

1 Domain Name Systems-Based 2 Electronic Mail Security

3 Executive Summary

- 4 ■ Both public and private sector business operations are heavily reliant on electronic mail (email)
5 exchanges but the integrity of these transactions is often at risk, including financial and other
6 proprietary information as well as the privacy of employees and clients.
- 7 ■ Protocols such as Transport Layer Security (TLS), Secure/Multipurpose Internet Mail Extensions (S/
8 MIME), Domain Name System Security Extensions (DNSSEC), and Domain Name System (DNS)
9 Authentication of Named Entities (DANE) exist and are capable of providing needed email security
10 and privacy protection.
- 11 ■ Impediments such as the absence of comprehensive configuration instructions for a composed set of
12 mail client, mail transfer agents, and DNS security components, absence of resource guides to easily
13 implemented software libraries and software applications for system administrators, and functional
14 characteristics of security applications that negatively impact the performance of email systems have
15 limited adoption of these existing security and privacy protocols.
- 16 ■ Operating email systems without employing available security and privacy protocols increases the
17 opportunities for attackers to breach sensitive enterprise information by introducing false addresses
18 into mail messages, disrupting secure communication signaling, and improving the probability of
19 successfully inducing enterprise users to open malicious attachments - still the most common method
20 for introducing malware and breaching enterprise systems.
- 21 ■ The National Cybersecurity Center of Excellence (NCCoE) developed a set of example DNS-based
22 email security solutions that organizations can use to facilitate implementation of security and privacy
23 protocols, thus reducing the likelihood of a data breach. The solution sets include tools that support
24 installation and set-up of trustworthy email systems.
- 25 ■ The security characteristics in this guide are informed by guidance and best practices from standards
26 organizations. How the solution set addresses security requirements and best practices is addressed
27 in a volume that includes the security approach, architecture, and security characteristics.
- 28 ■ The NCCoE's approach uses both open source and commercially available products that can be
29 included alongside current mail products in existing infrastructure.
- 30 ■ The example solution is described in a "How To" guide that shows how to implement a set of
31 standards-based, commercially available cybersecurity technologies in the real world. The guide will
32 help organizations utilize technologies to reduce the risk of untrustworthy email, while saving them
33 research and proof of concept costs.

34 THE CHALLENGE

35 Whether the security service desired is authentication of the source of an email message or assurance
36 that the message has not been altered by or disclosed to an unauthorized party, organizations must
37 employ some cryptographic protection mechanism. Economies of scale and a need for uniform security
38 implementation drive most enterprises to rely on mail servers and/or Internet service providers (ISPs) to
39 provide security to all members of an enterprise. Many current server-based email security mechanisms
40 are vulnerable to, and have been defeated by, attacks on the integrity of the cryptographic
41 implementations on which they depend. The consequences of these vulnerabilities frequently involve
42 unauthorized parties being able to read or modify supposedly secure information, or to use email as a
43 vector for inserting malware into the system in order to gain access to enterprise systems or information.
44 Protocols exist that are capable of providing needed email security and privacy, but impediments such as
45 unavailability of easily implemented software libraries and software applications characteristics that
46 complicate operation of email systems have limited adoption of existing security and privacy protocols.

47 THE SOLUTION

48 The Domain Name System-Based Security for Electronic Mail (Email) project has produced a proof of
49 concept security platform that demonstrates trustworthy email exchanges across organizational
50 boundaries. The goals of the project include authentication of mail servers, signing and encryption of
51 email, and binding cryptographic key certificates to the servers. The Domain Name System Security
52 Extension (DNSSEC) protocol is used to authenticate server addresses and certificates used for Transport
53 Layer Security (TLS) to DNS names. The business value of the security platform demonstrated by this
54 project includes improved privacy and security protection for users' operations and improved support for
55 implementation and use of the protection technologies. The platform also expands the set of available
56 DNS security applications and encourages wider implementation of DNSSEC, TLS and S/MIME to protect
57 internet communications.

58 Project deliverables include:

- 59 ■ demonstration prototypes of DNS-based secure email platforms
- 60 ■ this publicly available NIST Cybersecurity Practice Guide that explains how to employ the platform(s)
61 to meet industry security and privacy best practices as well as requirements for federal government
62 agencies
- 63 ■ platform documentation necessary to efficiently compose a DNS-based email security platform from
64 off-the-shelf components
- 65 ■ recommendations for effective implementation in a manner that is consistent with applicable
66 standards documentation

67 Approach

68 The secure email project involves composition of a variety of components that have been provided by a
69 number of different technology providers, including Microsoft Corporation, the Internet Systems
70 Consortium, Secure64, Fraunhofer IAO, and Stichting NLnet Laboratories. Each of these collaborators has
71 entered into a Cooperative Research and Development Agreement (CRADA) with NIST to participate in
72 this consortium effort. These components include client systems, DNS/DNSSEC services, mail transfer
73 agents (MTA), and certificate sources.

74 We demonstrate how security can be supported through standards-based configuration and operation
75 DNS servers, electronic mail applications and MTAs in a manner that supports trustworthy email by the
76 organization.

77 The guide:

- 78 ■ identifies the security characteristics needed to sufficiently reduce the risks to information exchanged
79 by email
- 80 ■ maps security characteristics to standards and best practices from NIST and other organizations
- 81 ■ describes a detailed example solution, along with instructions for implementers and security
82 engineers on efficiently installing, configuring, and integrating the solution into existing IT
83 infrastructures
- 84 ■ provides an example solution that is operationally practical and evaluates the performance of the
85 solution in real-world scenarios

86 **BENEFITS**

87 Our example solution has several benefits, including the following:

- 88 ■ reduces risk so that employees are able to exchange personal and enterprise information via email
89 with significantly reduced risk of disclosure or compromise
- 90 ■ enables the use of existing security protocols more efficiently and with minimal impact to email
91 service performance
- 92 ■ integrates capabilities into various server and client IT infrastructure environments
- 93 ■ enhances visibility for system administrators into email security events, providing for recognition of
94 authentication failures that could result in device and data compromises
- 95 ■ implements both commercial and open source industry standard network and email security controls
96 reducing long term costs and decreasing the risk of vendor lock-in
- 97 ■ can be extended to other enterprise information exchange technologies that are growing in use (e.g.,
98 text messages, chat)

99 **TECHNOLOGY PARTNERS AND COLLABORATORS**

100 The technology vendors who participated in this project submitted their capabilities in response to a call
101 in the Federal Register. Companies with relevant products were invited to sign a Cooperative Research and
102 Development Agreement with NIST, allowing them to participate in a consortium to build this example
103 solution. We worked with:

- 104 ■ [Microsoft Corporation](#)
- 105 ■ [NLnet Laboratories](#)
- 106 ■ [Secure64](#)
- 107 ■ [Internet Systems Consortium](#)
- 108 ■ [Fraunhofer IAO](#)

109 **SHARE YOUR FEEDBACK**

110 You can get the guide through the NCCoE web site, <http://nccoe.nist.gov>. Help us make it better by
111 sharing your thoughts with us as you review the guide. If you adopt this solution for your own
112 organization, share your experience and advice with us. We recognize that technical solutions alone will
113 not fully enable the benefits of our solution, so we encourage organizations to share lessons learned and
114 best practices for transforming the business processes associated with implementing it.

115 ■ email dns-email-nccoe@nist.gov

116 ■ join our Community of Interest to offer your insights and expertise; email us at [dns-email-](mailto:dns-email-nccoe@nist.gov)
117 nccoe@nist.gov

118 To learn more by arranging a demonstration of this reference solution, contacting us at [dns-email-](mailto:dns-email-nccoe@nist.gov)
119 nccoe@nist.gov.

The National Cybersecurity Center of Excellence at the National Institute of Standards and Technology addresses businesses' most pressing cybersecurity problems with practical, standards-based example solutions using commercially available technologies. As the U.S. national lab for cybersecurity, the NCCoE seeks problems that are applicable to whole sectors, or across sectors. The center's work results in publicly available NIST Cybersecurity Practice Guides that provide modular, open, end-to-end reference designs.

LEARN MORE

<http://nccoe.nist.gov>

ARRANGE A DEMONSTRATION

nccoe@nist.gov

301-975-0200