Digital Signature Acceptance Policy

Created by or for the SANS Institute. Feel free to modify or use for your organization. If you have a policy to contribute, please send e-mail to stephen@sans.edu

1.0 Purpose

The purpose of this policy is to provide guidance on when digital signatures are considered accepted means of validating the identity of a signer in <Company Name> electronic documents and correspondence, and thus a substitute for traditional "wet" signatures, within the organization. Because communication has become primarily electronic, the goal is to reduce confusion about when a digital signature is trusted.

2.0 Scope

This policy applies to all <Company Name> employees, contractors, and other agents conducting <Company Name> business with a <Company Name>-provided digital key pair. This policy applies only to intra-organization digitally signed documents and correspondence and not to electronic materials sent to or received from non-<Company Name> affiliated persons or organizations.

3.0 Policy

3.1 General Policy Statement

A digital signature is an acceptable substitute for a wet signature on any intra-organization document or correspondence, with the exception of those noted on the site of the Chief Financial Officer (CFO) on the organization's intranet: <CFO's Office URL>

The CFO's office will maintain an organization-wide list of the types of documents and correspondence that are not covered by this policy.

Digital signatures must apply to individuals only. Digital signatures for roles, positions, or titles (e.g. the CFO) are not considered valid.

3.2 Responsibilities

Digital signature acceptance requires specific action on both the part of the employee signing the document or correspondence (hereafter the *signer*), and the employee receiving/reading the document or correspondence (hereafter the *recipient*).

3.2.1 Signer Responsibilities

a. Signers must obtain a signing key pair from <Company's identity management group>. This key pair will be generated using <Company Name>'s Public Key Infrastructure (PKI) and the public key will be signed by the <Company Name>'s Certificate Authority (CA), <CA Name>.
b. Signers must sign documents and correspondence using software approved by <Company's IT organization>.
c. Signers must protect their private key and keep it secret.
d. If a signer believes that the signer's private key was stolen or otherwise compromised, the signer must contact <Company's identity management group> immediately to have the signer's digital key pair revoked.

3.2.2 Recipient Responsibilities

a. Recipients must read documents and correspondence using software approved by <Company's IT department>.

b. Recipients must verify that the signer's public key was signed by the <Company Name>'s Certificate Authority (CA), <CA Name>, by viewing the details about the signed key using the software they are using to read the document or correspondence.
c. If the signer's digital signature does not appear valid, the recipient must not trust the source of the document or correspondence.
d. If a recipient believes that a digital signature has been abused, the recipient must report the recipient's concern to <Company's identity management group> immediately.

4.0 References

<Note that these references were used only as guidance in the creation of this policy template. We highly recommend that you consult with your organization's legal counsel, since there may be federal, state, or local regulations to which you must comply. Any other PKI-related policies your organization has may also be cited here.>

American Bar Association (ABA) Digital Signature Guidelines
http://www.abanet.org/scitech/ec/isc/dsgfree.html

Texas Administrative Code (TAC) §203: Management of Electronic Transactions and Signed Records.
http://www.dir.state.tx.us/standards/S203.htm

Texas DIR Standards Review and Recommendation Publication (SRRPUB) 13: Digital Signatures & Public Key Infrastructure (PKI) Guidelines. http://www.dir.state.tx.us/standards/srrpub13.htm

Minnesota State Agency Digital Signature Implementation and Use.
http://www.state.mn.us/portal/mn/jsp/content.do?id=-536891917&subchannel=-536891918&sc2=null&sc3=null&contentid=536911215&contenttype=EDITORIAL&programid=536911146&agency=OETweb

Minnesota Electronic Authentication Act.
https://www.revisor.leg.state.mn.us/statutes/?id=325K&view=chapter - stat.325K.001

City of Albuquerque E-Mail Encryption / Digital Signature Policy.
http://mesa.cabq.gov/policy.nsf/WebApprovedX/4D4D4667D0A7953A87256E7B004F6720?OpenDocument

West Virginia Code §39A-3-2: Acceptance of electronic signature by governmental entities in satisfaction of signature requirement. http://law.justia.com/westvirginia/codes/39a/wvc39a-3-2.html

5.0 Enforcement

Any employee found to have violated this policy is subject to disciplinary action including, without limitation, termination.

6.0 Definitions

Certificate Authority (CA). An entity trusted by all parties in a transaction that is used to verify the identities of those parties by signing the public key for each of those parties.

Digital Key Pair. A private key and its corresponding public key. The private key is used to create the digital signature, and the public key is used to verify that its corresponding private key created the digital signature.

Digital Signature. An electronic identifier created with a signer's private key that allows the recipient to determine whether or not the identifier was created by the signer's private key, and whether the initial signed message has been altered.

Public Key Infrastructure (PKI). PKI is the collection of systems and applications that comprise an organization's ability to issue digital key pairs.

Wet Signature. An original written identifier or mark manually placed on a physical page; a traditional signature.

7.0 Revision History
9/15/2009 – Version 1.0, Charlie Scott