**References to the terms HTTP Post, HTTP Request, HTTP Response describe application-level protocols that are not related to security and do not need to be reviewed for possible modification.**

**References in the WGQ QEDM Manual (Version 3.1) that support staying out of the processes that occur behind the firewall:**

|  |  |  |
| --- | --- | --- |
| Page # | Applicable Text | Item # |
| 32 | To prevent unwanted intruders from connecting to Web sites, HTTP Basic Authentication using transport layer security is required. Additional issues such as firewall security are discussed in the standards and specific security implementation details should be addressed by each organization. | D1 |

**WGQ Principles that support staying out of the processes that occur behind the firewall:**

|  |  |  |
| --- | --- | --- |
| Principle | Text of the Principle | Item # |
| 4.1.15 | The North American Energy Standards Board Wholesale Gas Quadrant should not set standards for site-level security. Individual organization security standards should be relied upon. | D2 – delete – see Pipeline 4.1.15 WP |
| 10.1.7 | The NAESB Internet ET should not set standards for site-level security. Individual organization security standards should be relied upon. | D3 – see pipeline 4.1.15 WP |

**Retail Principles that support staying out of the processes that occur behind the firewall:**

|  |  |  |
| --- | --- | --- |
| Principle | Text of the Principle | Item # |
| 7.1.7 | The NAESB Internet ET should not set standards for site-level security. Individual organization security standards should be relied upon. | D4  see pipeline 4.1.15 WP |

**WGQ Principles to be reviewed for possible conversion to a standard**

|  |  |  |
| --- | --- | --- |
| Principle | Text of the Principle | Item # |
| 4.1.39 | Trading Partners should mutually agree to use either the current, or the immediately previous published version of the NAESB WGQ EDM standards as a basis under which to operate, unless:   1. Security standards with the current NAESB Internet Electronic Transport and/or the WGQ QEDM are not compatible with security standards in the previous version, and/or   (b) specified otherwise by an applicable regulatory authority. | D5 – make a 4.3.xx standard |
| 10.1.9 | Trading Partners should mutually agree to either the current, or the immediately previous (unless NAESB Internet Electronic Transport security standards are not compatible), published version of the NAESB Internet Electronic Transport standards as a basis under which to operate, unless specified otherwise by an applicable regulatory authority. | D6 – modify as 4.1.39 above. |

**Retail Principles to be reviewed for possible conversion to a standard**

|  |  |  |
| --- | --- | --- |
| Principle | Text of the Principle | Item # |
| 5.1.6 | Trading Partners should mutually agree to use either the current, or the immediately previous version of the NAESB RXQ Model Business Practices under which to operate, unless specified otherwise by the Applicable Regulatory Authority. Trading Partners should also mutually agree to upgrade or adopt later versions of RXQ Model Business Practices as needed, unless specified otherwise by the Applicable Regulatory Authority. | D7 – modify as above?? |
| 7.1.9 | Trading Partners should mutually agree to either the current, or the immediately previous, published version of the NAESB Internet Electronic Transport standards as a basis under which to operate, unless specified otherwise by an applicable regulatory authority. | D8 - modify as above?? |

**WGQ Standards to be reviewed for possible modification**

| Standard | Text of the Standard | Item # |
| --- | --- | --- |
| 4.3.60 | Access to the Customer Activities Web Site should be protected by HTTP Basic Authentication using transport layer security or similar logon/password mechanism(s). A Customer Activities Web site should require a single logon/password pair for each user session. | D9 |
| 4.3.61 | Customer Activities Web sites should utilize transport layer security, as specified in Appendix B of the Quadrant Electronic Delivery Mechanism Related Standards. | D10 |
| 4.3.62 | Custom downloadable modules presented by a Customer Activities Web site should be signed by the author. The signatures on these modules should be communicated in advance to Web site users. | D11 |
| 4.3.83 | For Interactive Flat File EDM, transport layer security should be used, as specified in Appendix B of the Quadrant Electronic Delivery Mechanism Related Standards. | D12 |
| 4.3.84 | Access to Interactive Flat File EDM should be protected by HTTP Basic Authentication using transport layer security, as specified in Appendix B of the Quadrant Electronic Delivery Mechanism Related Standards. | D13  Reference RFC(7617) for Basic Authentication in Appendix |
| 10.2.33 | ‘;’TLS’. Transport Layer Security; a privacy technique that uses encryption to hide information from electronic observers on the Internet. | D14 |
| 10.2.34 | ‘PGP’. Pretty Good Privacy; software used to create Public and Private Keys for privacy and digital signature applications. | D15 |
| 10.2.xx | ‘OpenPGP’. Open Pretty Good Privacy; open source encryption used to create Public and Private Keys for privacy and digital signature applications. | D15  Refernece RFC(4880) for OpenPGP in Appendix |
| 10.3.4 | All trading partners should communicate using the minimum HTTP version, as specified in Appendix A of the NAESB Internet Electronic Transport Related Standards. | D16 |
| 10.3.15 | Trading partners should implement all security features (privacy, secure authentication, integrity, and non-repudiation) using a file-based approach using an OpenPGP product or, on a mutually agreed basis, PGP, as specified in Appendix A of the NAESB Internet ET Related Standards. | D17  Move all RFC or version # to Appendix A. |
| 10.3.16 | Trading partners should implement HTTP Basic Authentication using transport layer security, as specified in Appendix A of the NAESB Internet ET Related Standards. | D18 Update Appendix A with transport layer security. |
| 10.3.25 | Internet ET servers should use transport layer security, as specified in Appendix A of the NAESB Internet Electronic Transport Related Standards. | D19 |

**Retail Model Business Practices to be reviewed for possible modification**

| MBP | Text of the Model Business Practice | Item # |
| --- | --- | --- |
| 5.3.2.2 | All RXQ EDM payloads should be encrypted with a minimum 128-bit key when sent on unsecured networks (Internet). This mechanism is specified in the NAESB RGQ & REQ Internet Electronic Transport Model Business Practices . Where other transport options are used, comparable transport layer security should be used. | D20 |
| 5.3.4.14 | FF/EDM payloads should be encrypted prior to Internet transport when not using NAESB RGQ & REQ Internet Electronic Transport Model Business Practices. | D21 |
| 7.2.34t | ‘PGP’. Pretty Good Privacy; software used to create Public and Private Keys for privacy and digital signature applications. | D22 |
| 7.2.33t | **‘**; ‘TLS’. Transport Layer Security; a privacy technique that uses encryption to hide information from electronic observers on the Internet. | D23 |
| 7.3.4 | The minimum acceptable protocol should be HTTP. All trading partners should communicate using the minimum HTTP version as specified in Appendix A of the NAESB RGQ & REQ Internet Electronic Transport Model Business Practices | D24 |
| 7.3.16 | Trading partners should implement HTTP Basic Authentication using transport layer security, as specified in the NAESB RGQ & REQ Internet Electronic Transport Model Business Practices. | D25 |
| 7.3.25 | Internet Electronic Transport servers should use transport layer security, as specified in the NAESB RGQ & REQ Internet Electronic Transport Model Business Practices | D26 |
| 7.3.15 | Trading partners should implement all security features (privacy, secure authentication, integrity, and nonrepudiation) using a file-based approach using an OpenPGP product or, on a mutually agreed basis, PGP, as specified in Appendix A of the NAESB RGQ & REQ Internet Electronic Transport Model Business Practices. | Update Appendix A |

**References in the WGQ QEDM Manual (Version 3.1) that should be reviewed**

| Page # | Applicable Text | Item # |
| --- | --- | --- |
| 90 | **Login and Encryption**  Customer Activities Web sites should require a single logon/password pair for each user session. HTTP Basic Authentication or similar logon/password mechanism(s) using transport layer security, as specified in Appendix B, should protect access to Customer Activities Web sites. | D27 |
| 92 | FF/EDM employs HTTPS transport layer security . Implementers of FF/EDM should refer to Appendix B - Minimum Technical Characteristics and Guidelines for the Developer and User of the Customer Activities Web Site. This portion of the guide assumes an HTTP multipart form file upload. | D28  Update RFC to 5246 and place in Appendix |
| 97 | **Authentication**  NAESB WGQ Standard No. 4.3.84 calls for use of HTTP Basic Authentication, using transport layer security which is a standard part of the HTTP specification. Access to Interactive FF/EDM screens requires user-id and password. Login screens should be protected using transport layer security as described below. | D29 |
| 97 | **Encryption**  NAESB WGQ Standard No. 4.3.83 calls for the use of transport layer security. Transport layer security, as specified in Appendix B, is accomplished by obtaining a certificate from providers and using Web servers capable of using these certificates. Browsers specified in Appendix B and Appendix C are compatible with sites protected by transport layer security. Pages to be protected with transport layer security must be invoked with the HTTPS protocol by using “https” (versus “http”) as part of the hyperlink (HREF) name. The use of the HTTPS protocol requires the fully qualified URL rather than a relative link name. | D30 |
| 98  (App A) | **HTTP**  The NAESB WGQ EDM architecture is based on HTTP 1.1, and all implementations should be compatible with this version. | D31 |
| 100 (App B) | Browser:  The latest Generally Available (GA) versions of both Mozilla Firefox®Extended Support Release and Microsoft Internet Explorer®within 9 months of such GA version becoming available, characteristics including -  TLS (minimum 128-bit RSA Encryption) using a trusted third party commercial certificate provider. | D32 |
| 100 (App B) | Plug-ins (GA versions within 9 months of such GA versions becoming available) | D33 |
| 104 (App D) | For EDM communications, trading partners should seek to utilize the latest Generally Available version of transport layer security (minimum 128-bit RSA encryption) within 9 months of such version being supported by major development platforms. | D34 |

**References in the Retail QEDM Manual (Version 3.2) that should be reviewed**

| Page # | Applicable Text | Item # |
| --- | --- | --- |
| 35 | Q4: How does this document relate to the Internet Electronic Transport standard and the Model Business Practices developed for specific business processes (e.g. Billing and Payments)?  A: RXQ EDM Model Business Practices are designed to work in concert with the NAESB Internet Electronic Transport standards, and with each Model Business Practices book developed by NAESB REQ and RGQ business subcommittees. The table below summarizes the scope of the different documents:  Transport security layer  OpenPGP/PGP encryption/decryption | D35 |

**References in the WGQ Internet Electronic Transport Manual (Version 3.1) and Retail Internet Electronic Transport Manual (Version 3.2) that should be reviewed**

| WGQ Page | RMQ Page | Applicable Text | Item # |
| --- | --- | --- | --- |
| 5 | 7 | In the Internet Electronic Transport life-cycle, the party sending data, the ‘Sender’, creates an electronic package by encrypting the data payload and applying appropriate header ‘envelope’ information such as ‘to’ and ‘from’. This electronic package is submitted to the trading partner’s transport layer security protected Web server as an HTTP Request using the POST method. | D36 |
| 20 | 14 | Internet Electronic Transport allows encryption using both OpenPGP and PGP as defined in the Internet Electronic Transport appendices. | D37  Move all RFC or version # to Appendix |
| 20 | 14 | ~~PGP 2.6 (minimum) or higher (strongly encouraged), with RSA keys can be used on a mutually agreed basis~~ | D38  Move all RFC or version # to Appendix |
| 20 | 14 | Internet Electronic Transport uses base64-encoding and transport layer security to protect username and password. | D39 |
| 20 | 14 | Authentication  Authentication is the assurance to one entity that another entity is who he/she/it claims to be. HTTP Basic Authentication is the required standard to prevent intruders from connecting to Internet Electronic Transport Web sites. Internet Electronic Transport uses transport layer security to protect usernames and passwords used inauthentication. Optional techniques such as firewall security enable further authentication. | D40 |
| 20 | 14 | Integrity  Integrity is the assurance to an entity that data has not been altered, intentionally or unintentionally, between there and here, or between then and now. Data Integrity is established via OpenPGP/PGP encryption, and via the ‘content-length’ HTTP header field. | D41 |
| 28 | 24 | The NAESB Internet Electronic Transport uses the following technologies and components to securely and reliably transport electronic packages to trading partners:   * OpenPGP and PGP encryption and digital signatures | D42 |
| 33 | 29 | **Abuse of Refnum and Refnum-orig**  There is potential for abuse/error when using the functionality of these mutually-agreed data elements. Parties should monitor for the re-use of numbers used with both refnum and refnum-orig for the receipt and delivery functions. | D43  TBD |
| 33 | 30 | **Using an Interactive Browser for Internet ET**  Electronic packages can be uploaded to a trading partner using an interactive browser secured using transport layer security. | D44 |
| 35 | 31 | **Authentication**  Userids and passwords must be base64-encoded. HTTP Basic Authentication includes a ‘userid’ and ‘password’ and is protected using transport layer security. Interactive browsers include a basic authentication feature that automatically prompts for ‘userid’ and ‘password’. In a batch browser, the authentication must be specifically coded. The ‘userid’ and ‘password’ are to be base64-encoded within the document header. | D45 |
| 39 | 36 | EXAMPLE: AN X12 EDI FILE ENCRYPTED WITH PGP | D46 |
| 50 | n/a | **Pre-validation before Decryption**  Proper trapping of the range of decryption process errors listed in Table 1 (Internet ET Standard Error Codes and Messages) may require program code which is external to the decryption algorithm. Some versions of the PGP software do not explicitly discriminate between EEDM601, EEDM602, EEDM603, and EEDM699 type errors. | D47 |
| n/a | 49 | **Pre-validation before Decryption**  Proper trapping of the range of decryption process errors listed in Table A (Internet ET Standard Error Codes and Messages) may require program code which is external to the decryption algorithm. Some versions of the PGP software do not explicitly discriminate between EEDM601, EEDM602, EEDM603, and EEDM699 type errors. | D48 |
| 50 | 49 | Under such a circumstance, files inbound to the decryption process should be preprocessed to trap the errors not identified by the PGP/OpenPGP version being used. For example, searching the file for the text strings ‘BEGIN PGP MESSAGE’ and ‘END PGP MESSAGE’ can quickly identify ‘EEDM602 File not encrypted’ and ‘EEDM603 Encrypted file truncated’ type errors when the implemented PGP version only identifies decryption success, invalid Public Key (EEDM601), and decryption failure (EEDM699). | D49 |
| 51 | 50 | In general, these needs are met by using the Basic Authentication capability of the Web server and the encryption and digital signature capability of the OpenPGP and PGP security application for securing transactions. | D50 |
| 51 | 50 | **Understanding OpenPGP and PGP**  Pretty Good Privacy (PGP) is the name of a proprietary encryption software chosen for Internet Electronic Transport to both digitally sign and encrypt payloads being sent. OpenPGP is the Internet Engineering Task Force (IETF) standard version of PGP that excludes all patented algorithms, allowing free commercial use of the standard. Both OpenPGP and PGP use a Public Key/Private Key pair to secure and sign files for transfer. The Private Key must be known only to the company that generated it. The Public Key counterpart is shared with trading partners. | D51 |
| 51 | 50 | Each company must generate its Public Key and Private Key pair. The RSA key generation algorithm should be chosen for versions of PGP that offer alternatives. Implementers of OpenPGP should choose DSA and El Gamal when creating their key pair. The Public Keys should be distributed electronically to the company’s trading partners in a secure manner. | D52 |
| 51 | 50 | You should never divulge your Private Key to another party. If an untrusted party has your Private Key, your security is compromised. | D53  Key size RSA minimum 2048 (4096 recommended) in appendix |
| 51 | 50 | **Encryption / Digital Signature**  Encryption and digital signatures are applied to payload files before they are sent by the batch browser. The use of internal file or payload encryption (including but not limited to X12.58 encryption) is outside the scope of NAESB encryption standards but does not conflict with OpenPGP/PGP. | D54 |
| 51 | 51 | Encryption and digital signatures are created using OpenPGP, or on a mutually agreed basis, PGP. Regardless of encrypting in a manual or automated fashion, it is essential that the correct Public Key of the trading partner be used to encrypt and just as essential that the correct Sender’s own Private Key be used to digitally sign the file. | D55 |
| 52 | 51 | **Decryption / Digital Signature Verification**  After a package is received and processed by the Receiving Program, it is ready to be decrypted and have its digital signature verified. Given the correct userID for a trading partner, OpenPGP/PGP uses the appropriate key pair to encrypt, sign and decrypt. Upon request for signature verification, the OpenPGP/PGP will return a human-readable descriptive text such as DUNS number or company name. | D56 |
| 52 | 52 | **OpenPGP or PGP File Encryption**.  Payload files are encrypted using OpenPGP, or on a mutually agreed basis, PGP. | D57 |
| 54 | 53 | PGP MIME malformed (found with some versions of PGP/OpenPGP) | D58 |
| 55 | 55 | Simulated Errors. Test various simulated errors in both file transfers and in OpenPGP or PGP decryption. | D59 |
| 59 | 59 | **OpenPGP Software**  The IETF OpenPGP standard is available at http://www.ietf.org/rfc/rfc4880.txt  Software implementations of the OpenPGP standard are freely available for commercial use from the Free Software Foundation at http://www.gnupg.org. | D60 |
| 60 | 59 | **PGP Software**  PGP is available for a variety of operating systems and platforms. For more information contact Symantec (https://www.symantec.com/products/encryption | D61 |
| 61 | 61 | Q8: Use of ANSI X12.58. If we use ANSI X12.58 encryption do we still need to use OpenPGP or PGP encryption? | D62 |
| 61 | 61 | Q9: What does NAESB recommend for the OpenPGP/PGP descriptive text? | D63 |
| 62 | 62 | ***Q3: What cryptographic algorithms should we use or not use?***  A: OpenPGP implementations should use DSA and El Gamal, and PGP implementations should use RSA. | D64 |
| 63 | 63 | ***Q8: Use of ANSI X12.58. If we use ANSI X12.58 encryption do we still need to use OpenPGP or PGP encryption?***  A: Yes. The use of encryption such as X12.58 on payload files is outside the scope of the NAESB encryption standards. | D65 |
| 63 | 63 | ***Q9: What does NAESB recommend for the OpenPGP/PGP descriptive text?***  A: There are no Internet Electronic Transport standards for the information provided in the OpenPGP/PGP descriptive text data element. Implementers are encouraged to use their company name in this data element. | D66 |