Standard ID:	**SE-ESI-001**
Title:	**Electronic Signature**
Domain:	**Security**
Discipline:	**Physical Network**
Revision Date: Revision no.: Original date:	**12/31/2015** **4** **1/01/2005**

I. Authority, Applicability and Purpose

A) **Authority:** Title 29, Chapter 90C provides broad statutory authority to the Department of Technology and Information to implement statewide and inter-agency technology solutions, policy, standards and guidelines for the State of Delaware's technology infrastructure. "Technology" means computing and telecommunications systems, their supporting infrastructure and interconnectivity used to acquire, transport, process, analyze, store and disseminate information or data electronically. The term "technology" includes systems and equipment associated with e-government and Internet initiatives.

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:** In light of State and Federal regulations, a need exists to establish the State's technologies for electronic signatures. This standard covers the levels of security technologies to be used for electronic signatures. The approach for this standard was heavily borrowed from the State of Arizona.

II. Scope

A. **State of Delaware:** The need for electronic signatures may be required by Federal regulations such as HIPAA (Health Insurance Portability and Accountability Act of 1996), Sarbanes-Oxley, Gramm-Leach-Bliley and others. This standard will cover all State organizations and transactions requiring the extra security of electronic signatures as specified by Agency Policy.

B. Areas Covered: This standard covers Email, Instant Messaging, Cloud Computing, Web Site Forms, Electronic Data Interchange (EDI), Electronic Agents, Credit Card Payments, official documents and Online Agreements.

C. Environments: This standard covers all State of Delaware employees, contractors, agents, and external businesses, Governments, and Citizens doing business with the State.

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 regularly reviewed. 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

1. **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]

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

2. **Electronic Signatures:** A traceable e-mail or a biometric identifier applied to a message. The identifier may be based on digitized handwriting or another biometric feature (such as a fingerprint). The electronic signature cannot be removed and applied to other documents to forge a signature.[2]

3. **Secure:** means ensuring that only the intended recipients can read the message, and also guaranteeing that it was not intercepted, or modified, and that it was delivered. This requires that email be protected, controlled, tracked and recallable.

4. **PKC** (**Public Key Cryptography):** Public-key cryptosystems have two primary uses, encryption and digital signatures. In a system, each person gets a pair of keys, one called the public key and the other called the private key. The public key is published, while the private key is kept secret. The need for the sender and receiver to share secret information is eliminated; all communications involve only public keys, and no private key is ever transmitted. In a public-key cryptosystem, the private key is always linked mathematically to the public key. Therefore, it is always possible to attack a public-key system by deriving the private key from the public key. Typically, the defense against this is to make the problem of deriving the private key from the public key as difficult as possible. For instance, some public-key cryptosystems are designed such that deriving the private key from the public key requires the attacker to factor a large number, it this case it is computationally infeasible to perform the derivation.[3]

5. **False Messages:** It is very easy to construct messages that appear to be from someone other than who they are actually from. Many viruses use this facility to propagate themselves. In general, there is no way to be sure that the apparent sender of a message actually sent the message - it could just as easily be fabricated.

6. **Message Replay:** Just as a message can be modified, messages can be saved, modified, and re-sent later. This could result in getting multiple messages and thus taking actions that were not requested.

7. **Repudiation:** Because email messages can be forged, there is no way to prove that someone sent a particular message. This means that even if someone did send a message, they can successfully deny it. This has implications with regards to using email for contracts, business communications, electronic commerce, etc.

8. **Non-Repudiation:** A process and use of technologies that ensure the following:

   a) The data (message, document, file, etc) that was sent is the same data that was received.

   b) The person who sent the message has been identified and can be directly tied to the data.

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

[3] http://www.rsasecurity.com/

9. **Symmetric Key Encryption:** In symmetric key encryption, the sender and receiver share a "secret" key. Using this key, a message can be encrypted into "cyphertext". Cyphertext looks like a random sequence of characters and is completely meaningless to anyone unless they also have the secret key, in which case they can decrypt the cyphertext back into the original message and read it.

   Using symmetric key encryption, eavesdropping and unwanted backups of messages no longer are a problem (unless the eavesdropper knows what the secret key is). It also becomes harder for someone to modify messages 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. Unless you meet in person, how do you communicate this key in a way that is secure? What if you want to send a secure message to someone on the other side of the world? How do you get them the secret key quickly in a way that eavesdroppers can't detect?

10. **Asymmetric Key Encryption:** In asymmetric key encryption, also known as "public key" encryption, each person has two keys. Any cyphertext created using one of the keys can only be decrypted using the other key. For example, keys "K1" and "K2". If you encrypt your message with K1, then only K2 can be used to decrypt it. Similarly, if you encrypt using K2, only K1 can be used to decrypt it. 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.

    Asymmetric key encryption allows you to do many things:

    a) **Send an Encrypted Message:** To send a secure message to someone, encrypt it with their public key. In this way, only the intended recipient, who has the respective private key, should ever be able to decrypt and read the message. This solves the problem of eavesdropping and the problem of communicating secret keys that is inherent in symmetric encryption.

    b) **Prove You Sent A Message:** To prove to someone that you sent a message, encrypt the message (or just a piece of it) with your private key. Then, anyone can decrypt it with your public key and read the contents. The fact that your public key decrypts the message proves that you sent it -- you cannot deny this fact.

    c) **Sign a Message:** A message signature proves that you sent the message AND allows the recipient to determine if the message was altered in transit. This is done by encrypting a digest of the message using your private key. The recipient can decrypt this and compare it to a digest of the message actually received. If they match, then the message is unaltered and was sent by you.

d) **Encrypted, Signed Messages:** The most secure form of communication is to first add a signature to the message and then to encrypt the message plus signature with the recipient's public key. This combines all of the benefits of all of the techniques: security against eavesdropping and unexpected storage, proof of sender, and proof on message integrity.

11. **Desktop to Desktop / Gateway to Gateway:** With desktop to desktop encryption, the message is encrypted at the originating desktop and is decrypted at the destination desktop(s). With gateway to gateway, the message travels through the enterprise as un-encrypted and is only encrypted at the gateway. If the message is from one State entity to another (as is usually the case) the message will never hit a gateway and will never be encrypted, even though it should have been.
12. **Gateway:** An email device that is used to virus check, content filter and perform administrative functions such as forwarding, ensuring delivery, etc.
13. **Push:** Sending a message to multiple recipients, for example, pay advices.
14. **Pull:** Each node requests its message from a server, a technique usually used to keep software updated.
15. **Sender control**: Be able to expire the message before or after it is read so that it can no longer be read by the recipient(s).
16. **LDAP (Lightweight Directory Access Protocol):** A server-to-server interface for directory information exchange among directories, devised as a low-cost, simpler implementation of the X.500 Directory Access Protocol. It facilitates the implementation of replication and chaining among dissimilar directories. Proposed by the University of Michigan, it was adopted by Netscape in 1996 for directory lookup, and has become the preferred access path for looking up directory information not only in X.500 directories, but also in many other directory structures on the Internet.[4]
17. **Kerberos:** An authentication system used for dial-up, remote or Internet connections. An Internet Engineering Task Force standard, Kerberos works by having a central server grant a "ticket" honored by all networked nodes running Kerberos.[5]

B. Declarations

1. Electronic Signatures:
   a) Must comply with State of Delaware code such as Title 6.
   b) Must comply with Federal regulations such as HIPAA, Sarbanes-Oxley, Gramm-Leach-Bliley and others.
   c) Must be accessible by the Internet for external customers.

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

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

d) Must provide automatic key management at the server level.

e) Must have an audit trail capability.

f) Must provide sender control. (Must be able to revoke an offer or acceptance before agreement).

g) Must support desktop to desktop and gateway communication.

h) Must utilize push technology and not pull.

i) Must run on all standard desktop operating systems.

j) Must be Server Based, and centrally managed.

k) Must be LDAP / KERBEROS integrated.

l) All State Agencies, the Courts, Legislature and K-12 are included

m) Must support standard State email package(s) when applicable.

n) Must consider whether non-repudiation is a requirement. If non-repudiation is required, then the project team and sponsor need to determine the appropriate level of technology that must applied to their situation.

o) Must be enabled in all cloud computing service environment(s) used by the State. The use of electronic signatures will depend upon the requirements.

2. Digital Signatures in addition to the above:

a) Must be X.509 certificate compatible.

b) Must be asymmetric.

c) Must provide central Key Management.

V. Definition 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 5+ 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.	These components must be explicitly approved by DTI for **new projects**. They can be used for **minor enhancement** and **system maintenance** without explicit DTI approval.
• **DISALLOWED** – DTI declares the component to be unacceptable for use and will actively intervene to disallow its use when discovered.	

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

#	Risk	Rating	Identification*	Verification	Data Classification
1	**High**	Standard	Prior Letter of Trust	Possession of PKI key or Token	Top Secret, Secret, Confidential or Public is acceptable.
2	**Medium**	Standard	Username	Password	Secret, Confidential and Public is acceptable. Top Secret is not acceptable.
3	**Low**	Standard	Knowledge of User data (for example name)	Data or Document	Public is acceptable Confidential, Secret or Top Secret is not acceptable

* Security begins with adequately identifying the parties prior to establishing trust. The process, and procedure for issuing logon ID's and Certificates of Trust must be managed properly.

Available tools and technologies to assist with electronic signatures

- The State's secure email solution
- The use of digital signatures for emails within the State
- The use of tokens such as Entrust
- The use of digital signatures within pdf documents and InfoPath forms

.