| | |
|---|---|
| Standard ID: | **SE-SDT-001** |
| Title: | **Secure File Transport** |
| Domain: | **Security** |
| Discipline: | **Network Security** |
| Effective Date:<br>Revision no.:<br>Original date: | **9/27/2019**<br>**5**<br>**09/01/2004** |

## I. Authority, Applicability and Purpose

**A. Authority:** Title 29 Chapter 90C Delaware Code, §9004C – General Powers, duties and functions of DTI "2) Create, implement and enforce statewide and agency technology solutions, policies, standards and guidelines, including as recommended by the Technology Investment Council on an ongoing basis and the CIO"

**B. Applicability:** Applies to all State of Delaware communications and computing resources. DTI is an Executive Branch Agency and has no authority over the customers in Legislative and Judicial Branches, as well as School Districts, and other Federal and Local Government entities that use these resources. However, all users, including these entities, must agree to abide by all policies, standards promulgated by DTI as a condition of funding, access and continued use of these resources.

**C. Purpose:** This standard will address the solution set to be used by employees and agents of the State of Delaware to secure data classified as confidential or higher per Data Classification Policy while moving data from point A to B as it is transported across a network.

## II. Scope

**A. Audience**: - This document is intended for Systems Administrators, Network Administrators, Computer Auditors, and Application Development personnel, Project Leaders, Third Party Software Providers and non IT personnel.

**B. Functions:** The Organization Information Security Officer (ISO) and Information Resource Manager (IRM) in concert with the business managers of the State organization are to determine the level of security needed. This standard will cover data determined to require extra security in transport. Once determined, the tools outlined in this document are to be used to secure it. This standard does not cover secure email or attachments. They are covered by the Secure Email Standard.

**C.** **Areas Covered:** This standard covers all data that is to be secured as it is being moved from point A to point B. This standard applies to all data that is owned or maintained by the State of Delaware and will encompass those security requirements mandated by various Federal regulations such as the Health Insurance Portability and Accountability Act of 1996 (HIPAA), Sarbanes-Oxley, and Gramm-Leach-Bliley. This standard will also reflect any applicable court rulings or opinions of the State Attorney General or other data requiring encryption security. This standard does not address what data should be secured. For an aid in determining a reasonable level of data security please consult the Data Classification Policy.

**D.** **Platforms:** Any device being used to move data from point A to point B. This includes State owned servers, mainframes, PC's, notebooks (laptops), and tablet PC's. All third party servers, mainframes, PC's, notebooks (laptops), and tablet PC's that are connected behind the State's firewall are also covered by this standard.

## III. PROCESS

**A.** **Adoption:** These standards have been adopted by the Department of Technology and Information (DTI) through the Technology and Architecture Standards Committee (TASC) and are applicable to all Information Technology use throughout the state of Delaware.

**B.** **Revision:** Technology is constantly evolving; therefore the standards will need to be reviewed regularly. It is the intent of the TASC to review each standard annually. The TASC is open to suggestions and comments from knowledgeable individuals within the state, although we ask that they be channeled through your Information Resource Manager (IRM).

**C.** **Contractors:** Contractors or other third parties are required to comply with these standards when proposing technology solutions to DTI or other state entities. Failure to do so could result in rejection by the Delaware Technology Investment Council. For further guidance, or to seek review of a component that is not rated below, contact the TASC at dti_tasc@state.de.us.

**D.** **Implementation responsibility:** DTI and/or the organization's technical staff will implement these best practices during the course of normal business activities, including business case review, architectural review, project execution and the design, development, or support of systems.

**E.** **Enforcement:** DTI will enforce these best practices during the course of normal business activities, including business case and architectural review of proposed projects and during the design, development, or support of systems. These best practices may also be enforced by others during the course of their normal business activities, including audits and design reviews.

**F.** **Contact us:** – Any questions or comments should be directed to dti_tasc@state.de.us.

## IV. Definitions/Declarations

### A. Definitions/Explanations

**1.** Application Encryption: Data is scrambled by the application before it is stored in the database; database queries return scrambled data that can only be unscrambled by the application. The data is scrambled in the transport stages.

**2.** Asymmetric Key Encryption: In asymmetric key encryption, also known as "public key" encryption, each person has two keys. Any scrambled text created using one of the keys can only be de- scrambled using the other key. This is distinctly different from symmetric encryption where you only have one key that performs both functions on the same message. In asymmetric key encryption, the two keys that each person possesses are commonly named the "private" and "public" keys because the "public" one is published or given out freely to anyone who wants a copy and the "private" one is kept secret. The security of asymmetric key encryption depends on the fact that no one except you can ever access your private key. It must be noted that Asymmetric Key Encryption can be 100 to 1,000 times slower than Symmetric cryptography

**3.** Certificate Authority: Issues and manages security credentials and public keys for message encryption.

**4.** Checkpoint Restart: In the event of an interruption during a file transport this provides a means of automatically restarting the transport at the point where the transport was interrupted, rather than at the beginning of the file.

**5.** Column-level Encryption: Fields within the database are scrambled based on their column; only authorized users see the plain text results. Unauthorized users see scrambled or blank results for those columns that are scrambled. Data is scrambled only in the rest stage.

**6.** Common Public Key Algorithms:

**a)** RSA-for both digital signatures and key exchange. The Rivest-Shamir-Adleman (RSA) cryptographic algorithms are the most widely used public-key algorithms today, especially for data sent over the Internet. The algorithm is named after its three inventors, Ron Rivest, Adi Shamir, and Leonard Adleman. The security of the RSA algorithm is based on the difficulty (in terms of computer processing power and time) of factoring large numbers. RSA is unique among the commonly used public-key algorithms in that it is capable of both digital signature and key exchange operations. The RSA cryptographic algorithms are supported by the Microsoft Base Cryptographic Service Provider (Microsoft Base CSP1) and the Microsoft Enhanced Cryptographic Service Provider (Microsoft Enhanced CSP2) and are built into many software products, including Microsoft Internet Explorer.

**b)** DSA-for digital signatures only. The Digital Signature Algorithm (DSA), invented by the United States National Security Agency (NSA), has been incorporated by the U.S. National Institute of Standards and Technology (NIST) into their Federal Information Processing Standard (FIPS) for digital signatures. DSA derives its security from the difficulty of calculating discrete logarithms. This algorithm can be used only for digital signature operations (not for data encryption). Microsoft CSPs support the DSA algorithm.

**c)** Diffie-Hellman-for key exchange only. Diffie-Hellman, the first public-key algorithm invented, is named after its inventors Whitfield Diffie and Martin Hellman. Diffie-Hellman derives its security from the difficulty of calculating discrete logarithms.

**7.** Confidentiality (encryption): Protecting data from exposure to unauthorized entities. In addition, it is also referred to as privacy.

**8.** Data Encryption: The process of converting plain text into scrambled text in such a fashion that only the intended recipients can decrypt the text back into plain text.

**9.** Digital Signature: A core component of a public key infrastructure (PKI) security installation. A digital signature can prove identity because it is created with the private key portion (which only the key holder should access) of a public/private key pair. Anyone with the sender's widely published public key can decrypt the signature and, by doing so, receive the assurance that the data must have come from the sender (non-repudiation of the sender) and that the data has not changed (integrity). The data that is encrypted with the private key is not the entire message, but a short, fixed-length block of data that is computed from the message using a so-called "hash" function.[1]

**10.** File transport: The transmittal of the contents of a collection of records (file) from point A to point B.

**11.** File Transport Protocol (FTP): A Transmission Control Protocol/Internet Protocol (TCP/IP) standard used to log onto a network, list directories and copy files. FTP authenticates users and allows them to transfer files, list directories, delete and rename files on a remote host, and perform wild-card transfers.[1]

**12.** Hash: A primitive mathematical method used to ensure that what was sent was received by creating a number via a formula that corresponds to various elements in the file. This will be compared to a number generated by that same formula once the file is received.

**13.** Non-repudiation: Ensuring transactions / activities are binding and meaningful (one cannot subsequently deny having performed an activity).

**14.** PGP: Public-key encryption software sold by Network Associates. PGP began as an open standard for message encryption. Add-ons are available for a number of desktop products. The underlying protocol has been designated a military weapon by the United States and some other countries in an effort to regulate its distribution, but similar software is widely available on the Internet.[1]

[1] Gartner, Inc. -- http://www.gartner.com/6_help/glossary/GlossaryMain.jsp

15. Request for Comment (RFC): A document submitted for comment and put through a review process under the auspices of the Internet Engineering Task Force (IETF). When accepted, it has the weight of a standard in the Internet community. Each RFC is given a tracking number. For example, RFC 822 describes the address format and data definitions for addressing electronic messages over the Internet, while RFC 1490 is a standard specification for encapsulating multiple protocols over a wide-area frame relay network.[1]
16. Secure Copy (SCP): http://en.wikipedia.org/wiki/Secure_copy
17. Secure File Transport: The transmittal of data from one computer to another while it is encrypted.
18. Secure file transfer protocol (SFTP): http://en.wikipedia.org/wiki/SSH_file_transfer_protocol
19. Secure Shell (SSH): http://en.wikipedia.org/wiki/Secure_Shell
20. Secure Sockets Layer (SSL): An Internet security standard developed by Netscape Communications. SSL offers session-level security — that is, after a secure session has been initiated, all information transmitted over the Internet during that session is encrypted. SSL also offers features such as server and client authentication as well as message integrity.[1]
21. Symmetric Key Encryption: In symmetric key encryption, the sender and receiver share a "secret" key. Using this key, a file can be encrypted into scrambled text. Using symmetric key encryption, eavesdropping no longer is a problem (unless the eavesdropper knows what the secret key is). It also becomes harder for someone to modify file in transit in any kind of a meaningful way. The problem with symmetric key encryption is precisely the fact that the sender and receiver must share the same secret key
22. Transport Layer Security (TLS): A protocol designed to secure the privacy of communications over the Internet. It is defined in request for comment 2246 from the Internet Engineering Task Force.[1]

## B. Declarations

1. The tools (encryption systems, secure file transport managers, etc.) chosen must be compatible with the diverse environment of the State's IT infrastructure. Either encrypt the pipe (network transport) or the files/data being transported.
2. When authentication is needed to transport files, the authentication must be secure.

## V. Definitions of Ratings

Individual components within a Standard will be rated in one of the following categories.

| COMPONENT RATING | USAGE NOTES |
|---|---|
| **STANDARD** – DTI offers internal support and/or has arranged for external vendor support as well (where applicable). DTI believes the component is robust and can be expected to enjoy a useful life of 3+ years from the Effective Date. | These components can be used without explicit DTI approval for both **new projects** and **enhancement** of existing systems. |
| **DECLINING** – Deprecated - DTI considers the component to be a likely candidate to have support discontinued in the near future. A deprecated element is one becoming invalid or obsolete. | Via the State's waiver process, these components must be explicitly approved by DTI for **all projects**. They must not be used for **minor enhancement** and **system maintenance** without explicit DTI approval via the State's waiver process. |
| **DISALLOWED** – DTI declares the component to be unacceptable for use and will actively intervene to disallow its use when discovered. | No waiver requests for new solutions with this component rating will be considered. |

**A. Missing Components** – No conclusions should be inferred if a specific component is not listed. Instead, contact the TASC to obtain further information.

## VI. Component Assessments

**A.** If the Business Manager (who is the Steward of the data) determines that the data should be encrypted, the Systems Administrators, Network Administrators, Computer Auditors, and Application Development personnel, Project Leaders, and Third Party Software Providers are responsible for ensuring that the entire structure of the environment housing this data is secure. For further information please consult the State of Delaware Information Security Policy. For an aid in determining a reasonable level of data security please consult the Data Classification Policy

**B.** The chosen encryption method must comply with the State's standards.

**C.** The industry is fluctuating between standards bodies and vendor offerings. Data security, however, cannot be ignored while these technologies catch up to business needs. Therefore, this standard will be re-visited every year. It is our intention to select appropriate software products and enter into enterprise-wide licensing agreements when the industry has matured and the funding is available.

**D.** The current states of the vendor products appear to have one thing in common: interoperability problems. No 'Standard' cited below should be taken as acceptable in your environment without a thorough test by you of the product to ensure it can work in your environment.

**E.** State organizations may continue to use their current encryption software as long as it meets the standards outlined by the State and it meets industry requirements for security, privacy and password protection. It must also be compatible with the State approved encryption methods. However, State organizations that do not currently have software and are not in compliance with all Federal Regulations and State Attorney General Rulings or opinions for the transmitting of personally identifiable State Employee information, will need to purchase a package that is from the list of State approved encryption methods.

## Encryption algorithms used during file transports

| Component | Rating | Comments |
|---|---|---|
| AES – 256 bit encryption | Standard | Appropriate for data classified as 'Top Secret' |
| AES – 128 bit encryption | Standard | |
| Triple DES | Disallowed | |
| DES | Disallowed | |
| | | |
| The above are minimum encryption levels accepted by the State of Delaware. Increasing the level of encryption is preferred as the level of data classification increases but can be limited by the systems resources. | | |

## File Transport

| Component | Rating | Comments |
|---|---|---|
| SSH-2 (SFTP, SCP) | Standard | It must conform to RFC 4251 – The Secure Shell (SSH) Protocol Architecture (see http://tools.ietf.org/html/rfc4251)<br>Configure all servers to accept SSH-2 |
| TLS (SSL) | Standard | It must conform to RFC 5246 – The Transport Layer Security (TLS) Protocol V 1.2 (see http://tools.ietf.org/html/rfc5246) |
| FTPS (Explicit Mode) | Standard | |
| FTP | Disallowed | |
| FTP/PGP | Disallowed | |
| SSH-1 | Disallowed | Configure all servers to accept SSH-2 |