

IT107  
Encryption Policy

|  |  |
| --- | --- |
| Status | Final |
| Version | 1.11 |
| Classification | Confidential |
| Owner | Razvan Anghelidi, Directory of IT |
| Address | 1705 Tech Avenue, Unit 3, Mississauga, ON, L4W 0A2, Canada |

*Statement of Confidentiality: This document and supporting materials contain confidential and proprietary business information of Signifi Solutions Inc. These materials may be printed or photocopied for use internally and must not be shared with other parties.*

[Document Control iii](#_Toc25265011)

[Introduction 4](#_Toc25265012)

[Purpose 4](#_Toc25265013)

[Audience 4](#_Toc25265014)

[Scope 5](#_Toc25265015)

[Policy Statement 5](#_Toc25265016)

[Enforcement 14](#_Toc25265017)

[Revision History 14](#_Toc25265018)

All rights reserved

No part of this document may be reproduced in any form, including photocopying or transmission electronically to any computer, without prior written consent of Signifi Solutions Inc (from now on, Signifi). The information contained in this document is proprietary to Signifi and may not be used or disclosed except as expressly authorized in writing by Signifi.

Trademarks

Other product names mentioned in this document may be trademarks or registered trademarks of their respective companies and are hereby acknowledged.

Document Control

The electronic version of this document is recognized as the only valid version.

Approval History

|  |  |  |
| --- | --- | --- |
| APPROVER(S) | TITLE/DEPARTMENT | APPROVED DATE |
| Shamira Jaffer | CEO | December 23rd, 2021 |
| Shamira Jaffer | CEO | December 7th, 2020 |
| Shamira Jaffer | CEO | December 19th, 2019 |
|  |  |  |

Document Sensitivity Level

Confidential

Introduction

Overview

Encryption is the process of converting a plaintext message into a secure-coded form of text, call cipher text, which cannot be understood without converting back, via decryption (the reverse process), to plaintext. This is done via a mathematical function and a special encryption/description process.

Encryption is generally used to:

* Protect data in transit over networks from unauthorized interception and manipulation.
* Protect information stored on computers from unauthorized viewing and manipulation.
* Deter inadvertent and intentional alteration or disclosure of data; and Verify authenticity of a transaction or document.

Purpose

The purpose of this policy is to provide direction on effective use of encryption. It addresses the Signifi approved cryptographic algorithms, and relative key length/strength.

Audience

This policy applies to all Signifi employees, associates, part-time and temporary workers, trainees, contractors, and vendors.

Scope

This policy is to set the criteria for the creation of strong passwords, the protection of those passwords, and the frequency of change. The combination of a User ID and Password provides authenticated access to Signifi systems and services. In some cases, additional authentication factors, such as RSA Tokens, are also used but are beyond the scope for this policy.

Policy Statement

1. General
   1. Cryptographic controls must be considered to protect Highly Confidential or Confidential information from unauthorized viewing or tampering.
   2. Encryption algorithms and cryptosystems used must be well accepted in the industry for a sustained period of time. Proven, standard algorithms such as, Blowfish, RSA, and AES should be used as the basis for encryption technologies.
   3. Cryptographic algorithms shall be sourced from recognized and established security technologies. The type, strength and quality of the encryption algorithm must be based on the required level of protection needed for the information being encrypted. Consult with the Signifi Information Security team if in doubt of the cryptographic algorithm’s strength.
   4. There are two types of cryptographic systems: the symmetric and the asymmetric key systems. Symmetric key systems use single, secret, bidirectional (encrypt/decrypt), complementary keys, one of which is usually secret and the other publicly known.
   5. Symmetric cryptosystem key lengths must be at least 128 bits and asymmetric crypto-system keys must be at least 2048-bit key length where supported.
   6. Cryptographic keys shall be protected from modification, destruction and unauthorized disclosure during the life cycle of the key (generation, distribution, archiving, updating, revocation and destruction):
      * Only authorized Information Technology (IT) personnel will have access to cryptographic keys. Access to cryptographic keys must be based on ‘Need-to-Know’ criteria.
      * Cryptographic key management activities must be logged.
      * All use of encryption technology must be managed in a manner that permits properly designated Signifi IT staff prompt access to all data, for purposes of investigation and business continuity; and
      * Encryption processes must be highly automated and integrated in the infrastructure whenever possible.

The following is a list of cipher suites, their recommended usage, and their relative minimum strength:

|  |  |  |
| --- | --- | --- |
| Recommended Use | Cipher Suites | Server Certificate |
| Highest Security | Encryption: Advanced Encryption Standard (AES) 128-bit or RSA-3072 or higher encryption.  HMAC: Secure Hash Algorithm 2 (SHA-256)  Authentication: Digital Signature Standard (DSS) or RSA | DSS or RSA with a key size of 2048 bits or higher, and/or SHA-256 hash function. Note that use of SHA-256 in certificates may cause incompatibilities with older clients. |
| Security and  Performance | Encryption: AES 128-bit encryption  HMAC: SHA-2  Authentication: DSS or RSA | DSS or RSA with a key size of 2048 bits or higher and SHA-2 |
| Security and Compatibility | Encryption: AES 128-bit encryption or RSA-3072 or higher encryption.  HMAC: SHA-2  Authentication: DSS or RSA | DSS or RSA with a key size of 1024 bits (only to be used when incompatibility with 2048-bit key is observed) or higher and  SHA-2. |
| Authentication and Tamper Detection | HMAC: SHA-2  Authentication: DSS or RSA | DSS or RSA with a key size of 1024 bits (only to be used when incompatibility with 2048-bit key is observed) or higher and  SHA-2. |

|  |  |  |  |
| --- | --- | --- | --- |
| Algorithm | Minimum Key Length | Appropriate Usage | |
| **Symmetric Key Algorithms** | | | |
| AES | 128-bits | Data encryption:   * Session * Storage   + Backup   + Archival | Key encryption:   * Session * Storage   + Backup   + Archival |
| Skipjack | 80-bits, with 32 iterations | Data encryption:   * Session * Storage   + Backup   + Archival, < 5 years | |
| Triple DES | 112-bits | Data encryption:   * Session * Storage * Backup * Archival | Key encryption:   * Session * Storage   + Backup   + Archival |
| **Asymmetric Key Algorithms** | | | |
| Elliptic Curve | 160-bits | Data encryption:   * Session * Storage * Backup * Archival   Digital Signature | Key encryption:   * Session * Storage * Backup * Archival   Session key establishment |
| RSA | 2048-bits | Data encryption:   * Session * Storage * Backup * Archival   Digital Signature | Key encryption:   * Session * Storage * Backup * Archival   Session key establishment |
| **MACs and Hashes** | | | |
| AES MAC | 128-bits | Message authentication | |
| MD5[[1]](#footnote-1) | 128-bits, with 16 iterations | Message authentication and message digest | |
| SHA-1[[2]](#footnote-2) | Not applicable. | Message authentication and message digest | |
| SHA-2 | Not applicable | Message authentication and message digest | |
| TDES (Triple DES) MAC | 112-bits | Message authentication | |
| **Digital Signatures** | | | |
| DSA (Digital Signature Algorithm) | 1024-bits | Digital Signature | |
| Elliptic Curve DSA | 160-bits | Digital Signature | |
| RSA DSA | 2048-bits | Digital Signature | |
| **Digital Certificates** | | | |
| X.509 v3 compliant | N/A | Binds a public key with a specific identity. | |
| **Key Transport/Agreement Algorithms** | | | |
| Diffie-Hellman | 1024-bits | Digital Session key establishment | |
| Elliptic Curve Diffie-Hellman | 160-bits | Digital Session key establishment | |
| **Cryptographic Protocols** | | | |
| TLS 1.2 and higher | N/A | Protocol to authenticate and encrypt communication between authenticated parties. | |

* 1. An SSL Certificate associates an entity (person, organization, host, etc.) with a Public Key. In an SSL connection the client authenticates the remote server using the server’s certificate and extracts the Public Key in the certificate to establish the secure connection.
  2. The client can trust that the server certificate belongs to the server only if it is signed by a mutually trusted third-party Certificate Authority (CA). Certificates must be issued for a period of 3 years as applicable. Self-signed certificates should be created for testing purposes only. These should not be used on and any production or critical servers. All Signifi public facing servers requiring an SSL certificate must have a certificate from a trusted third-party certificate authority (CA) or a trusted internal CA.
  3. Ensure that all digital certificates are revocable with a cryptographically secured certificate revocation list (CRL) system.
  4. Ensure that a digital certificate is only trusted once it has been cryptographically validated and does not appear on a trusted CRL.
  5. Protect cryptographic keys for endpoints against unauthorized access (in the case of secret and private keys), modification, loss, and accidental or intentional destruction.
  6. Ensure that equipment used to generate, load, store and archive cryptographic keys for endpoints are physically protected against unauthorized access or modification.
  7. Ensure process for managing cryptographic keys for endpoints exists, which covers:
     + The secure generation, distribution, loading, storage, recovery, replacement, revocation and destruction of cryptographic keys, and
     + The secure back-up and archive of cryptographic keys.
  8. Maintain an inventory of their cryptographic keys and key components associated with endpoints. The inventory should contain the following:
     + Key name and purpose/usage
     + Key type
     + Key generation date
     + Component number, including the total number of components
     + Storage location(s)
     + All key custodians since generation, including the dates of custodial changes, and
     + Date the key was destroyed, and proof of destruction.
  9. Review the inventory of keys associated with endpoints annually.
  10. Only use cryptographic keys on endpoints for a single intended purpose and must never share these keys between production and non-production environments.
  11. A certificate key lifespan must be no longer than 7 years.
  12. Replace uncompromised key used endpoints on or before its stipulated lifespan.
  13. Ensure that key custodians understand their responsibility to never disclose the key or key component in their custody to anyone, not even to a manager or an auditor, except to another authorize key custodian for that specific key or key component.
  14. Ensure that cryptographic solutions on endpoints fail close (i.e., access is denied if a failure occurs).

1. Data Transmission
   1. When Highly Confidential, Confidential and Internal information is transmitted over unprotected networks such as the Internet, the information must be encrypted at all times.
   2. Secure protocols such as SSH v2. IPsec v2, TLS v1.2 are appropriate and acceptable to transmit sensitive data.
   3. Signifi managed wireless access points must require encryption along with the ability to recognize rogue wireless devices.
   4. All remote and administrative access must be encrypted. Network level encryption protocols such as SSH v2, IPsec v2, or TLS v1.2, must be used to protect the User ID, password and traffic from eavesdropping. Other approved encryption technologies may also be used for the purposes of non-console remote administration tasks.
2. Data Storage
   1. Password authentication credentials must be encrypted when placed in persistent storage or transmitted across the network. Credentials must not be displayed in clear text.

**Payment Card Industry - PCI Cardholder Data Environments:**

* 1. Encrypt all non-console administrative access using strong cryptography. For web-based management and other non-console administrative access use SSH v2, IPsec v2, or TLS v1.2.
  2. Verify encryption keys were changed from vendor default settings at installation for wireless environments and are changed anytime anyone with knowledge of the keys leaves the company or changes positions.
  3. If disk encryption is used (rather than file or column-level database encryption), logical access must be managed independently of native operating system access control mechanisms (for example, by not using local User account databases). Decryption keys must not be tied to User accounts.
  4. Cardholder data on removable media must be encrypted wherever stored or rendered non readable through some other method.
  5. If Signifi Highly Confidential (i.e. credit card numbers, social security numbers and financial information, passwords) information must be sent by electronic communication systems (network) or stored, encryption or similar technologies to protect the data must be employed;
  6. The standard algorithm is Advance Encryption Standard (AES) with a minimum standard key strength of 128 bit. Other strong symmetric and asymmetric encryption algorithms are acceptable.
  7. Use strong cryptography and security protocols (for example, TLS, IPSEC, SSH, etc.) to safeguard sensitive cardholder data during transmission over open, public networks.
  8. Key management procedures exist for keys used for encryption of cardholder data.
  9. Access to cryptographic keys must be restricted to the fewest number of custodians necessary; and
  10. Keys should be stored in encrypted format and key-encrypting keys must be stored separately from data-encrypting keys.

Enforcement

Signifi may monitor applications/systems, devices, and network traffic at any time to ensure compliance with this policy. All instances of non-compliance will be reviewed by the department director.

The department director, with the assistance of the Human Resources department has the authority to impose disciplinary actions, up to and including termination of employment or contractual agreement.

Update

This policy and all supporting documentation will be reviewed and updated annually or upon material changes to Signifi business rules, technology processes, organizational goals, or information security objectives to ensure its continuing suitability, adequacy, and effectiveness.

Revision History

|  |  |  |  |
| --- | --- | --- | --- |
| VERSION | DATE | SUMMARY OF CHANGE | CHANGED BY |
| 1.0 | 2019-12-05 | First version | Darace Rose |
| 1.1 | 2019-12-17 | Update template | Razvan Anghelidi |
| 1.11 | 2020-12-01 | Annual review | Razvan Anghelidi |
| 1.12 | 2021-12-12 | Annual review | Hadeel Alzuhairi |

1. All *new* implementations of MACs and hashes must not be based on MD5. [↑](#footnote-ref-1)
2. All *new* implementations of MACs and hashes must not be based on SHA-1. [↑](#footnote-ref-2)