BUILDING BLOCK WHITE PAPER

DOMAIN NAME SYSTEM-BASED SECURITY FOR ELECTRONIC MAIL

William C. Barker
Information Technology Laboratory
National Institute of Standards and Technology

FINAL DRAFT
March 4, 2016
dns-email-nccoe@nist.gov

This revision incorporates comments from the public.

The National Cybersecurity Center of Excellence (NCCoE) at the National Institute of Standards and Technology (NIST) works with industry, academic and government experts to find practical solutions for businesses' most pressing cybersecurity needs. The NCCoE collaborates to build open, standards-based, modular, end-to-end reference designs that are broadly applicable and help businesses more easily align with relevant standards and best practices. To learn more about the NCCoE, visit http://nccoe.nist.gov. To learn more about NIST, visit http://www.nist.gov.

NCCoE building blocks address technology gaps that affect multiple industry sectors.

ABSTRACT

The Domain Name System-Based Security for Electronic Mail project will produce a proof of concept security platform that will demonstrate trustworthy email exchanges across organizational boundaries. The product of the project will include authentication of mail servers, signing and encryption of email, and binding cryptographic key certificates to the servers. Domain Name System Security Extension (DNSSEC) protocols will be used to authenticate server addresses and certificates by binding the X.509 certificates used for Transport Layer Security (TLS) to DNS names verified by DNSSEC. The business value of the security platform that will result from this project will not only improve privacy and security protection for users' operations, but will also expand the set of available DNS security applications and encourage wider implementation of the protocols that provide Internet users confidence that entities to which they believe they are connecting are the entities to which they are actually connecting. This project will result in one or more demonstration prototype DNS-based secure email platforms, a publicly available NIST Cybersecurity Practice Guide that explains how to employ the platform(s) to meet Federal and industry security and privacy requirements, platform documentation necessary to compose a DNS-based email security platform from off-the-shelf components, and any recommendations for improvements to applicable standards documentation. The secure email project will involve composition of a variety of components that will be provided by a number of different vendors. Client systems, DNS/DNSSEC services, mail transfer agents, and certificate providers (Certificate Authorities or CAs) are included. The NCCoE is currently entering into cooperative research and development agreements with technology providers for components and expertise including DNS resolvers (stub and recursive) for DNSSEC, authoritative DNS servers for DNSSEC signed zones, mail servers and mail security components, and extended validation and domain validation TLS certificates.

KEYWORDS

cryptographic key, cryptography, Domain Name System (DNS), DNS-based Authentication of Named Entities (DANE), Domain Name System Security (DNSSEC), electronic mail (email), privacy, security

DISCLAIMER

Certain commercial entities, equipment, or materials may be identified in this document in order to describe an experimental procedure or concept adequately. Such identification is not intended to imply recommendation or endorsement by NIST or NCCoE, nor is it intended to imply that the entities, materials or equipment are necessarily the best available for the purpose.

COMMENTS ON NCCOE DOCUMENTS

Organizations are encouraged to review all draft project publications during public comment periods and provide feedback. All publications from NIST's National Cybersecurity Center of Excellence are available at http://nccoe.nist.gov.

ACKNOWLEDGEMENTS

The following individuals have made significant contributions to this document. Their assistance is greatly appreciated.

Name	Organization
Burt Kaliski	Verisign Labs
Allison Mankin	Verisign Labs
Joe Gersch	Secure64 Software
Janet Jones	Microsoft
Doug Montgomery	NIST, ITL, Advanced Network Technologies Division
Scott Rose	NIST, ITL, Advanced Network Technologies Division

TABLE OF CONTENTS

1. Executive Summary

Both public and private sector business operations are heavily reliant on electronic mail (email) exchanges. The need to protect business plans and strategies; the integrity of transactions, financial, and other proprietary information; and privacy of employees and clients are only three of the factors that motivate organizations to secure their email exchanges. Whether the security service desired is authentication of the source of an email message, assurance that the message has not been altered by an unauthorized party, or confidentiality of message contents, cryptographic functions are usually employed in providing the service. Economies of scale and a need for uniform security implementation drive most enterprises to rely on mail servers and/or Internet service providers (ISPs) to provide security to the members of an enterprise rather than end-to-end security mechanisms operated by individual users. Many current server-based email security mechanisms are vulnerable to, and have been defeated by, attacks on the integrity of the cryptographic implementations on which they depend. The consequences frequently involve unauthorized parties being able to read or modify supposedly secure information, or to use email as a vector for inserting malware into the system that is intended to deny access to critical information or processes or to damage or destroy system components and/or information. Improved email security can help protect organizations and individuals against these consequences and also serve as a marketing discriminator for email service providers while also improving the trustworthiness of enterprise email exchanges.

Domain Name System Security Extensions (DNSSEC) for the Domain Name System (DNS) are technical mechanisms employed by Internet service providers to protect against unauthorized modification to the DNS, the system which converts domain names (e.g., .com, .gov, .org) to Internet Protocol (IP) addresses. DNS-based Authentication of Named Entities (DANE) is a protocol that securely associates domain names with cryptographic certificates and related security information so that they can't be fraudulently modified or replaced to breach security. In spite of the dangers of failure to authenticate the identities of network devices, adoption of DNSSEC has been slow. Demonstration of DANE-supported applications such as reliably secure email may support increased user demand for domain name system security. Follow-on projects might include HTTPS, IOT, IPSEC keys in DNS, and DNS service discovery.

The current project will demonstrate a proof-of-concept security platform, composed of off-the-shelf components, that provides trustworthy mail server-to-mail server email exchanges across organizational boundaries. The DANE protocol will initially be used to authenticate servers and certificates in two roles in the DNS-Based Security for Email Project:

By binding the X.509 certificates used for

1. Transport Layer Security (TLS) to DNS names verified by DNSSEC and supporting the use of these certificates in the mail server-to-mail server communication;

2. Secure Secure/Multipurpose Internet Mail Extensions (S/MIME) to email addresses encoded as DNS names verified by DNSSEC.

These bindings support trust in the use of S/MIME certificates in the end-to-end email communication. The resulting building block will encrypt email traffic between servers, allow individual email users to digitally sign and/or encrypt email messages to other end users, and allow individual email users to obtain other users' certificates in order to validate signed email or send encrypted email. The project will include an email sending policy consistent with a stated privacy policy that can be parsed by receiving servers so that receiving servers can apply the correct security checks and report back the correctness of the email stream. Documentation of the resulting platform will include statements of the security and privacy policies and standards (e.g., Executive Orders, NIST standards and guidelines, IETF RFCs) supported, technical specifications for hardware and software, implementation requirements, and a mapping of implementation requirements to the applicable policies, standards, and best practices.

The secure email project will involve composition of a variety of components that will be provided by a number of different vendors. Client systems, DNS/DNSSEC services, mail transfer agents, and certificate providers (CAs) are generally involved. Collaborators are being sought to provide components and expertise for DNS resolvers (stub and recursive) for DNSSEC, authoritative DNS servers for DNSSEC signed zones, S/MIME certificates mail servers and mail security components, extended validation and domain validation TLS certificates. Although this initial project description focuses on SMTP over TLS and S/MIME, it does not necessarily rule out inclusion of other off-the-shelf standards-based components and capabilities that are compatible with DNSSEC. Comments and suggestions regarding approaches to achieving the project goal are solicited.

This project will result in one or more demonstration prototype DNS-based secure email platforms, a publicly available NIST Cybersecurity Practice Guide that explains how to employ the platform(s) to meet security and privacy requirements, and platform documentation necessary to compose a DNS-based email security platform from off-the-shelf components.

This project description includes

1. a statement of the business value to be derived from adoption and use of the building block
2. a description of the purpose of, scope of, and assumptions underlying the project
3. usage scenarios to be demonstrated in the course of the building block project
4. our current perception of the challenges to our meeting the project goals
5. standards and policies that will be used by the project team to inform project activities

6. characteristics of the products of the project
7. identification of security categories in the Framework for Improving Critical Infrastructure Cybersecurity (CSF) that adoption of the building block will help organizations to satisfy
8. a high-level diagram of email functionality where DNS-based security for email is used
9. a list of anticipated building block project components

A general description of threats to server-based email exchanges and potential consequences of exploitation of unprotected email and email whose protection has been bypassed or defeated is included as Appendix A.

1.1 Business Value

Sectors across industries, as well as the federal government, are concerned about email security and the use of email as an attack vector. Both public and private sector business operations are heavily reliant on email exchanges. The need to protect business plans and tactics; the integrity of transactions, financial and other proprietary information; and privacy of employees and clients are among the factors that motivate organizations to secure their email. Whether the service desired is authentication of the source of an email message, assurance that the message has not been altered by an unauthorized party, or message confidentiality, cryptographic functions are usually employed. Economies of scale and a need for uniform implementation drive most enterprises to rely on mail servers to provide security to the members of an enterprise rather than end-to-end security operated by individual users. Many server-based email security mechanisms are vulnerable to attacks involving

- faked or fraudulent key certificates
- otherwise invalid certificates
- failure to actually invoke a security process as a result of connection to or through a fraudulent server.[1]

The consequences often involve unauthorized reading or modification of information or fraudulently causing legitimate parties to bypass the protection mechanisms altogether. Worse, users continue to click on links to malware-ridden websites in fraudulent emails, a major factor in most confirmed data breaches. Improved email security can both serve as a marketing discriminator for email service providers and improve the security of enterprise email exchanges. DNSSEC protects against unauthorized modifications to network management information and host IP addresses. In spite of the dangers of failure to authenticate the identities of network devices, adoption of DNSSEC has been

[1] "How Cybercrime Exploits Digital Certificates," Infosec Instutute, General Security, July 28, 2014, http://resources.infosecinstitute.com/cybercrime-exploits-digital-certificates

slow. Demonstration of DNSSEC-supported applications such as reliably secure email will support increased user demand for domain name system security.

The business value of the security platform that results from this project will include improved privacy and security protections for users' operations, as well as expansion of the set of DNS security applications. It will encourage wider implementation of the protocols that provide Internet users with confidence that entities to which they believe they are connecting are the entities to which they are actually connecting.

2. DESCRIPTION

2.1 Purpose of the document

This document is intended to elicit comments regarding the utility of DNS-based secure email; the proposed approach to composing a DNS-based secure email platform; interest in participating in a DNS-based secure email proof-of-concept demonstration; characteristics that are desired or required in a DNS-based secure email platform; and provide technical, implementation, standards, and best-practices documentation required to make a DNS-based secure email platform a useful and desirable element of organizations' information technology infrastructures.

2.2 Audience

The NCCoE is seeking providers of off-the shelf information technology security products who can contribute components and expertise to the development a proof-of-concept security platform that provides trustworthy mail server-to-mail server email exchanges across organizational boundaries. Particular products and expertise sought include email client systems, DNS/DNSSEC services, mail transfer agents, and X.509 cryptographic key certificate sources (components and services). Collaborators are being sought to provide components and expertise for DNS resolvers (stub and recursive) for DNSSEC, authoritative DNS servers for DNSSEC signed zones, S/MIME certificates mail servers and mail security components, extended validation and domain validation TLS certificates. Although this initial project description focuses on SMTP over TLS and S/MIME, it does not necessarily rule out inclusion of other off-the-shelf standards-based components and capabilities that are compatible with DNSSEC. Comments and suggestions regarding approaches to achieving the project goal are solicited.

Anticipated users for the product of this activity include IT systems owners and administrators and organizations and individuals who desire reliable negotiation of security services and reliable sources of keying material for cryptographic source authentication, content integrity protection, and confidentiality protection. Comments regarding desirable performance, security, cost, integration, and usability characteristics for the building block are also solicited.

2.3 Goal

The DNS-based secure email building block project will demonstrate a security platform that provides trustworthy email exchanges across organizational boundaries. The project includes authentication of mail servers, signing and encryption of email, and binding cryptographic key certificates to the servers.

2.4 Background

Both private industry and the government are concerned about email security and the use of email as an attack vector for cyber crime. Business operations are heavily reliant on email exchanges and need to protect the confidentiality of business information, the integrity of transactions, and privacy of individuals. Cryptographic services are used to authenticate the source of email messages, protect against undetected unauthorized alteration of messages in transit, and maintain message confidentiality. Efficiency and policies support reliance on mail servers to provide cryptographic protection for email rather than on end-to-end security operated by individual users. However, organizations need to protect their server-based email security mechanisms against intrusion and man-in-the-middle attacks during the automated cryptographic service negotiation process. In the absence of an appropriate combination of DNSSEC and certificate-based protections, any of these attacks can result in reading or modification of information by unauthorized third parties. The attacks can also enable an attacker to pose as one of the parties to an email exchange and send email that contains links to malware-ridden websites. If other content in a fraudulent message successfully motivates the user to click on the link or the user's system is configured to automatically follow some links or download content other than text, the malware will infect the user's system. Inclusion of links to malware is a major factor in most confirmed data breaches. Consequences of such breaches can range from exposure of sensitive or private information, to enabling fraudulent activity by the attacker posing as the victimized user, to disabling or destroying the user's system—or that of the user's parent organization. Beyond avoidance of negative consequences to users, improved email security can also serve as a marketing discriminator for email service providers.

DNSSEC protects against unauthorized modifications to domain name information and consequent connection to incorrect devices. In spite of the dangers of failure to authenticate the identities of network devices, adoption of DNSSEC has been slow. Demonstration of DNSSEC-supported applications such as reliably secure email will support increased user demand for domain name system security.

2.5 Scope

The scope of this building block project includes demonstration and explanation of how to effectively implement a security platform composed of off-the-shelf components that provides trustworthy mail server-to-mail server email exchanges across organizational boundaries. The DNSSEC-based DANE protocol will be used to authenticate servers and certificates by binding the X.509 certificates used for TLS to DNS names verified by

DNSSEC (example references include IETF RFCs 6394, 6698, 7218, 5321, 5751, draft-ietf-dane-smime-02, and draft-ietf-dane-smtp-with-dane-17). This project will provide tools to encrypt email traffic between servers, allow individual email users to digitally sign and/or encrypt email messages to other end users, and allow individual email users to obtain other users' certificates in order to validate signed email or send encrypted email. In addition, the secure email platform or organization responsible for the email platform will generate information that can be queried by email recipients to identify valid email senders for a domain and that a given message originated from one of the valid senders. The project will include an email sending policy consistent with a stated security policy that can be parsed by receiving servers so that receiving servers can apply the correct security checks and report back the correctness of the email stream. Documentation of the resulting platform will include statements of security and privacy policies and standards (e.g., IETF RFCs) supported, technical specifications for hardware and software, implementation requirements, and a mapping of implementation requirements to the applicable policies, standards, and best practices. The secure email project will involve composition/adaptation of a variety of off-the shelf components, some potential sources for which have been identified.

2.6 Assumptions

The DNS-based secure email building block project assumes, and is dependent upon, the availability of off-the shelf information technology security products for and subject matter experts on trustworthy mail server-to-mail server email exchanges across organizational boundaries. Particular products and expertise on which the project is dependent include those for client systems, DNS/DNSSEC services, mail transfer agents, and X.509 cryptographic key certificate sources (CA's and certificate management components). DNS resolvers (stub and recursive) for DNSSEC validation, authoritative DNS servers for DNSSEC signed zones, and mail server/mail security components.

3. Scenarios

The building block project currently envisages two usage scenarios for DANE-enabled secure email:

1. "ordinary" email where the email exchanges between two organizations' email servers are carried over TLS, and the TLS key management is protected by DANE and DNSSEC
2. end-to-end signed email, where the email exchanges between organizations are carried over TLS as in (1), the email messages are signed and verified with S/MIME on the end-users' client devices, and the S/MIME key management is protected by DANE and DNSSEC

In both scenarios, private certificates are generated by Certificate Authorities (CAs). Self-signed certificates will not be used in either scenario.

This building block does not include an end-to-end encrypted email scenario; for example, a scenario in which the email messages are encrypted and decrypted with S/MIME on the end-users' client devices.

In the two supported scenarios, encryption is performed on bulk exchanges between email services. The only per-message cryptography is digital signatures. This addresses the main security concerns in enterprise environments, which are the target of the project, but not necessarily those of individual users who may also want to reduce information disclosure to their email providers. The two scenarios that are included may serve as enablers for end-to-end encryption. Participation by parties having a primarily end-to-end encryption focus may succeed in generating industry support for the building blocks needed to support end-to-end encryption.

3.1 Usage Scenario 1

An individual needs to enter into an email exchange with an individual in another organization that requires transfer of protected personally identifiable information (PII). Each individual exchanges email via the respective parent organizations' mail servers. User connections to their organizations' respective mail servers are established and maintained within a physically protected zone of control.

The privacy policy of the parent organizations requires encryption of the PII being exchanged. The security afforded by the cryptographic process is dependent on the confidentiality of encryption keys such that no unauthorized third party has access to the encryption keys employed. The mail servers are configured to use X.509 certificates that convey keying material to protect the integrity of the encryption keys during an encryption key establishment process. DNSSEC protocols are employed to ensure that each sending mail server is actually connected to the legitimate and authorized receiving mail server from which its X.509 certificate is obtained.

DNSSEC protocols are used to provide assurance that the originating user's mail server connects to the intended recipient's mail server. DANE protocols are employed to bind the cryptographic keying material to the appropriate server. TLS protocols are employed to negotiate the cryptography and protocols to be employed in the email exchange in which the PII is transferred. Encryption of the email message is accomplished by the originator's email server, and decryption of the email message is accomplished by the recipient's email server using the X.509 certificate and standard server libraries.

Demonstration of the security platform in this scenario will include an attempt by a fraudulent mail server to pose as the legitimate mail server for the receiver of the email and a man-in-the-middle attacker to attempt to notify the originating party that no encryption service is available for the desired destination with the objective of achieving an unencrypted transmission of the email. Both attempts should fail due to use of DNSSEC/DANE protocols.

3.2 Usage Scenario 2

An individual needs to enter into an email exchange with an individual in another organization that authorizes transfer of a large sum of money from the originator's organization to the recipient's organization. Each individual exchanges email via the respective parent organizations' mail servers. User connections to their organizations' respective mail servers are established and maintained within a physically protected zone of control.

The policy of the parent organizations requires cryptographic digital signature of the transaction to maintain integrity protection for the exchange (authorized source and destination, and content unchanged from that entered by the sender). The security afforded by the cryptographic process is dependent on the confidentiality of signature keys such that no unauthorized third party has access to the secret keys employed. S/MIME is the protocol used for electronic mail. Each organization generates X.509 certificates for their users to encode the public portion of their signature key. These certificates are then encoded in the DNS using the appropriate DANE DNS record type.

DNSSEC protocols are used to provide assurance that the originating user's mail server connects to the intended recipient's mail server. DANE protocols are employed to bind the cryptographic keying material to the appropriate server and individual user digital signature certificates. TLS protocols are employed to negotiate the cryptography to be employed in the email exchange in which the authorization is provided for the funds transfer. Digital signature of the email message is accomplished by the originator's email client, and checking the correctness of the signature (hence the integrity of the authorization provided in the email message is accomplished by the recipient's email client).

Demonstration of the security platform in this scenario will include an attempt by a fraudulent actor to pose as the originator of the email and a man-in-the-middle attacker to attempt to notify the receiving party that no digital signature certificate is available for the purported sender with the objective of achieving an unsecured transmission of the email. Both attempts should fail due to use of DNSSEC/DANE protocols.

4. Current Building Block Challenges

The DNS-Based Email Security building block faces some technical challenges, such as split DNS resolution, limitations of DNSSEC as a trust model, security and usability trade-offs in provisioning of certificates in DNS zone files, and DNS-based queries for individuals and groups, and extension to additional protocols. However, the success of the building block effort will be heavily dependent on our ability to address the following business challenges:

4.1 First Challenge

For the building block to result in the building block's adoption in the marketplace and in its effective use, participation by client systems and mail server developers and vendors is essential and requires the implementation of the new servers by a significant number of participants.

4.2 Second Challenge

The security platform resulting from this building block project will require X.509 certificate sources from established CAs if it is to result in large-scale adoption.

4.3 Third Challenge

The security platform involves composition of a significant number of components from different vendors. Although application program interfaces(APIs) have been developed that should permit interoperability, long-term support of these APIs will have to be developed to provide stability in the face of version changes to individual components.

5. Relevant Standards

Standards relevant to the building block described in this initial plan include the following:

- Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile; IETF RFC 2459; Housley (SPYRUS), Ford (Verisign), Polk (NIST), Solo (Citicorp); January 1999
- Security Requirements for Cryptographic Modules, Federal Information Processing Standard (FIPS), FIPS 140-2, May 2001
- Federal S/MIME V3 Client Profile, NIST Special Publication, SP 800-49, Chernick, November 2002
- Threat Analysis of the Domain Name System (DNS), IETF RFC 3833, Atkins (IHTFP Consulting) and Austein (ISC), August 2004
- Guidelines on Electronic Mail Security; NIST Special Publication; SP 800-45 Ver. 2; Tracy, Jansen, Scarfone, Butterfield; February 2007
- Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile; Proposed Standard; IETF RFC 5280; Cooper (NIST), Santesson (Microsoft), Farrell (Trinity College, Dublin), Boeyen (Entrust), Housley (Vigil Security), Polk (NIST); May 2008
- Securing the Federal Government's Domain Name System Infrastructure, Executive Office of the President, Office of Management and Budget, Memorandum for Chief Information Officers, M-08-23, August 22, 2008
- Internet Message Format, IETF RFC 5322, Resnick, October 2008
- Simple Mail Transfer Protocol, IETF RFC 5321, Draft Standard, Kleinstein, October 2008.

- Security Requirements for Cryptographic Modules, Revised Draft, Federal Information Processing Standard (FIPS), FIPS 140-3, December 2009
- Secure/Multipurpose Internet Mail Extensions (S/MIME), Version 3.2, Message Specification, Proposed Standard, IETF RFC 5751, ISSN: 2070-1721, Ramsdell (Brute Squad Labs) and Turner (IECA), January 2010
- Guide for Applying the Risk Management Framework to Federal Information Systems: A security Lifecycle Approach, NIST Special Publication, SP 800-37 Rev. 1, Joint Task Force Transformation Initiative; February 2010 with updates as of June 5, 2014
- Guidelines for the Secure Deployment of IPv6; NIST Special Publication, SP 800-119; Frankel, Graveman, Pearce, Rooks; December 2010
- Use Cases and Requirements for DNS-Based Authentication of Named Entities (DANE), IETF RFC 6394, ISSN: 2070-1721, Barnes (BBN Technologies), October 2011
- The DNS-Based Authentication of Named Entities (DANE) Transport Layer Security Protocol: TLSA, Proposed Standard, IETF RFC 6698, ISSN: 2070-1721, Hoffman (VPN Consortium) and Schlyter (Kirei AB), August 2012
- Updates to the Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile, Proposed Standard, IETF RFC 6818, ISSN: 2070-1721, Yee (AKAYLA), January 2013
- Security and Privacy Controls For Federal Information Systems And Organizations, NIST Special Publication, SP 800-53 Rev. 4, Joint Task Force Transformation Initiative, April 2013
- A Framework for Designing Cryptographic Key Management Systems; NIST Special Publication; SP 800-130; Barker, Branstad, Smid, Chokhani; August 2013
- Using Secure DNS to Associate Certificates with Domain Names For S/MIME, IETF Internet Draft, draft-ietf-dane-smime-02, September 30, 2013.
- Secure Domain Name System (DNS) Deployment Guide, NIST Special Publication, SP 800-81-2, Chandramouli and Rose, September 2013
- Framework for Improving Critical Infrastructure Cybersecurity, National Institute of Standards and Technology, February 12, 2014
- Adding Acronyms to Simplify Conversations about DNS-Based Authentication of Named Entities (DANE), IETF RFC 7218, ISSN: 2070-1721, Gudmundsson (Shinkuro Inc.), April 2014
- Guidelines for the Selection, Configuration, and Use of Transport Layer Security (TLS) Implementations; NIST Special Publication; SP 800-52 Rev. 1; Polk, McKay, Chokhani; April 2014
- Systems Security Engineering: An Integrated Approach to Building Trustworthy Resilient Systems, Draft, NIST Special Publication, SP 800-160, May, 12, 2014

- A Profile for U.S. Federal Cryptographic Key Management Systems (CKMS); Third Draft; NIST Special Publication; SP 800-152; Barker, Smid, Branstad; December 18, 2014
- Recommendation for Key Management: Part 3 – Application-Specific Key Management Guidance, NIST Special Publication, SP 800-57 Part 3 Rev. 1, Barker and Dang, January 2015
- Using Secure DNS to Associate Certificates with Domain Names for S/MIME, draft-ietf-dane-smime-08, Hoffman (VPN Consortium) and Schlyter (Kirei AB), February 20, 2015
- SMTP security via opportunistic DANE TLS, draft-ietf-dane-smtp-with-dane-18, Dukhovni (Two Sigma) and Hardaker (Parsons), May 26, 2015

6. Desired Solution Characteristics

The building block will consist of a proof-of-concept security platform, composed of off-the-shelf components, that provides trustworthy mail server-to-mail server email exchanges across organizational boundaries. The DANE protocol will be used to authenticate servers and certificates in two roles in the Security for Email Project by binding the X.509 certificates used for

1. Transport Layer Security (TLS) to DNS names verified by DNSSEC and supporting the use of these certificates in the mail server to mail server communication
2. Secure Secure/Multipurpose Internet Mail Extensions (S/MIME) to DNS names verified by DNSSEC and supporting the use of these S/MIME certificates in the end-to-end email communication

It will encrypt email traffic between servers, allow individual email users to digitally sign and/or encrypt email messages to other end users, and allow individual email users to obtain other users' certificates in order to validate signed email or send encrypted email. The project will include an email sending policy consistent with a stated privacy policy that can be parsed by receiving servers so that receiving servers can apply the correct security checks and report back the correctness of the email stream. Documentation of the resulting platform will include statements of security and privacy policies and standards (e.g., IETF RFCs) supported, technical specifications for hardware and software, implementation requirements, and a mapping of implementation requirements to the applicable policies, standards, and best practices. The secure email building block will involve composition of a variety of components that will be provided by a number of different vendors. Client systems, DNS/DNSSEC services, mail transfer agents, and certificate providers (CAs) are generally involved. DNS resolvers (stub and recursive) for DNSSEC validation , authoritative DNS servers for DNSSEC signed zones, mail server/mail security systems, S/MIME certificates, and extended validation and domain validation TLS certificates are expected to be included in the solution.

7. Security Control Map

This table maps the characteristics of the commercial products that the NCCoE will apply to this cybersecurity challenge to the applicable standards and best practices described in the *Framework for Improving Critical Infrastructure Cybersecurity (CSF)*, and other NIST activities. This exercise is meant to demonstrate the real-world applicability of standards and best practices, but does not imply that products with these characteristics will meet your industry's requirements for regulatory approval or accreditation. Correct implementation of the security platform resulting from this project will support achievement of improved maturity in the *Identify, Protect, and Detect* functions identified in the Cybersecurity Framework.

Table 1: Security Control Map

Function	Category	Subcategory	Informative Reference
IDENTIFY (ID)	**Asset Management (ID.AM):** The data, personnel, devices, systems, and facilities that enable the organization to achieve business purposes are identified and managed consistent with their relative importance to business objectives and the organization's risk strategy.	**ID.AM-3:** Organizational communication and data flows are mapped[1]	**CCS CSC** 1 **COBIT 5** DSS05.02 **ISA 6443-2-1:2009** 4.2.3.4 **ISO/IEC 27001:2013** A.13.2.1 **NIST SP 800-53 Rev. 4** AC-4, CA-3, CA-9, PL-8
		ID.AM-4: External information systems are catalogued.[2]	**COBIT 5** APO02.02 **ISO/IEC 27001:2013** A.11.2.6 **NIST SP 800-53 Rev. 4** AC-20, SA-9
	Risk Assessment (ID.RA): The organization understands the cybersecurity risk to organizational operations, organizational assets, and individuals.	**ID.RA-6:** Risk responses are identified and prioritized	**COBIT 5** APO 12.05, APO 13.02 **NIST SP 800-53 Rev. 4** PM-4, PM-9
PROTECT (PR)	**Data Security (PR.DS):** Information and records (data) are managed consistent with the organization's risk strategy to protect	**PR.AC-5:** Network Integrity is protected, incorporating network segregation where appropriate	**COBIT 5** APO 13.01, DSS01.04, DSS05.03 **ISA 6443-2-1:2009** 4.3.3.6.6 **ISA 6443-3-3:2013** SR 1.13, SR .2.6

Function	Category	Subcategory	Informative Reference
	the confidentiality, integrity, and availability of information.		**ISO/IEC 27001:2013** A.6.2.2, A.13.1.1, A.13.2.1 **NIST SP 800-53 Rev. 4** AC-17, AC-19, AC-20
		PR.DS-2: Data in transit is protected	**ISA 6443-2-1:2009** 4.3.3.4 **ISA 62443-3-3:2013** SR 3.1, SR 3.8 **ISO/IEC 27001:2013** A.13.1.1, A.13.1.3, A.13.2.1 **NIST SP 800-53 Rev. 4** AC-4, SC-7
		PR.DS-5: Protections against leaks are implemented	**CCS CSC** 17 **COBIT 5** APO01.06 **ISA 6443-3-3:2013** SR 5.2 **ISO/IEC 27001:2013** A.6.1.2, A.7.1.1, A.7.1.2, A7.3.1, A.8.2.2, A.8.2.3, A.9.1.1, A.9.1.2, A.9.2.3, A.9.4.1, A.9.4.4, A.9.4.5, A.13.1.3, A.13.2.1, A.13.2.3, A.13.2.4, A.14.1.2, A.14.1.3 **NIST SP 800-53 Rev. 4** AC-4, AC-5, AC-6, PE-19, PS-3, PS-6, SC-7, SC-8, SC-13, SC-31, SI-4
		PR.DS-6: Integrity checking mechanisms are used to verify software, firmware, and information integrity	**ISA 6443-3-3:2013** SR 3.1, SR 3.3, SR 3.4, SR 3.8 **ISO/IEC 27001:2013** A.12.2.1, A.12.5.1, A.14.1.2, A.14.1.3 **NIST SP 800-53 Rev. 4** SI-7

Function	Category	Subcategory	Informative Reference
	Protective Technology (PR.PT): Technical security solutions are managed to ensure the security and resilience of systems ands assets, consistent with related policies, procedures, and agreements.	**PR.PT-4:** Communications and control networks are protected	**CCS CSC** 7 **COBIT 5** DSS05.02, APO 13.01 **ISA 62443-3-3:2013** SR 3.1, SR 3.5, SR 3.8, SR 4.1, SR 4.3, SR 5.1, SR 5.2, SR 5.3, SR 7.1, SR 7.6 **ISO/IEC 27001:2013** A.13.1.1, A.13.2.1 **NIST SP 800-53 Rev. 4** AC-4, AC-17, AC-18, CP-8, SC-7
DETECT (DE)	**Security Continuous Monitoring (DE.CM):** The information system and assets re monitored at discrete intervals to identify cybersecurity events and verify the effectiveness of protective measures.	**DE.CM-8:** Monitoring for unauthorized personnel, connections, devices, and software is performed	**COBIT 5** BAI03.10 **ISA 62443-2-1:2009** SR 4.2.3.1, SR 4.2.3.7 **ISO/IEC 27001:2013** A.12.6.1 **NIST SP 800-53 Rev. 4** RA-5

[1] It is necessary to understand to what devices one is connected to be sure of organizational data flows.

[2] It is necessary to understand to what devices one is actually connecting to understand what external systems is part of the actual enterprise.

8. High-Level Architecture

The figure below is a high-level depiction of email functionality where DNS-based security for email is used. In this example architecture, encryption is actually performed by the email servers in both scenarios to be demonstrated. Encryption is performed on bulk exchanges between email services. This addresses the main security concerns in enterprise environments, which are the target of the project, but not necessarily those of individual users who may also want to reduce information disclosure to their email providers. The only per-message cryptography is digital signatures. In the second scenario, digital signature protection is provided by the clients.

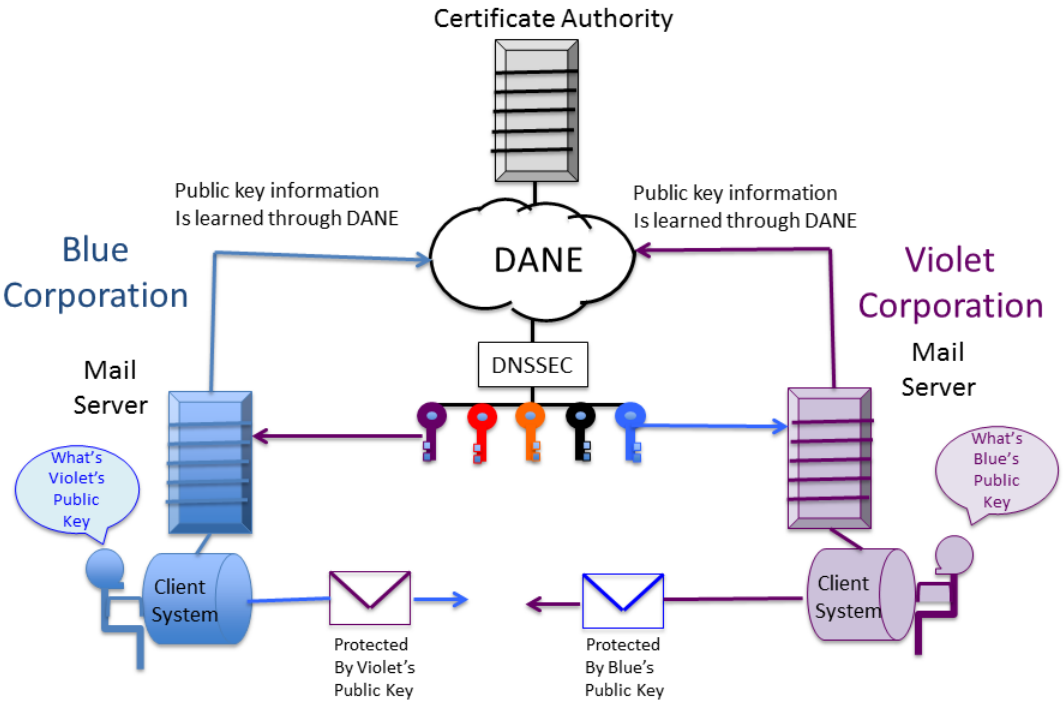

Figure 1. High-Level Architecture

9. Component List

- Client systems
- DNS/DNSSEC services
- Mail transfer agents
- DNS resolvers (stub and recursive) for DNSSEC validation
- Authoritative DNS servers for DNSSEC signed zones
- Mail server/mail security systems
- S/MIME certificates
- Extended validation and domain validation TLS certificates

Appendix A - Risk Assessment

Both public and private sector business operations are heavily reliant on email exchanges. The need to protect business plans and tactics; the integrity of transactions, financial and other proprietary information; and privacy of employees and clients are factors that motivate organizations to secure their email.

Email, unless protected by cryptographic integrity and confidentiality mechanisms is inherently susceptible to being read or modified by unauthorized individuals and processes. Unprotected email is also commonly used as an attack vector for insertion of malware into organizations' and users' systems. Whether the service desired is authentication of the source of an email message, assurance that the message has not been altered by an unauthorized party, or message confidentiality, cryptographic functions are usually employed.

Economies of scale and a need for uniform implementation drive most enterprises to rely on mail servers to provide security to the members of an enterprise rather than end-to-end security operated by individual users. Most server-based email security mechanisms are vulnerable to attacks involving

1. faked or fraudulent key certificates
2. otherwise invalid certificates
3. failure to actually invoke a security process as a result of connection to or through a fraudulent server

The consequences most often involve unauthorized reading or modification of information or fraudulently causing legitimate parties to bypass the protection mechanisms altogether. Use of email as an attack vector for phishing and insertion of malware is a persistent problem because users continue to click on links to malware-ridden websites in fraudulent emails, a major factor in most confirmed data breaches.

Sources of threats to public and private sector organizations and individuals include malicious individuals, unscrupulous competitors, professional criminals and criminal enterprises, law enforcement and regulatory investigators, and nation states seeking political, commercial, or military advantage.

Some examples of consequences of exploitation of unprotected email and email whose protection mechanism have been bypassed or defeated include the following:

- Privacy breaches due to exposure of PII to unauthorized individuals
- Regulatory or reputational consequences of privacy breaches
- Expenses resulting from notification and corrective action required as a result of privacy breaches
- Damage to individual or organizational reputations due to exposure of the individual's or organization's information to and by unauthorized entities
- Illicit authorization of business transactions, including financial transactions
- Intercept and blocking of business-critical transactions
- Legal and regulatory consequences due to intercept and blocking, modification, and/or pre-mature exposure of individuals' and organizations' information

- Loss of IT and/or dependent operational service availability resulting from insertion of destructive malware
- Interruption of business-critical operations due to loss of IT and/or dependent operational service availability resulting from insertion of destructive malware

APPENDIX B - ACRONYMS AND ABBREVIATIONS

ANSI	American National Standards Institute
API	Application Program Interface
CA	Certificate Authority
CCS CSC	Council on CyberSecurity Top 20 Critical Security Controls
COBIT	Control Objectives for Information and Related Technology
DANE	DNS-Based Authentication of Named Entities
DNS	Domain Name System
DNSSEC	Domain Name System Security Extensions
EMAIL	Electronic Mail
FIPS	Federal Information Processing Standard
HTTPS	Secure Hypertext Transfer Protocol
IEC	International Electrotechnical Commission
IETF	Internet Engineering Task Force
IOT	Internet of Things
IP	Internet Protocol
IPSEC	Internet Security Protocol
ISA	Instrumentation, Systems, and Automation Society
ISO	International Organization for Standardization
NCCoE	National Cybersecurity Center of Excellence
NIST	National Institute of Standards and Technology
RFC	Request for Comments
S/MIME	Secure/Multipurpose Internet Mail Extensions
SMTP	Simple Mail Transfer Protocol
SP	Special Publication
TLS	Transport Layer Security

502

APPENDIX C – GLOSSARY

Application Program Interface	A software intermediary that makes it possible for application programs to interact with each other and share data
Cryptographic Key	In cryptography, a key is a piece of information that determines the functional output of a cryptographic algorithm or cipher. Without a key, the algorithm would produce no useful result.
Cryptography	The enciphering and deciphering of messages in secret code or cipher; also, the computerized encoding and decoding of information
Digital Signature	The result of a cryptographic transformation of data that, when properly implemented with a supporting infrastructure and policy, provides the services of: 1. Origin authentication, 2. Data integrity, and 3. Signer non-repudiation.
Domain Name System	A system for naming computers and network services that is organized into a hierarchy of domains. DNS naming is used in networks such as the Internet to locate computers and services through user-friendly names.
Encryption	The process of changing plaintext into ciphertext using a cryptographic algorithm and key.
Entity	An individual (person), organization, device or process.
Malware	A computer program that is covertly inserted into another program with the intent to destroy data, run destructive or intrusive programs, or otherwise compromise the confidentiality, integrity, or availability of the victim's data, applications, or operating system.
Man-in-the-middle attack	n cryptography and computer security, a man-in-the-middle attack is an attack where the attacker secretly relays and possibly alters the communication between two parties who believe they are directly communicating with each other.
Public Key	a cryptographic key that can be obtained and used by anyone to encrypt messages intended for a particular recipient, such that the encrypted messages can be deciphered only by using a second key that is known only to the recipient (the private key).

Protocol	A set of rules governing the format of data sent over the Internet or other network.

APPENDIX D – REFERENCES

[1] American National Standards Institute, ANSI/ISA-62443-2-1 (99.02.01)-2009, Security for Industrial Automation and Control Systems: Establishing an Industrial Automation and Control Systems Security Program: http://www.isa.org/Template.cfm?Section=Standards8&Template=/Ecommerce/ProductDisplay.cfm&ProductID=10243

[2] American National Standards Institute, ANSI /ISA-62443-3-3 (99.03.03)-2013, Security for Industrial Automation and Control Systems: System Security Requirements and Security Levels: http://www.isa.org/Template.cfm?Section=Standards2&template=/Ecommerce/ProductDisplay.cfm&ProductID=13420

[3] Control Objectives for Information and Related Technology (COBIT): http://www.isaca.org/COBIT/Pages/default.aspx

[4] Council on CyberSecurity (CCS) Top 20 Critical Security Controls (CSC): http://www.counciloncybersecurity.org

[5] *Cybersecurity Framework*, National Institute of Standards and Technology [Web site], http://www.nist.gov/cyberframework/ or www.nist.gov/cyberframework/upload/cybersecurity-framework-021214.pdf).

[6] Executive Order no. 13636, *Improving Critical Infrastructure Cybersecurity*, DCPD-201300091, February 12, 2013. http://www.gpo.gov/fdsys/pkg/FR-2013-02-19/pdf/2013-03915.pdf

[7] International Organization for Standardization/International Electrotechnical Commission, *Information technology – Security techniques – Information security risk management*, ISO/IEC 27005:2011, 2011. http://www.iso.org/iso/catalogue_detail?csnumber=56742

[8] International Organization for Standardization/International Electrotechnical Commission, *Information technology -- Security techniques -- Information security management systems – Requirements*, ISO/IEC 27001,

http://www.iso.org/iso/home/store/catalogue_ics/catalogue_detail_ics.htm?csnumber=54534

[9] Joint Task Force Transformation Initiative; *Guide for Applying the Risk Management Framework to Federal Information Systems: A security Lifecycle Approach*, NIST Special Publication, SP 800-37 Rev. 1, February 2010 with updates as of June 5, 2014. nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-37r1.pdf

[10] Joint Task Force Transformation Initiative, *Security and Privacy Controls For Federal Information Systems And Organizations*, NIST Special Publication, SP 800-53 Rev. 4, April 2013. nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf

[11] National Institute of Standards and Technology, *Security Requirements for Cryptographic Module*s, Federal Information Processing Standard (FIPS), FIPS 140-2, May 2001. csrc.nist.gov/publications/fips/fips140-2/fips1402.pdf

[12] National Institute of Standards and Technology, *Security Requirements for Cryptographic Modules*, Revised Draft, Federal Information Processing Standard (FIPS), FIPS 140-3, December 2009. csrc.nist.gov/groups/ST/FIPS_140-3

[13] Office of Management and Budget (OMB), *E-Authentication Guidance for Federal Agencies,* OMB Memorandum 04-04, December 16, 2003. http://www.whitehouse.gov/sites/default/files/omb/assets/omb/memoranda/fy04/m04-04.pdf.

[14] Office of Management and Budget (OMB), *Securing the Federal Government's Domain Name System Infrastructure*, OMB Memorandum for Chief Information Officers, M-08-23, August 22, 2008 georgewbush-whitehouse.archives.gov/omb/memoranda/fy2008/m08-23.pdf

[15] Public Law, E-Government Act of 2002, Pub. L. 107-347, 116 Stat 2899. http://www.gpo.gov/fdsys/pkg/PLAW-107publ347/pdf/PLAW-107publ347.pdf.

[16] Public Law, Federal Information Security Management Act of 2002, Pub. L. 107-347 (Title III), 116 Stat 2946. http://www.gpo.gov/fdsys/pkg/PLAW-107publ347/pdf/PLAW-107publ347.pdf.

[17] Atkins and Austein, *Threat Analysis of the Domain Name System (DNS)*, IETF RFC 3833, August 2004. tools.ietf.org/html/rfc3833

[18] Barker, Branstad, Smid, Chokhani; *A Framework for Designing Cryptographic Key Management Systems*; NIST Special Publication; SP 800-130; August 2013. nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-130.pdf

[19] Barker, Barker, Burr, Polk, Smid; *Recommendation for Key Management: Part 1: General*, NIST Special Publication, SP 800-57 Part 1 Rev. 3, July 2012. csrc.nist.gov/publications/nistpubs/800-57/sp800-57_part1_rev3.pdf

[20] Barker and Dang, *Recommendation for Key Management: Part 3 – Application-Specific Key Management Guidance*, NIST Special Publication, SP 800-57 Part 3 Rev. 1, January 2015. nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.57Pt3r1.pdf

[21] Barker, Smid, Branstad; *A Profile for U.S. Federal Cryptographic Key Management Systems (CKMS)*; Third Draft; NIST Special Publication; SP 800-152; Barker, Smid, Branstad; December 18, 2014. csrc.nist.gov/publications/drafts/800-152/sp800-152_third_draft.pdf

[22] Barnes, *Use Cases and Requirements for DNS-Based Authentication of Named Entities (DANE)*, IETF RFC 6394, ISSN: 2070-1721, October 2011. tools.ietf.org/html/rfc6394

[23] Chandramouli and Rose, *Secure Domain Name System (DNS) Deployment Guide*, NIST Special Publication, SP 800-81-2, September 2013. nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-81-2.pdf

[24] Chernick, Federal S/MIME V3 Client Profile, NIST Special Publication, SP 800-49, November 2002. csrc.nist.gov/publications/nistpubs/800-49/sp800-49.pdf

[25] Cooper, Santesson, Farrell, Boeyen, Housley, and Polk, *Internet X.509 Public Key Infrastructure Certification and Certificate Revocation List (CRL) Profile*, Internet Engineering Task Force (IETF) Network Working Group Request for Comments (RFC) 5280, May 2008. http://www.ietf.org/rfc/rfc5280.txt

[26] Dukhovni and Hardaker, *SMTP security via opportunistic DANE TLS*, draft-ietf-dane-smtp-with-dane-18i, May 26, 2015. datatracker.ietf.org/doc/draft-ietf-dane-smtp-with-dane

[27] Frankel, Graveman, Pearce, Rooks; *Guidelines for the Secure Deployment of IPv6*; NIST Special Publication, SP 800-119; December 2010. , May, 12, 2014. csrc.nist.gov/publications/nistpubs/800-119/sp800-119.pdf

[28] Gudmundsson, *Adding Acronyms to Simplify Conversations about DNS-Based Authentication of Named Entities (DANE)*, IETF RFC 7218, ISSN: 2070-1721, April 2014. tools.ietf.org/html/rfc7218

[29] Hoffman and Schlyter, *The DNS-Based Authentication of Named Entities (DANE) Transport Layer Security Protocol: TLSA*, Proposed Standard, IETF RFC 6698, ISSN: 2070-1721, August 2012. tools.ietf.org/html/rfc7698

[30] Hoffman and Schlyter, *Using Secure DNS to Associate Certificates with Domain Names for S/MIME*, draft-ietf-dane-smime-08, February 20, 2015. datatracker.ietf.org/doc/ietf-dane-smime

[31] Hoffman, Schlyter, Kirei, Rose; *Using Secure DNS to Associate Certificates with Domain Names For S/MIME*, IETF Internet Draft, draft-ietf-dane-smime-02, September 30, 2013. https://tools.ietf.org/html/draft-ietf-dane-smime-02

[32] Housley, Ford, Polk, Solo; *Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile*; IETF RFC 2459; January 1999. tools.ietf.org/html/rfc2459

[33] Kleinstein, *Simple Mail Transfer Protocol*, IETF RFC 5321, Draft Standard, October 2008. tools.ietf.org/html/rfc5321

[34] Polk, McKay, Chokhani; *Guidelines for the Selection, Configuration, and Use of Transport Layer Security (TLS) Implementations*; NIST Special Publication; SP 800-52 Rev. 1; April 2014. nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-52r1.pdf

[35] Ramsdell and Turner, *Secure/Multipurpose Internet Mail Extensions (S/MIME), Version 3.2, Message Specification*, Proposed Standard, IETF RFC 5751, ISSN: 2070-1721, January 2010. tools.ietf.org/html/rfc5751

[36] Resnick, *Internet Message Format*, IETF RFC 5322, Draft Standard, October 2008 https://tools.ietf.org/html/rfc5322

[36] Ross, Oren, McEvilley; *Systems Security Engineering: An Integrated Approach to Building Trustworthy Resilient Systems*, Draft, NIST Special Publication, SP 800-160, May, 12, 2014. csrc.nist.gov/publications/drafts/800-160/sp800-160_draft.pdf

[37] Tracy, Jansen, Scarfone, Butterfield; *Guidelines on Electronic Mail Security*; NIST Special Publication; SP 800-45 Ver. 2; February 2007. csrc.nist.gov/publications/nistpubs/800-45-version2/SP800-45v2.pdf

[38] Yee, *Updates to the Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile*, Proposed Standard, IETF RFC 6818, ISSN: 2070-1721, January 2013. tools.ietf.org/html/rfc6818

[39] Infosec Instutute, General Security, "How Cybercrime Exploits Digital Certificates," July 28, 2014, http://resources.infosecinstitute.com/cybercrime-exploits-digital-certificates

504

505