Digital Signature Acceptance Policy

Free Use Disclaimer: *This policy was created by or for the SANS Institute for the Internet community. All or parts of this policy can be freely used for your organization. There is no prior approval required. If you would like to contribute a new policy or updated version of this policy, please send email to policy-resources@sans.org.*

Things to Consider: *Please consult the Things to Consider FAQ for additional guidelines and suggestions for personalizing the SANS policies for your organization.*

Last Update Status: *Updated June 2014*

1. Overview

See Purpose.

2. 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.

3. Scope

This policy applies to all <Company Name> employees and affiliates.

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.

4. Policy

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.

4.1 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*).

4.2 Signer Responsibilities

4.2.1 Signers must obtain a signing key pair from <Company Name 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>.

4.2.2 Signers must sign documents and correspondence using software approved by <Company Name> IT organization.

4.2.3 Signers must protect their private key and keep it secret.

4.2.4 If a signer believes that the signer's private key was stolen or otherwise compromised, the signer must contact <Company Name> Identity Management Group immediately to have the signer's digital key pair revoked.

4.3 Recipient Responsibilities

4.3.1 Recipients must read documents and correspondence using software approved by <Company Name> IT department.

4.3.2 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.

4.3.3 If the signer's digital signature does not appear valid, the recipient must not trust the source of the document or correspondence.

4.3.4 If a recipient believes that a digital signature has been abused, the recipient must report the recipient's concern to <Company Name> Identity Management Group.

5. Policy Compliance

5.1 Compliance Measurement

The Infosec team will verify compliance to this policy through various methods, including but not limited to, business tool reports, internal and external audits, and feedback to the policy owner.

5.2 Exceptions

Any exception to the policy must be approved by the Infosec team in advance.

5.3 Non-Compliance

An employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

6 Related Standards, Policies and Processes

None.

7 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

Minnesota State Agency Digital Signature Implementation and Use
http://mn.gov/oet/policies-and-standards/business/policy-pages/standard_digital_signature.jsp

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

8 Definitions and Terms

None.

9 Revision History

Date of Change	Responsible	Summary of Change
June 2014	SANS Policy Team	Updated and converted to new format.