5.1.2.1 S/MIME Certificate Management S/MIME certificates are used for digitally signed and (optionally) encrypted email messages. For information about getting or creating S/MIME certificates, see: http://kb.mozillazine.org/Getting\_an\_SMIME\_certificate. Installing an S/MIME certificate Note: Before a user can create or import his or her own certificate and private key, he or she must first set a master password if this has not already been done. The master password is needed so that imported certificates are stored securely. See http://kb.mozillazine.org/Master\_password for instructions for setting a master password. The user may have his or her own personal certificate and private key in a .p12 or .pfx file, and may wish to import it into Thunderbird. Once a Master Password has been set, the user can import/install a personal S/MIME certificate from a .p12 or .pfx file by doing the following steps. 1. Open the Certificate Manager by going to Tools -> Options... -> Advanced -> Certificates -> Manage Certificates.... NIST SP 1800-6B: Domain Name System-Based Electronic Mail Security 48 This publication is available free of charge from: https://doi.org/10.6028/NIST.SP.1800-6. 2. Go to the tab named Your Certificates. 3. Click on Import. 4. Select the PKCS12 certificate file (.pfx or .p12). 5. It will ask the user for the master password for the software security device. The user enters his or her master password and clicks OK. 6. Next, it will ask the user for the password protecting his or her personal certificate. If the user’s .p12 or .pfx file has a password, he or she enters it here, otherwise leave this field empty. Then click OK. The S/MIME certificate should now have been imported. If the certificate was not trusted, consult the instructions at http://kb.mozillazine.org/Thunderbird\_:\_FAQs\_:\_Import\_CA\_Certificate. Configuring Thunderbird for using the certificate to sign email Go to Tools -> Account Settings... in Thunderbird. Then find the account with the email address that matches the email address in the certificate that has just been installed. Choose Security under that account and select the certificate that has just been installed. The rest of the options should be selfexplanatory. When the user selects a certificate in Account Settings, that selection only applies to the account’s default identity or identities. There is no user interface for specifying certificates for an account’s other identities. If desired, this can be worked around by editing the settings manually, copying the settings from an account’s default identity to some other identity. The settings have names ending in: signing\_cert\_name, sign\_mail, encryption\_cert\_name, and encryptionpolicy. User installation of a self-signed S/MIME certificate If the S/MIME certificate in a user’s .p12 or .pfx file is a self-signed certificate for the user’s own identity, then before that file can be installed into the tab named Your Certificates, the user must first install that certificate as a certificate authority in the Authorities tab. The PKCS12 certificate file will not install into the Authorities tab. The user will need a copy of a self-signed certificate that does not contain the user’s private key. This is usually in the form of a .cer file. One way to obtain the .cer form of a certificate from the .p12 file is to use the Firefox Add-on Key Manager to extract the .cer certificate from the .p12 file. With that Add-on installed in Thunderbird, the user goes to Tools -> Key Manager Toolbox -> Key Manager -> Your Keys, select his or her key, selects Export and chooses X.509 as file format. 1. Go to Tools -> Options... -> Advanced -> Certificates -> Manage Certificates.... 2. Go to the Authorities tab. 3. Click on Import. NIST SP 1800-6B: Domain Name System-Based Electronic Mail Security 49 This publication is available free of charge from: https://doi.org/10.6028/NIST.SP.1800-6. 4. Select the .cer file. 5. It will ask the user for what purposes he or she wants to trust the certificate. Select Trust this CA to identify email users. 6. Click OK to complete the import. Note: Thunderbird automatically adds other people’s S/MIME certificates to the Other People’s tab of a user’s Certificate Manager when he or she receives from them a digitally signed message with a valid signature and with an S/MIME certificate issued by a recognized and trusted CA. CA certificates that appear in Thunderbird’s Authorities tab are recognized, and may also be trusted. CA certificates that do not appear in that tab are considered unrecognized. An S/MIME certificate that was issued by an unrecognized CA will not be automatically added to the Other People’s tab of the user’s Certificate Manager. If the user attempts to manually import an S/MIME certificate that was issued by an unrecognized CA, nothing will happen--literally. Thunderbird will not even display an error dialog. It will just not import the S/MIME certificate. This is generally not a problem when receiving an S/MIME certificate that was issued by a trusted CA, but could be a problem for a certificate that was issued by an unrecognized or untrusted CA, or for a certificate that is self-signed (i.e., it has no CA other than itself). So, before a user can import an S/MIME certificate that is issued by an unrecognized CA or is self-signed, he or she must first acquire and import the certificate for the issuing CA. In the case of a self-signed certificate, a .cer file needs to be acquired from the individual whose certificate the user wishes to add. 5.1.2.2 Sending a Digitally Signed Email 1. Compose the message as usual. 2. To digitally sign a message, select OpenPGP from the Thunderbird menu and enable the Sign Message option. 3. If the email address is associated with a cryptographic certificate, the message will be signed with the key contained in that certificate. If the email address is not associated with a cryptographic certificate, a certificate must be selected from a list. 4. Send the message as usual. NIST SP 1800-6B: Domain Name System-Based Electronic Mail Security 50 This publication is available free of charge from: https://doi.org/10.6028/NIST.SP.1800-6. 5.1.2.3 Reading a Digitally Signed Email When a signed message is received, and If Thunderbird recognizes the signature, a green bar (as shown below) appears above the message. To determine whether or not the incoming message has been signed, look at the information bar above the message body.37 If the message has been signed, the green bar also displays the text, “Signed message”. A message that has not been signed could be from someone trying to impersonate someone else. 5.2 The System Administrator’s Experience The system administrator(s) will generally be responsible for configuring the MUAs, MTA, and DNS servers. Specific installation and configuration instructions and examples are provided in Section 2, Section 3, Appendix F, Appendix G, and Appendix H of the How-To Guides, SP 1800-6C. Configuration includes setting up and publishing certificates in the DNS as TLSA and SMIMEA RRs. Certificate management using Well-Known CA-issued certificates or Enterprise CA-issued certificates is required for federal government applications and is strongly recommended in other applications. While instructions for configuration for DNSSEC are provided for environments described in SP 1800-6C, this more secure set of configuration options are not generally invoked by default. Therefore, more effort and expertise are needed on the part of the DNS administrator. Configuring and activation of mail servers (MTAs) for channel encryption by default is described in section 3.3 of SP 1800-6C. Summary information is provided here and in links for illustration purposes for Microsoft Office 365 Exchange and Postfix. In general, the bulk of the system administrator’s effort is in acquiring and publishing the necessary certificates. Maintenance of the security functions, once they’ve been set up, is a relatively routine system administration activity. 5.2.1 Microsoft Exchange Only Microsoft Exchange for Office 365 encrypts users’ data while it is on Microsoft servers and while it is being transmitted between the MTAs. Exchange for Office 365 does provide controls for end users and administrators to fine tune what kind of encryption is desired to protect files and email communications. 37 If the message is also encrypted on a user-to-user basis, Thunderbird will also ask for the entry of a secret passphrase to decrypt the message. NIST SP 1800-6B: Domain Name System-Based Electronic Mail Security 51 This publication is available free of charge from: https://doi.org/10.6028/NIST.SP.1800-6. 5.2.2 Postfix Postfix TLS support is described at http://www.postfix.org/TLS\_README.html. Postfix can be configured to always use TLS when offered by receivers.38 6 Security Characteristic Analysis 6.1 Assumptions and Limitations This security characteristic evaluation has the following limitations: ♣ It is not a comprehensive test of all security components, nor is it a red team exercise. ♣ It cannot identify all weaknesses. ♣ It does not include the lab infrastructure. It is assumed that its devices are hardened. Testing these devices would reveal only weaknesses in implementation that would not be relevant to those adopting this reference architecture. 6.2 Build Testing The evaluation included analysis of the security platforms to identify weaknesses and to discuss mitigations. The focus of this portion of the evaluation was hands-on testing of the laboratory build and examination of product manuals and documentation. Our objective was to evaluate the building block and not specific products. The presence of four primary OSs for domains tested (Linux, macOS, SourceT Micro OS, and Windows) made complete product-independent hands-on testing unrealistic. Table 6.1 describes the goals of each sequence of test cases. For each sequence, the Cybersecurity Framework (CSF) Subcategories and associated SP 800-53 control(s), the test environment(s) involved, and evaluation objective of the test are identified. The results of the tests are provided in NIST SP 1800- 6C. In all test sequences, the sending MTA attempted to establish a TLS protected channel to deliver the email message to the receiver. In the attack scenarios, a malicious actor attempts to disrupt this transfer. In all test sequences, the sending MUA signed the message, and the receiving MUA, checked the signature. Exchange was used only for Scenario 2.39 In all test sequences, the sending MTA attempted to verify the correctness of all DNS responses via DNSSEC validation. In most scenarios, alice@ sent an email to bob@. Both senders and receivers had their own (separate) DNS infrastructures consisting of both authoritative and recursive servers. The Exchange 38 “Setting Postfix to encrypt all traffic when talking to other mail servers,” Snapdragon Tech Blog, August 9, 2013. http://blog.snapdragon.cc/2013/07/07/setting-postfix-to-encrypt-all-traffic-when-talking-to-other-mailservers/ 39 Exchange MTAs did not attempt to encrypt or decrypt MTA-to-MTA message exchanges. NIST SP 1800-6B: Domain Name System-Based Electronic Mail Security 52 This publication is available free of charge from: https://doi.org/10.6028/NIST.SP.1800-6. as Sender tests were conducted for completeness and for examples of SMTP over TLS without DANE support—what it looked like and how well it worked. NIST SP 1800-6B: Domain Name System-Based Electronic Mail Security 53 This publication is available free of charge from: https://doi.org/10.6028/NIST.SP.1800-6. Table 6.1 Tests Performed Test Sequence CSF Subcategories SP 800-53 Controls Configuration Evaluation Objective Sequence 1 PR.AC-1 PR.AC-5 PR.DS-1 PR.DS-2 PR.DS-6 RS.MI-2 AC-2, AC-17, AC-19, AC-20, IA Family, IR-4, SC-8, SC-28, SI-7 An Outlook MUA, interfacing with an Exchange MTA, was configured to use Active Directory and BIND DNS services in turn. Each of the six configurations exchanged email with ν a Secure64 MUA/MTA/DNS service stack that included a Postfix MTA and a Thunderbird MUA running on a Mac OS system ν an NLnet Labs MUA/MTA/DNS service stack that included a Postfix MTA and a Thunderbird MUA running on Linux The events include those showing use of Well-Known CAs (Certificate Usage Type 1 (CU=1)), Enterprise CAs (CU=2), and SelfSigned Certificates (CU=3) for TLS and S/MIME-enabled mail receivers and S/MIME. Figure 4.2 above depicts the set-up for laboratory support for the Secure64 destination variant of this test sequence.40 Email messages between Postfix MTAs were encrypted and successfully decrypted via TLS (Scenario 1). Signature was logged. All messages were S/MIME signed. Outlook attempted to verify received messages (Scenario 2). Signature verification results were noted. DNS name verification results were noted. 40 The connections depicted in the figure are actually for the Secure64 variant of the first Sequence 2 configuration. Capabilities for Sequence 1 support are shown as dotted lines. NIST SP 1800-6B: Domain Name System-Based Electronic Mail Security 54 This publication is available free of charge from: https://doi.org/10.6028/NIST.SP.1800-6. Test Sequence CSF Subcategories SP 800-53 Controls Configuration Evaluation Objective Sequence 2 PR.AC-1 PR.AC-5 PR.DS-1 PR.DS-2 PR.DS-6 RS.MI-2 AC-2, AC-17, AC-19, AC-20, IA Family, IR-4, SC-8, SC-28, SI-7 Outlook and Thunderbird MUAs, configured to use a Postfix MTA with Dovecot IMAP support, were configured in turn to use BIND and Secure64’s DNS Authority, DNS Cache, and DNS Signer implementations. Each of the six configurations exchanged email with a Secure64 MUA/MTA/DNS service stack that included a Thunderbird MUA, Postfix/Dovecot MTA, and DNS Signer/DNS Cache/DNS Authority services for processing received messages; and an NLnet Labs MUA/MTA/DNS service stack that included a Thunderbird MUA, Postfix/Dovecot MTA, and NSD4, Unbound, and OpenDNSSEC DNS services. The test events include using WellKnown CA issued (TLSA/SMIMEA CU=1), Enterprise CA issued (CU=2), and Self-Signed Certificates (CU=3). Figure 4.2 above depicts the setup for laboratory support for this test sequence. Email messages between MTAs were encrypted and successfully decrypted (Scenario 1). Signature and encryption were logged. All messages were S/MIME signed. Outlook attempted to verify received messages (Scenario 2). Signature verification results were noted. DNS name verification results were noted. NIST SP 1800-6B: Domain Name System-Based Electronic Mail Security 55 This publication is available free of charge from: https://doi.org/10.6028/NIST.SP.1800-6. Test Sequence CSF Subcategories SP 800-53 Controls Configuration Evaluation Objective Sequence 3 PR.AC-1 PR.AC-5 PR.DS-2 RS.MI-1 AC-2, AC-4, AC-17, AC-19, AC-20, IA Family, IR-4, SC-7, SC-8 Fraudulently S/MIME-signed email was sent from a malicious sender to recipients using Outlook and Thunderbird MUAs configured to use Exchange and Postfix as MTAs. The Outlook/Exchange configuration used Active Directory as its DNS server. The configurations employing Postfix/Dovecot MTAs were demonstrated with each of the other three contributed DNS Services. In one event, the Thunderbird MUA employed an Apple Key Chain Utility tool that allows a host to obtain X.509 certificates via of DANE RRs. All events were conducted using well-known CA and Enterprise CA-issued certificates for the impersonated sender. The setup for this sequence is depicted in Figure 4.3 above. The fraudulent site attempted to spoof a valid sending domain belonging to a Secure64 site. An Outlook/Exchange/ Active Directory setup acted as the fraudulent site. The email exchange between organizations was carried over TLS, and the email message was S/MIME signed on the fraudulent users’ client device. Where Well-Known CA-issued certificates or Enterprise CA-issued certificates were used, and the MTA was DANE aware, the MUA using a SMIMEA utility was able to detect the fraudulent email and mark the email as not validated. Sequence 4 PR.AC-1 PR.AC-5 PR.DS-2 PR.DS-6 RS.MI-1 RS.MI-2 AC-2, AC-4, AC-17, AC-19, AC-20, IA Family, IR-4, SC-7, SC-8, SI-7 The sender used an Outlook MUA sending mail through a Postfix/Dovecot MTA and using (in turn): Active Directory and DNS Server, BIND DNS Server, and NLnet Labs DNS Services. Self-signed certificates were used on the legitimate receiver side (TLSA RR parameter CU=3) for TLS. Each of the three configurations attempted to initiate an email exchange with an external Secure64 site. The setup for this sequence is depicted in Figure 4.4 above. The Outlook/Exchange/Active Directory stack attempted to intercept the email from the NCCoE Laboratory Configuration by acting as a man-in-themiddle. The email and DNS transactions were logged in each case, and the results are provided in Volume C Appendix C. Where the MTA was DANEaware, spoofing was detected. The mail connection to the MTA was established but closed the connection before the mail was transferred. Otherwise, the MTA failed to detect the man-in-themiddle and sent the email. NIST SP 1800-6B: Domain Name System-Based Electronic Mail Security 56 This publication is available free of charge from: https://doi.org/10.6028/NIST.SP.1800-6. Test Sequence CSF Subcategories SP 800-53 Controls Configuration Evaluation Objective Sequence 5 PR.AC-1 PR.DS-6 DE.CM-1 DE.DP-4 RS.CO-2 AC-4, IR-5, SC-5, SC-20, SC-21, SC-23, SI-4, SI-13 A DANE-enabled Postfix MTA sent message traffic to four MTAs with one Authoritative Server serving all four zones. An NSD4 Authoritative DNS server and Unbound recursive server were provided for the Postfix sending MTA, and a Secure64 DNS Authority and Signer provided the DNS services for the recipient zones. We reviewed the log files. One of the recipient MTAs did not employ TLSA, one employed a valid TLSA with the CU set to 3, one employed a TLSA with a certificate usage field of 1, but with an incomplete (i.e., bad) PKI certification path (PKI X.509 [PKIX] failure), and one employed mismatched server cert/TLSA with the certificate usage field set to 3 (DANE validation failure). A large number of email messages are generated in the Postfix server device using a Python script, and the Postfix MTA sends the messages to each of four recipient MTAs in different zones. In the recipient MTA running without TLSA and that running with a valid matching TLSA and certificate usage field set to 3, all messages should be accepted. In the recipient MTA with a TLSA RR using certificate usage of 1, but with an incomplete PKIX validation path, and the recipient MTA with a mismatched certificate/TLSA (cert usage 3), the sender should close the connection without sending the message. Logwatch running on the sending Postfix server device logged the instances of failure to deliver due to certificate expiration or bad certificate path. NIST SP 1800-6B: Domain Name System-Based Electronic Mail Security 57 This publication is available free of charge from: https://doi.org/10.6028/NIST.SP.1800-6. 6.3 Scenarios and Findings One aspect of our security evaluation involved assessing how well the reference design addresses the objectives of the scenario it was intended to support. 6.3.1 Scenario 1 Scenario 1 involved the ordinary exchange of email between two organizations’ email servers carried over TLS, where the TLS key management was protected by DANE and DNSSEC. Private certificates were generated by either well-known CAs, enterprise local CAs or self-signed. User connections to their organizations’ respective mail servers were established and maintained within a physically protected zone, and email was encrypted between mail servers using TLS. The confidentiality of encryption keys was maintained such that no unauthorized third party had access to the keys. The mail servers used X.509 certificates to store and transport public keys to establish the TLS channel. DNSSEC ensured that each sending mail server receives the IP address to the legitimate and authorized receiving mail server and (if applicable) validate its X.509 certificate. DANE bound the cryptographic keying material to the appropriate server. TLS was used to protect the confidentiality of the email exchange. Encryption of the email message was accomplished by the originator’s email server, and decryption of the email message was accomplished by the recipient’s email server using standard server libraries. The tests included an attempt by a fraudulent mail server to pose as the legitimate mail receiver for a domain. The tests also include a man-in-the-middle attack to attempt to disrupt the TLS connection with the objective of achieving an unencrypted transmission of the email. Both attempts failed due to use of DNSSEC and DANE. In both cases, an indication was made available to the sending email server when the DNSSEC signature associated with the domain data is determined to be invalid. 6.3.2 Scenario 2 Scenario 2 involved end-to-end signed email, where the email exchanges between organizations were carried over TLS as in (1), the email messages were signed and verified with S/MIME on the end users’ client devices, and the S/MIME key management was protected by DANE and DNSSEC. Private certificates were generated by well-known and enterprise local CAs. Self-signed certificates were not used. Individuals established connections to their domains’ respective mail servers within a physically protected zone of control. Cryptographic digital signatures were applied to messages to provide authentication and integrity protection for the email. S/MIME was the protocol used for the digital signing. These certificates were then encoded in the DNS using the appropriate DANE DNS record type. DNSSEC ensured that each originating user’s mail server connects to the intended recipient’s mail server. DANE bound the cryptographic keying material to the appropriate server and individual user digital signature certificates. TLS was employed to protect the confidentiality of the email. Digital signing of email messages was accomplished by the originator’s MUA, and checking the validity of the signature NIST SP 1800-6B: Domain Name System-Based Electronic Mail Security 58 This publication is available free of charge from: https://doi.org/10.6028/NIST.SP.1800-6. (hence the integrity of the authorization provided in the email message) was accomplished by the recipient’s MUA. The tests in this scenario included an attempt by a fraudulent actor to pose as an originator of the email. This attempt failed due to use of DNSSEC and DANE. The receiving MUA, using a third party SMIMEA tool, was able to fetch the sender’s real S/MIME certificate from the DNS and confirm that the fraudulent email was signed using a different certificate. 6.3.3 Effects of DANE Errors In addition to the scenarios described above, a DANE-enabled Postfix MTA sent message traffic to four other postfix MTAs. A single BIND instance was set up to serve the TLSA and A RRs for the four receivers. One of the receiving MTAs did not employ DANE. The second employed DANE with a valid TLSA with the certificate usage field2 set to 3. The third employed a TLSA with a certificate usage field of 2, but with an incomplete (i.e. bad) PKI certification path (generating a PKIX validation failure). The TLSA contained a local enterprise trust anchor, but the server did not have the full certificate chain (missing intermediate certificate). The final one employed DANE with a TLSA RR using Certificate Usage of 3, but there was a mismatch between the server cert and TLSA RR (generating a DANE validation failure). Little or nothing appeared in the sender’s logs for messages sent to either the MTA not employing TLS or the employing a valid TLSA. The growth rates for logs for the MTA that employed a TLSA with a certificate usage field of 1, but with a PKIX failure and the one that employed mismatched server cert/TLSA (i.e., DANE validation failure) were measured. When the sender was configured to never use TLS, the mail was sent in plaintext regardless of the TLS/DANE configuration of the receiver. When the sender was configured to use TLS opportunistically, it used TLS regardless of the status of the certificate, or TLSA. In fact, the sender did not issue a query to find TLSA RRs even if published. When the sender used opportunistic DANE, it used TLS when available regardless of the DANE validations results. If validation failed, the mail was still sent and the result was logged as an “Untrusted” or “Anonymous” TLS connection, depending on the presence of a TLSA RR. Of the four options used in the lab, “dane-only” is the most rigorous in what a sender would accept before sending mail. When the receiver did not offer the STARTTLS option, or lacked a TLSA RR, mail was not sent. Likewise, if a TLSA RR was present, but there was an error in validation (either the TLSA RR itself had an error, or PKIX failed), the mail was not sent. Therefore, use of this option is not recommended for general use as this will result in the majority of email being deferred. It should only be used in scenarios where senders and receivers are coordinated and maintain a stable DANE deployment. NIST SP 1800-6B: Domain Name System-Based Electronic Mail Security 59 This publication is available free of charge from: https://doi.org/10.6028/NIST.SP.1800-6. 7 Future Build Considerations Both public sector and private sector enterprises are heavily dependent on web-based technology other than email for e-commerce and other public-facing applications. Fraudulent web sites pose at least as great a security and privacy problem as fraudulent email. Further, as email becomes a more difficult medium for malicious entities to use as a penetration vector, other web-based media will be more intensively exploited. Already, emerging communications trends appear to be replacing email exchanges among individuals with other social media (e.g., Baidu, Facebook, Facebook Messenger, Google+, Instagram, LinkedIn, Pinterest, Snapchat, Tieba, Tumblr, Twitter, Viber, WhatsApp, and YouTube). Therefore, an extension of the current project that focuses on use of improved DNSSEC applications such as DANE for web applications other than mail may be justified. Additionally, the test scenarios did not include the Exchange for Office 365 MTA to demonstrate Scenario 1. Future builds might be considered to demonstrate this capability. Finally, utilities are currently under development that would provide improved support for SMIMEA and improved system notification of failed DNSSEC signature validation events. Future builds might be considered to demonstrate these capabilities as well. NIST SP 1800 -6B: Domain Name System -Based Electronic Mail Security 60 This publication is available free of charge from: https://doi.org/10.6028/NIST.SP.1800-6. Appendix A List of Acronyms AES Advanced Encryption Standard ANTD Advanced Network Technologies Division ASCII American Standard Code for Information Interchange ASN.1 Abstract Syntax Notation One AXFR DNS Full Zone Transfer Query Type BGP Border Gateway Protocol BIND Berkeley Internet Name Domain CA Certificate Authority CKMS Cryptographic Key Management System CRADA Cooperative Research and Development Agreement CRL Certificate Revocation List CSF Cybersecurity Framework CU Certificate Usage Type CVE Common Vulnerabilities and Exposures DANE DNS - Based Authentication of Named Entities DARPA Defense Advanced Research Projects Agency DES Data Encryption Standard DNS Domain Name System DNSSEC DNS Security Extensions Email Electronic Mail EMC Electromagnetic Compatibility EMI Electromagnetic Interference FCKMS Federal Cryptographic Key Management System FIPS Federal Information Processing Standard FOIA Freedom of Information Act NIST SP 1800 -6B: Domain Name System -Based Electronic Mail Security 61 This publication is available free of charge from: https://doi.org/10.6028/NIST.SP.1800-6. HIPAA Health Insurance Portability and Accountability Act HTTPS Hypertext Transfer Protocol Secure IDIQ Indefinite Delivery/Indefinite Quantity IEC International Electrotechnical Commission IEEE Institute of Electrical and Electronics Engineers IETF Internet Engineering Task Force IoT Internet of Things IP Internet Protocol IPsec Internet Protocol Security IRS Internal Revenue Service ISC Internet Systems Consortium ISO Internet Organization for Standardization IT Information Technology ITL Information Technology Laboratory MIME Multipurpose Internet Mail Extension MTA Mail Transfer Agent MUA Mail User Agent MX Mail Exchange (Resource Record) NCCoE National Cybersecurity Center of Excellence NIST National Institute of Standards and Technology NVD National Vulnerability Database OMB Office of Management and Budget OS Operating System PKI Public Key Infrastructure PKIX Public Key Infrastructure X.509 RFC Request for Comments RMF Risk Management Framework NIST SP 1800 -6B: Domain Name System -Based Electronic Mail Security 62 This publication is available free of charge from: https://doi.org/10.6028/NIST.SP.1800-6. RR Resource Record RRL Response Rate Limiting S/MIME Secure/Multipurpose Internet Mail Extensions SHA Secure Hash Algorithm SMIMEA S/MIME Certificate Association (Resource Record) SMTP Simple Mail Transfer Protocol SP Special Publication SQL Structured Query Language TLS Transport Layer Security TLSA TLS Certificate Association (Resource Record) UA User Agent VM Virtual Machine NIST SP 1800-6B: Domain Name System-Based Electronic Mail Security 63 This publication is available free of charge from: https://doi.org/10.6028/NIST.SP.1800-6. Appendix B References Securing the Federal Government’s Domain Name System Infrastructure, Executive Office of the President, Office of Management and Budget, M-08-23, August 22, 2008. https://www.whitehouse.gov/sites/whitehouse.gov/files/omb/memoranda/2008/m08-23.pdf Enhancing the Security of Federal Information and Information Systems, Executive Office of the President, Office of Management and Budget, M-14-03, November 18, 2013. https://www.whitehouse.gov/sites/whitehouse.gov/files/omb/memoranda/2014/m-14-03.pdf Improving Critical Infrastructure Cybersecurity, Executive Office of the President, Executive Order 13636, February 12, 2013. https://obamawhitehouse.archives.gov/the-pressoffice/2013/02/12/executive-order-improving-critical-infrastructure-cybersecurity Federal Information Security Management Act, United States Congress, Public Law 107-347, December 17, 2002. https://www.govtrack.us/congress/bills/107/hr2458 Gramm-Leach-Bliley Act, United States Congress, Public Law 104-191, August 21, 1996. https://www.gpo.gov/fdsys/pkg/PLAW-106publ102/html/PLAW-106publ102.htm Health Insurance Portability and Accountability Act, United States Congress, Public Law 106-102, November 12, 1999. https://aspe.hhs.gov/report/health-insurance-portability-andaccountability-act-1996 Managing Information as a Strategic Resource, OMB Circular A-130, Executive Office of the President, Office of Management and Budget, July 28, 2016. https://www.federalregister.gov/documents/2016/07/28/2016-17872/revision-of-ombcircular-no-a-130-managing-information-as-a-strategic-resource Rules Governing Practice before the Internal Revenue Service, Internal Revenue Service, Circular Number 230, Revised June 2014. https://www.irs.gov/tax-professionals/circular-230-tax-professionals Security Requirements for Cryptographic Modules, Federal Information Processing Standard (FIPS) 140- 2, May 2001 (including change notices as of 12-03-2002). https://doi.org/10.6028/NIST.FIPS.140-2 Guide for Conducting Risk Assessments, NIST Special Publication 800-30 Revision 1, Joint Transformation Initiative, September 2012. https://doi.org/10.6028/NIST.SP.800-30r1 Guide for Applying the Risk Management Framework to Federal Information Systems: A security Lifecycle Approach, NIST Special Publication 800-37 Rev. 1, Joint Task Force Transformation Initiative; February 2010 with updates as of June 5, 2014. https://doi.org/10.6028/NIST.SP.800- 37r1 NIST SP 1800-6B: Domain Name System-Based Electronic Mail Security 64 This publication is available free of charge from: https://doi.org/10.6028/NIST.SP.1800-6. Managing Information Security Risk: Organization, Mission, and Information System View, NIST Special Publication 800-39, Joint Task Force Transformation Initiative, March 2011. https://doi.org/10.6028/NIST.SP.800-39 Guidelines on Electronic Mail Security; NIST Special Publication 800-45 Ver. 2; Tracy, Jansen, Scarfone, Butterfield; February 2007. https://doi.org/10.6028/NIST.SP.800-45ver2 Federal S/MIME V3 Client Profile, NIST Special Publication 800-49, Chernick, November 2002. https://doi.org/10.6028/NIST.SP.800-49 Guidelines for the Selection, Configuration, and Use of Transport Layer Security (TLS) Implementations; NIST Special Publication 800-52 Rev. 1; Polk, McKay, Chokhani; April 2014. https://doi.org/10.6028/NIST.SP.800-52r1 Security and Privacy Controls for Federal Information Systems and Organizations, NIST Special Publication 800-53 Rev. 4, Joint Task Force Transformation Initiative, April 2013. https://doi.org/10.6028/NIST.SP.800-53r4 Recommendation for Key Management: Part 1 - General, NIST Special Publication 800-57 Part 1 Rev.4, Barker, January 2016. https://doi.org/10.6028/NIST.SP.800-57pt1r4 Recommendation for Key Management: Part 2 - Best Practices for Key Management Organization, NIST Special Publication 800-57 Part 2, Barker, Barker, Burr, Polk, and Smid, August 2005. https://doi.org/10.6028/NIST.SP.800-57p2 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. https://doi.org/10.6028/NIST.SP.800-57pt3r1 Electronic Authentication Guideline; NIST Special Publication 800-63-2; Burr, Dodson, Newton, Perlner, Polk, Gupta, Nabbus; August 2013. doi:10.6028/NIST.SP.800-63-2 [Direct Link] Digital Identity Guidelines; NIST Special Publication 800-63-3; Burr, Choong, Danker, Grassi, Garcia, Greene, Fenton, Lefkovitz, Nadeau, Netwon, Perlner, Regenscheid, Richer, Squire, Theofanos; June 2017. doi:10.6028/NIST.SP.800-63-3 https://pages.nist.gov/800-63-3/ Secure Domain Name System (DNS) Deployment Guide, NIST Special Publication 800-81-2, Chandramouli and Rose, September 2013. https://doi.org/10.6028/NIST.SP.800-81-2 A Framework for Designing Cryptographic Key Management Systems; NIST Special Publication 800-130; Barker, Branstad, Smid, Chokhani; August 2013. https://doi.org/10.6028/NIST.SP.800-130 A Profile for U.S. Federal Cryptographic Key Management Systems (CKMS); NIST Special Publication 800- 152; Barker, Smid, Branstad; October 2015. https://doi.org/10.6028/NIST.SP.800-152 NIST SP 1800-6B: Domain Name System-Based Electronic Mail Security 65 This publication is available free of charge from: https://doi.org/10.6028/NIST.SP.1800-6. Systems Security Engineering: Considerations for a Multidisciplinary Approach in the Engineering of Trustworthy Secure Systems, NIST Special Publication 800-160, Ross, McEvilley, Oren, November 2016. https://doi.org/10.6028/NIST.SP.800-160. Trustworthy Email; NIST Special Publication 800-177; Chandramouli, Garfinkel, Nightingale and Rose; September 2016. https://doi.org/10.6028/NIST.SP.800-177 “Internet of Things: Standards and Guidance from the IETF”, IETF Journal, Keränen and Bormann, April 2016. https://www.ietfjournal.org/internet-of-things-standards-and-guidance-from-the-ietf/ X.509 Certificate Policy for the U.S. Federal PKI Common Policy Framework, Version 1.24. https://www.idmanagement.gov/wp-content/uploads/sites/1171/uploads/Common-PolicyFramework.pdf Internet Protocol, RFC 791, Defense Advanced Research Projects Agency (DARPA), September 1981. https://datatracker.ietf.org/doc/rfc791 Domain Names - Concepts and Facilities, RFC 1034, Mockapetris, November 1987. https://datatracker.ietf.org/doc/rfc1034 Domain Name System Structure and Delegation, RFC 1591, Postel, March 1994. https://datatracker.ietf.org/doc/rfc1591 Internet X.509 Public Key Infrastructure Certificate and CRL Profile, RFC 2459, Housley, Ford, Polk, and Solo, January 1999. https://datatracker.ietf.org/doc/rfc2459 The Secure HyperText Transfer Protocol, RFC 2660, Rescorla and Schiffman, August 1999. https://datatracker.ietf.org/doc/rfc2660 Threat Analysis of the Domain Name System (DNS), RFC 3833, Atkins and Austein, August 2004. https://datatracker.ietf.org/doc/rfc3833 A Method for Storing IPsec Keying Material in DNS, RFC 4025, Richardson, February 2005. https://datatracker.ietf.org/doc/rfc4025 DNS Security Introduction and Requirements, RFC 4033, Arends, Austein, Larson, Massey, and Rose, March 2005. https://datatracker.ietf.org/doc/rfc4033 A Border Gateway Protocol 4 (BGP-4), RFC 4271, Rekhter, Li, and Hares, January 2006. https://datatracker.ietf.org/doc/rfc4271 The Transport Layer Security (TLS) Protocol Version 1.2, RFC 5246, Dierks and Rescorla, August 2008. https://datatracker.ietf.org/doc/rfc5246 NIST SP 1800-6B: Domain Name System-Based Electronic Mail Security 66 This publication is available free of charge from: https://doi.org/10.6028/NIST.SP.1800-6. Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile, Proposed Standard, RFC 5280, Cooper, Santesson, Farrell, Boeyen (Entrust), Housley, and Polk, May 2008. https://datatracker.ietf.org/doc/rfc5280/ Simple Mail Transfer Protocol, RFC 5321, Draft Standard, Kleinstein, October 2008. https://datatracker.ietf.org/doc/rfc5321 Secure/Multipurpose Internet Mail Extensions (S/MIME), Version 3.2, Message Specification, Proposed Standard, RFC 5751, Ramsdell and Turner, January 2010. https://datatracker.ietf.org/doc/rfc5751 Use Cases and Requirements for DNS-Based Authentication of Named Entities (DANE), RFC 6394, Barnes, October 2011. https://datatracker.ietf.org/doc/rfc6394 The DNS-Based Authentication of Named Entities (DANE) Transport Layer Security Protocol: TLSA, Proposed Standard, RFC 6698, Hoffman and Schlyter, August 2012. https://datatracker.ietf.org/doc/rfc6698 DNS-Based Service Discovery, RFC 6763, Cheshire and Krotchmal, February 2013. https://datatracker.ietf.org/doc/rfc6763 Updates to the Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile, Proposed Standard, RFC 6818, Yee, January 2013. https://datatracker.ietf.org/doc/rfc6818 SMTP Security via Opportunistic DNS-Based Authentication Named Entities (DANE) Transport Layer Security (TLS), RFC 7672, Dukhovni and Hardaker, May 26, 2015. https://datatracker.ietf.org/doc/rfc7672 Using Secure DNS to Associate Certificates with Domain Names for S/MIME, RFC 8162, Hoffman and Schlyter, May 2017. https://datatracker.ietf.org/doc/rfc8162/ Domain Name System-Based Security for Electronic Mail, Barker, National Institute of Standards and Technology’s Dakota Consulting Indefinite Delivery/Indefinite Quantity (IDIQ) Contract SB1341- 12-CQ-0011, Task Order 15- 421 Task 3 Report #2, December 17, 2016. https://nccoe.nist.gov/library/dns-based-secured-email Task 2: Report #1 on Standards Review and Support for NCCoE Project Activities, Barker, National Institute of Standards and Technology’s Dakota Consulting IDIQ Contract SB1341-12-CQ-0011, Task Order 15-421 Task 2 Report #1, November 30, 2015. Task 3: Report #1 on Standards Review and Support for NCCoE Project Activities, Barker, National Institute of Standards and Technology’s Dakota Consulting IDIQ Contract SB1341-12-CQ-0011, Task Order 15-421 Task 3 Report #1, November 30, 2015. NIST SP 1800-6B: Domain Name System-Based Electronic Mail Security 67 This publication is available free of charge from: https://doi.org/10.6028/NIST.SP.1800-6. Appendix C Project Mapping to the Framework Core and Informative References The following tables map informative NIST and consensus security references to Framework Core Subcategories that are addressed by the project’s platform set. The references do not include protocol specifications that are implemented by the individual products that comprise the demonstrated security platforms. While some of the references provide general guidance that informs implementation of referenced Framework Core functions, the NIST Special Publication references provide specific recommendations that should be considered when composing and configuring security platforms from DNS and email components, implementing DNSSEC and mail security platforms, and operating email systems securely. Table C.1 PROTECT (PR) Category Subcategory Informative References Data Security (PR.DS): Information and records (data) are managed consistent with the organization’s risk strategy to protect the confidentiality, integrity, and availability of information. PR.DS-1: Data-at-rest is protected FIPS 140-2 Sec. 4 NIST SP 800-53 Rev. 4 SC-28 NIST SP 800-57 Part 1 Rev. 4 4.2.5, 5.1.1, 5.2.1, 5.3.4, 5.3.5, 5.3.6, 6.2.2.3 NIST SP 800-57 Part 2 2.2, 2.4, 3.2, 4.3, 5.3.3, 5.3.4, A.1.2, A.2.1, A.3.2 NIST SP 800-130 1, 2.1, 2.2, 2.9, 6.1, 6.2, 6.5 NIST SP 800-152 2.2, 4.3, 4.6, 4.7, 6.1.3, 6.4.14, 6.4.29 CCS CSC 17 COBIT 5 APO01.06, BAI02.01, BAI06.01, DSS06.06 ISA 62443-3-3:2013 SR 3.4, SR 4.1 ISO/IEC 27001:2013 A.8.2.3 PR.DS-2: Data-in-transit is protected FIPS 140-2 Sec. 4 NIST SP 1800-6B: Domain Name System-Based Electronic Mail Security 68 This publication is available free of charge from: https://doi.org/10.6028/NIST.SP.1800-6. Category Subcategory Informative References NIST SP 800-45 Ver. 2 All NIST SP 800-49 2 NIST SP 800-52 Rev. 1 3, 4, D1.4 NIST SP 800-53 Rev. 4 SC-8 NIST SP 800-57 Part 1 Rev. 4 4.2.5, 5.1.1, 5.2.1, 5.3.4, 5.3.5, 5.3.6, 6.2.1.3 NIST SP 800-57 Part 2 2.2, 5.3.3, A.2, A.3.1, A.3.2 NIST SP 800-81-2 All NIST SP 800-130 1, 2.1, 2.2, 2.9, 6.1, 6.2, 6.4, 6.7.2 NIST SP 800-152 6.1.2, 6.2.1 NIST SP 800-177 All CCS CSC 17 COBIT 5 APO01.06, DSS06.06 ISA 62443-3-3:2013 SR 3.1, SR 3.8, SR 4.1, SR 4.2 ISO/IEC 27001:2013 A.8.2.3, A.13.1.1, A.13.2.1, A.13.2.3, A.14.1.2, A.14.1.3 PR.DS-6: Integrity checking mechanisms are used to verify software, firmware, and information integrity FIPS 140-2 Sec. 4 NIST SP 800-45 Ver. 2 2.4.2, 3, 4.2.3, 4.3, 5.1, 6.1, 7.2.2, 8.2, 9.2 NIST SP 800-49 2.2.1, 2.3.2, 3.4 NIST SP 800-52 Rev. 1 3, 4, D1.4 NIST SP 800-53 Rev. 4 SI-7 NIST SP 800-57 Part 1 Rev. 4 5.5, 6.1, 8.1.5.1, B.3.2, B.5 NIST SP 1800-6B: Domain Name System-Based Electronic Mail Security 69 This publication is available free of charge from: https://doi.org/10.6028/NIST.SP.1800-6. Category Subcategory Informative References NIST SP 800-57 Part 2 1, 3.1.2.1.2, 4.1, 4.2, 4.3, A.2.2, A.3.2, C.2.2 NIST SP 800-81-2 All NIST SP 800-130 2.2, 4.3, 6.2.1, 63, 6.4, 6.5, 6.6.1 NIST SP 800-152 6.1.3, 6.2.1, 8.2.1, 8.2.4, 9.4 NIST SP 800-177 2.2, 4.1, 4.4, 4,5, 4,7, 5.2, 5.3 ISA 62443-3-3:2013 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 Protective Technology (PR.PT): Technical security solutions are managed to ensure the security and resilience of systems and assets, consistent with related policies, procedures, and agreements. PR.PT-4: Communications and control networks are protected OMB M-08-23 FIPS 140-2 Sec. 4 NIST SP 800-49 2.4.3, 2.4.4 NIST SP 800-52 Rev. 1 3, 4 NIST SP 800-53 Rev. 4 AC-4, AC-17, AC-18, CP-8, SC-7 NIST SP 800-57 Part 1 Rev. 4 5.3.1, 6.2.2 NIST SP 800-130 8.3 NIST SP 800-152 4.7, 4.11.1, 6.8.6, 8.3 CCS CSC 7 COBIT 5 DSS05.02, APO13.01 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 1800-6B: Domain Name System-Based Electronic Mail Security 70 This publication is available free of charge from: https://doi.org/10.6028/NIST.SP.1800-6. Table C.2 DETECT (DE) Category Subcategory Informative References Security Continuous Monitoring (DE.CM): The information system and assets are monitored at discrete intervals to identify cybersecurity events and verify the effectiveness of protective measures. DE.CM-1: The network is monitored to detect potential cybersecurity events FIPS 140-2 Sec. 4 SP 800-37 Rev. 1 3.6 NIST SP 800-45 Ver. 2 4.1, 5.1.1, 5.1.5, 6.2.1, 6.2.2, 7.2.2 NIST SP 800-53 Rev. 4 AC-2, AU-12, CA-7, CM-3, SC-5, SC-7, SI-4 NIST SP 800-81-2 2, 9, 12, 13 NIST SP 800-130 5, 6.8.5, 8.2.4, 9.8.4 NIST SP 800-152 6.8.5, 8.2.3, 8.2.4, 8.3, 8.5 NIST SP 800-177 3.1.1 CCS CSC 14, 16 COBIT 5 DSS05.07 ISA 62443-3-3:2013 SR 6.2 DE.CM-6: External service provider activity is monitored to detect potential cybersecurity events NIST SP 800-53 Rev. 4 CA-7, PS-7, SA-4, SA-9, SI-4 NIST SP 800-81-2 2, 9, 12, 13 NIST SP 800-130 6.8.5, 8.2.4, 9.8.4, 12 NIST SP 800-152 6.8.5, 8.2.3, 8.2.4, 8.3, 8.5 ISO/IEC 27001:2013 A.14.2.7, A.15.2.1 Detection Process (DE.DP): Detection processes and procedures are maintained and tested to ensure timely and DE.DP-4: Event detection information is communicated to appropriate parties NIST SP 800-45 Ver. 2 9.3 NIST SP 800-53 Rev. 4 AU-6, CA-2, CA-7, RA-5, SI-4 NIST SP 800-177 4.6 COBIT 5 APO12.06 NIST SP 1800-6B: Domain Name System-Based Electronic Mail Security 71 This publication is available free of charge from: https://doi.org/10.6028/NIST.SP.1800-6. Category Subcategory Informative References adequate awareness of anomalous events. ISA 62443-2-1:2009 4.3.4.5.9 ISA 62443-3-3:2013 SR 6.1 ISO/IEC 27001:2013 A.16.1.2 Table C.3 RESPOND (RS) Category Subcategory Informative References Response Planning (RS.RP): Response processes and procedures are executed and maintained, to ensure timely response to detected cybersecurity events. RS.RP-1: Response plan is executed during or after an event NIST SP 800-45 Ver. 2 9.3 NIST SP 800-53 Rev. 4 CP-2, CP-10, IR-4, IR-8 NIST SP 800-57 Part 1 Rev. 4 NIST SP 800-57 Part 2 3.1.2.1.3, 3.2.2.6 NIST SP 800-130 6.2.1, 6.4.5, 6.4.6, 6.8, 10.1 NIST SP 800-152 6.8, 10 NIST SP 800-177 4.6 COBIT 5 BAI01.10 CCS CSC 18 ISA 62443-2-1:2009 4.3.4.5.1 ISO/IEC 27001:2013 A.16.1.5 Communications (RS.CO): Response activities are coordinated with internal and external stakeholders, as appropriate, to include external RS.CO-2: Events are reported consistent with established criteria NIST SP 800-45 Ver. 2 9.3 NIST SP 800-53 Rev. 4 AU-6, IR-6, IR-8 NIST SP 800-57 Part 1 Rev. 4 8.3.5, 9.3.4, 10.2.9 NIST SP 1800-6B: Domain Name System-Based Electronic Mail Security 72 This publication is available free of charge from: https://doi.org/10.6028/NIST.SP.1800-6. Category Subcategory Informative References support from law enforcement agencies. NIST SP 800-57 Part 2 3.1.2.1.2, 3.2.2.10, 3.2.2.14, 3.2.2.15, A.1.1, A.1.4, C.2.2.12 NIST SP 800-130 6.8 NIST SP 800-152 6.8 NIST SP 800-177 4.6 ISA 62443-2-1:2009 4.3.4.5.5 ISO/IEC 27001:2013 A.6.1.3, A.16.1.2 Mitigation (RS.MI): Activities are performed to prevent expansion of an event, mitigate its effects, and eradicate the incident. RS.MI-1: Incidents are contained NIST SP 800-53 Rev. 4 IR-4 NIST SP 800-130 6.8.1 NIST SP 800-152 6.8 ISA 62443-2-1:2009 4.3.4.5.6 ISA 62443-3-3:2013 SR 5.1, SR 5.2, SR 5.4 ISO/IEC 27001:2013 A.16.1.5 RS.MI-2: Incidents are mitigated NIST SP 800-53 Rev. 4 IR-4 NIST SP 800-57 Part 1 Rev. 4 5.3, 5.4, 5.5, 8.3.4, 8.3.5 NIST SP 800-57 Part 2 5.3.7, 5.3.8 NIST SP 800-130 4.9.3, 6.8, 9.5, 12 NIST SP 800-152 3.4.2, 4.5, 6.8, 9.5, 9.8, 12 ISA 62443-2-1:2009 4.3.4.5.6, 4.3.4.5.10 ISO/IEC 27001:2013 A.12.2.1, A.16.1.5