or .gov e-mail address is required for access)

³³ *Trusted Internet Connection (TIC) Reference Architecture v2.0 Update*. Retrieved June 15, 2011, from http://www.nitrd.gov/subcommittee/lisn/jet/material/TIC_UPDATE_2011-04-13.pdf

6. Establish and Expand Communities of Interest

A community of interest is a helpful tool for solving problems and overcoming obstacles. Currently, there is no Government community for e-mail authentication concerns, but one could be added to the NIST DNSSEC community of interest. The expansion could include an annual conference focusing on identity and access management technologies. Such a conference could include incentive programs for technology adoption, such as awards for the greatest number of signed domains and for the greatest percentage of namespace covered by DNSSEC.

Operational Considerations

1. Update Implementation Guidance

Guidance provided by the NIST and other Federal entities should be updated to reflect new technologies. For example, NIST Special Publication 800-45V2, *Guidelines on Electronic Mail Security*³⁴, last revised in 2007, does not address current technologies such as DKIM and SPF for e-mail authentication. Agencies would benefit from updated implementation guidance.

Lesson Learned

Update Disaster Recovery plans to include any new DNSSEC configuration, and test the plans to ensure they remain effective.

2. Understand Operational Challenges of Key Management

DKIM and DNSSEC rely on the security of the public-private key pairs used to sign and validate messages. One step in maintaining security is key rotation, the replacement of keys when their useful lifespan has expired. Unfortunately, neither DKIM nor DNSSEC have a mechanism to alert a validating client to a key rotation. The agency must manually enforce a grace period, during which both the old and new keys are to be considered valid. This problem makes the timing of a key rotation critical, as all messages in transit during a key rotation might be rejected as invalid. Some agencies, including the Department of State and NIST, have developed Perl scripts to assist with key management. At least one agency has noted a substantial lack of guidance and help text related to key management on the dotgov.gov portal.

Lesson Learned

Test key rollover in a dedicated testing environment before deployment.

3. Standardize DNSSEC Validation Criteria

In the course of evaluating Federal agencies' rate of DNSSEC adoption, different interpretations of deployment criteria caused some disagreements. Consistent evaluation of DNSSEC and e-mail authentication adoption by agencies will be ensured by common, standardized validation criteria based upon an agreed interpretation of the relevant RFCs.

³⁴ <http://csrc.nist.gov/publications/nistpubs/800-45-version2/SP800-45v2.pdf>

4. Maintain Communications with Registrar

Changes at the registrar will impact operations. For example, one agency reported that a recent upgrade from DNSSEC next secure (NSEC) records³⁵, for authenticated denial of existence, to the updated standard, NSEC3 records, had an unexpected impact exacerbated by inadequate communications.

Lesson Learned

The GSA helpdesk is a useful resource in navigating the dotgov.gov registration process.
e-mail: registrar@dotgov.gov

5. Maintain Ability to Perform DNS Testing

The Government has recently announced a moratorium on the issuance of new .gov domains as well as a desire to reduce the number of top-level domains by about half.³⁶ One agency has noted it will be important to allow agencies to continue to obtain test domains in the .gov space to support DNSSEC deployments. The Secure Naming Infrastructure Pilot (SNIP), maintained by NIST, was created to allow Federal agencies to test DNSSEC deployments instead of obtaining new .gov delegations.

Lesson Learned

Consider testing during off-peak hours, when the potential impact is reduced, and ensure that testing is performed from multiple external networks. Consider using mobile device networks to test your configuration.

There are a number of useful tools available to help diagnose and test DNSSEC. Some tools are available at <http://www.kloth.net/> and <http://dnsviz.net>.

6. Manage the Decommissioning and Retirement of Government Domains

A standard procedure for correctly decommissioning and retiring a Government Web site (domain and URL) would be useful. This would address the issue of lame domains where the .gov top-level domain still has delegation information for these zones but whose servers are unreachable or not responding. Because .gov says these zones exist, attackers can spoof these domains, and existing security measures (including DNSSEC) cannot stop them.

7. Conduct Training

Training, which is still in the early stages of development, is particularly important for all personnel implementing DKIM, DNSSEC, and SPF because the protocols being implemented require more careful and consistent management than their insecure predecessors. Adequate training puts a large financial and logistical burden on organizations and agencies, especially considering budgetary constraints. There are several websites dedicated to providing administrators resources to teach themselves about identity verification technologies, but the quality of those sites varies greatly. Appendix A describes several training and education resources. The Federal CIO council does not maintain these sites, so it can make no claims or warranties about their accuracy or continued support for their resources.

³⁵ DNS Security (DNSSEC) Hashed Authenticated Denial of Existence, <http://tools.ietf.org/html/rfc5155>.

³⁶ <http://www.whitehouse.gov/sites/default/files/omb/memoranda/2011/m11-24.pdf>

Technical Considerations

1. DNSSEC Requirement

For operational security, both DKIM and SPF require DNSSEC be configured on all agency DNS servers, because the information a client can use to validate SPF and DKIM signatures is stored in the agency's DNS system, but the information does not have any inherent protection from spoofing, poisoning, man-in-the-middle, or other network-based attacks. DNSSEC is intended to provide protection for all records stored on or transmitted by the server, and to create a root of trust for any DNS-based cryptographic system. The 2010 FISMA audit revealed only 35 percent of second-level domains in the .gov namespace were signed and had a valid chain of trust to the .gov domain.

2. DNS Vulnerability to Caching Resolvers (Implementation)

An integral part of the DNS protocol, caching resolvers, are used to minimize the amount of DNS-related traffic sent across the Internet by locally caching a network's most frequently queried information. Although DNS records have a Time To Live (TTL) that is expected to limit their useful life span, DNS caching resolvers are not required to honor the specified TTL. DNS records may stay in a resolver's cache for an indeterminate amount of time³⁷ before they are refreshed (queried anew from the authoritative server). This could cause a problem when records (keys, signatures, and policies) for DKIM, DNSSEC, and SPF are changed on the authoritative DNS server, but those changes are not adopted by the caching resolver. Any client served by the caching resolver will receive out-of-date information that can, and likely will, cause DKIM, DNSSEC, and SPF transactions to fail unless very careful record management practices are in place.³⁸

Lesson Learned

Expect poorly configured caching servers on the Internet to present challenges during both testing and implementation.

3. Challenges of Complexity

Using DKIM, DNSSEC, or SPF could change the network traffic profile of the agency. Some of these traffic changes may be incompatible with existing network or security architecture. SPF and DKIM utilize DNS, which the Mail Transfer Agent (MTA) should already implement. Generally, these two technologies would not cause as many changes as DNSSEC. For example, DNSSEC packets are much larger than DNS packets. This could cause many nuances of configuration to interfere with packet transfer. User Datagram Protocol (UDP) packets may need to have jumbo frames enabled or may be fragmented on the wire. Fragmented packets, however, should generally be dropped by firewalls, due to security concerns, and jumbo packet frames are not supported by older hardware. This may cause DNS transmission to fail over to Transmission Control Protocol (TCP), to allow fragmentation at the transport layer rather than the datalink layer. Zone transfers, however, usually occur only over TCP port 53, so a

³⁷ Technically, the maximum time to live (TTL) is just over 68 years (RFC 1035 section 2.3.4), but, practically speaking, this is an indeterminate amount of time.

³⁸ Morris, S., Ihren, J., and Dickinson, J. (March 2011). *DNSSEC Key Timing Considerations*. (Draft) Retrieved May 18, 2011, from <http://tools.ietf.org/html/draft-ietf-dnsop-dnssec-key-timing-02>

sound firewall policy would block such (now possibly legitimate) traffic. In addition, an agency has reported problems with load balancers when changing a CNAME record to an A record. Such configuration issues are likely to occur if the agency upgrading the protocols does not have a good grasp of its internal configurations and policies.

Lesson Learned

Complexities in different networks have yielded an array of recommendations and implementation lessons.. For DNSSEC, these include the following:

- Ensure recursive and authoritative DNS servers are not the same machines
- Eliminate split-brain (split-horizon) DNS from your environment
- When implementing DNSSEC, stand up new DNS servers rather than upgrading or modifying existing servers. This facilitates rapid back-out and restoration to the previous state in the event something goes wrong
- Identify the correct points of contact for technical and managerial authority over DNS
- Use dotgov.gov capabilities to enable an agency-wide view of your domain inventory.
- Ensure your current infrastructure can support DNSSEC
- DNSSEC increases the size of DNS packets above the original UDP packet limit of 512 bytes. When this occurs, a client could attempt to use TCP port 53 instead. Some organizations may still have packet filtering rules to block DNS over TCP

For DKIM and SPF, additional lessons include the following:

- Use SPF and DKIM in combination to ensure the sending message server is permitted to send (SPF) and to ensure the authenticity of the digital signature (DKIM)
- Coordinate DKIM and SPF adoption across all current mail relays
- Use SPF for domains that will never send e-mail
- Test all DKIM and SPF rulesets for correctness in a simulated environment before deployment

4. Lack of Major Vendor Support for DKIM and SPF

IBM Lotus Notes and Domino 8.5, and Microsoft Exchange 2010, the latest versions of the most popular mail server software applications used by the Federal Government, do not natively support either DKIM or SPF. Many third-party add-ons for these mail servers provide DKIM, SPF, or both, such as SpamAssassin³⁹ and e-mailArchitect,⁴⁰ but these products may not have a FISMA compliant configuration, and they often significantly increase the administrative and training burden associated with e-mail servers.

³⁹ <http://spamassassin.apache.org/>

⁴⁰ <http://www.e-mailarchitect.net/>

5. Replay and Message Content Protection

Although DKIM is intended to provide message security and sender authentication, DKIM does not protect against resending (replay) of a message that already has a valid signature. Therefore, a transit intermediary or a recipient could repost the message in such a way that the signature would remain valid, though the new recipient(s) would not have been specified by the originator. This has implications for both insider threats and spam creation, both of which would persist under the DKIM framework. SPF is not intended to protect messages in transit or to prevent replay attacks but merely to identify what mail servers are allowed to send mail on behalf of a specific domain. DKIM and SPF can be used together to potentially offset some replay attack weaknesses. DKIM-protected mail messages subject to an SPF policy that only allows mail to be sent from specific servers makes spoofing and replaying mail significantly more difficult.

6. Reputation Policy

DKIM message processing is based on the concept of each e-mail domain having a reputation, and its mail servers accepting messages only from domains with a good reputation. The reputation of a sender domain and the required value for a good reputation depend entirely on the domain receiving the message. If all Federal agencies were allowed to set their own policies, or were subject to different policies by external receivers (Google, Yahoo!, etc.), mail delivery to and from any number of domains could very easily be unnecessarily complicated. A consistent reputation policy and value system is essential to a rollout of DKIM across all Federal agencies.

Conclusion

As remote digital transactions over the Internet become increasingly important in every citizen's daily life, it becomes increasingly critical these transactions have the same level of authenticity as face-to-face transactions. The current state of the Internet in general and of its use by Federal civilian agencies specifically, falls well short of that goal. Well-reasoned and established protocols (DNSSEC, DKIM, and SPF) exist for e-mail and name resolution (with DNS) that can greatly increase the authenticity of these digital interactions. Because these three technologies underpin almost all transactions on the Internet, securing them has both a high priority and high return on investment. Exploitation of information resources by organized actors is commonplace and will only continue to grow without user action. The technologies discussed in this document provide a foundation for and are important steps to properly adopt DNSSEC and e-mail Authentication.

Appendix A: Training and Resources for DKIM, SPF, and DNSSEC

DKIM Training and Resources

The Messaging Anti-Abuse Working Group (MAAWG) has a free online introduction and training presentation for DKIM that is about 90 minutes long: <<http://www.maawg.org/activities/training/dkim-video-list>>. The PowerPoint slides for the presentations are also available there for reference. MAAWG also organizes general meetings and international efforts to prevent message abuse, and it maintains many other useful resources on its Web site, <<http://www.maawg.org>>. Additional information on best practices is available at the Sendmail Web site: <http://www.sendmail.com/sm/wp/dkim_deploy_best_practices/43x_dkim_deploy_thanks/>.

SPF Training and Resources

The Web site <<http://www.openspf.org>> has various resources available, including a browser-based tool with a well-explained interface. The tool will create SPF records for a domain; see <<http://old.openspf.org/wizard.html>>. The site also supports a variety of mailing lists and forums where users can get help setting up all aspects of the SPF process. A description of the different mailing lists and forums is available at <<http://www.openspf.org/Forums>>.

More Web-based tools for testing and validating SPF deployment and records are available at <<http://www.kitterman.com/spf/validate.html>>.

DNSSEC Training and Resources

NIST has produced a guide to securing DNS resources. NIST SP 800-81, “Secure Domain Name System (DNS) Deployment Guide,” contains guidance on much more than DNSSEC. Section 9 provides detailed instructions for enabling DNSSEC in BIND and NSD.⁴¹

The DHS Federal Network Security branch has produced a number of reference architecture documents (available on OMB MAX <<https://max.omb.gov/maxportal/>>). Among these is “Domain Name System (DNS) Security Reference Architecture Version 1.0.”

An open source solution for signing an unsigned DNS zone and passing it to the zone’s authoritative name servers is available at <<http://www.opendnssec.org>>. The community also maintains a set of training materials on OpenDNSSEC at <<http://www.opendnssec.org/documentation/training/>> as well as a wiki for additional information, questions, and community and consulting support. Additional resources are available at <www.dnssec-deployment.org>.

Sandia National Laboratory has developed a Web-based tool to visualize and externally test how a DNSSEC appears to the outside world. It is available at <<http://dnsviz.net>>.

⁴¹ NIST. (March 2011). *NIST Special Publication SP 800-39 Managing Information Security Risk: Organization, Mission, and Information System View*. <http://csrc.nist.gov/publications/nistpubs/800-39/SP800-39-final.pdf>

There is also an open source toolset that can be used to implement DNSSEC in various common Windows and UNIX software applications (versions of programs such as OpenSSH, Firefox, and wget are available) and to visualize DNSSEC testing. This toolset complements the Sandia tools because it allows visualization from the inside of the organization going out, rather than from the outside in. The set is available at <http://www.dnssec-tools.org>.

The Internet Systems Consortium (ISC) writes and maintains BIND, the most popular DNS server implementation. BIND is open source, and the documentation for current releases is available at <http://www.isc.org/software/bind/documentation>. BIND 9 is DNSSEC enabled, and the documentation contains DNSSEC implementation information specific to the BIND release. The above Web page also contains links to FAQs about BIND and links to further resources for DNSSEC and DNS in general.

Additional Resources

Virtual Training Environment (VTE) -Federal agencies looking for a way to rapidly train large groups of employees on core Information Security issues should consider evaluating the material and capabilities in VTE. DHS is making access available to the Federal Civil Workforce in advance of the gov-wide rollout in FY10 in conjunction with the Department of State Foreign Service Institute <https://www.vte.cert.org/vteWeb/RequestAccess/FISMAProgram.aspx>

Secure Name Infrastructure Pilot (SNIP) <http://www.dnsops.gov/>

NIST IPv6/DNSSEC monitor <http://usgv6-deploymon.antd.nist.gov/>

DNSSEC Deployment Initiative <http://www.dnssec-deployment.org/>

DNSSEC.net Resource page <http://www.dnssec.net/>