Encryption Policy

BritePool

January 2020

Contents

Table 1: Control satisfaction

Standard	Controls Satisfied
TSC	CC9.9

Table 2: Document history

Date	Comment
Jan 2 2020	Initial document

1 Purpose and Scope

a. This policy defines organizational requirements for the use of cryptographic controls, as well as the requirements for cryptographic keys, in order to protect the confidentiality, integrity, authenticity and nonrepudiation of information.

b. This policy applies to all systems, equipment, facilities and information within the scope of the organization's information security program.

c. All employees, contractors, part-time and temporary workers, service providers, and those employed by others to perform work on behalf of the organization having to do with cryptographic systems, algorithms, or keying material are subject to this policy and must comply with it.

2 Background

a. This policy defines the high level objectives and implementation instructions for the organization's use of cryptographic algorithms and keys. It is vital that the organization adopt a standard approach to cryptographic controls across all work centers in order to ensure end-to-end security, while also promoting interoperability. This document defines the specific algorithms approved for use, requirements for key management and protection, and requirements for using cryptography in cloud environments.

3 Policy

a. The organization must protect individual systems or information by means of minimal cryptographic controls as defined in Table 3:

Name of System/ Type of Information	**Cryptographic Tool**	**Encryption Algorithm**	**Key Size**
Public Key Infrastructure for Authentication	OpenSSL	AES-256	256-bit key
Data Encryption Keys	OpenSSL	AES-256	256-bit key
Virtual Private Network (VPN) keys	OpenSSL and OpenVPN	AES-256	256-bit key
Website SSL Certificate	OpenSSL, CERT	AES-256	256-bit key

Table 3: Cryptographic Controls

a. Except where otherwise stated, keys must be managed by their owners.

b. Cryptographic keys must be protected against loss, change or destruction by applying appropriate access control mechanisms to prevent unauthorized use and backing up keys on a regular basis.

c. When required, customers of the organization's cloud-based software or platform offering must be able to obtain information regarding:

   i. The cryptographic tools used to protect their information.

   ii. Any capabilities that are available to allow cloud service customers to apply their own cryptographic solutions.

   iii. The identity of the countries where the cryptographic tools are used to store or transfer cloud service customers' data.

d. The use of organizationally-approved encryption must be governed in accordance with the laws of the country, region, or other regulating entity in which users perform their work. Encryption must not be used to violate any laws or regulations including import/export restrictions. The encryption used by the Company conforms to international standards and U.S. import/export requirements, and thus can be used across international boundaries for business purposes.

e. All key management must be performed using software that automatically manages access control, secure storage, backup and rotation of keys. Key management should adhere to the "Recommendation for Key Management - Best Practices for Key Management Organizations" NIST SP 800-57 Part

2 or the lastest superseding standard. Some important points from the policy:

f. The key management service must provide key access to specifically-designated users, with the ability to encrypt/decrypt information and generate data encryption keys.

g. The key management service must provide key administration access to specifically-designated users, with the ability to create, schedule delete, enable/disable rotation, and set usage policies for keys.

h. The key management service must store and backup keys for the entirety of their operational lifetime.

i. The key management service must rotate keys at least once every 12 months.

j. Refer to the latest version of the standard

k. All non public data should be transmitted through the use of an appropriately configured Transport Layer Security (TLS) implementation as defined in the "Guidelines for the Selection, Configuration, and Use of Transport Layer Security (TLS) Implementations" NIST SP 800-52 or the lastest superseding standard.

l. Ciphers that are proven, standard, highly tested, and free of patent encumbrances must be used as the basis for encrypting devices and communications. They must meet the requirements delineated in the National Institute of Standards and Technology (NIST) publication FIPS 140-2. Currently AES is highly recommended at this time, but refer to the latest version of the standard to verify. The use of proprietary ciphers is not allowed for any purpose.

m. Hash functions should meet or exceed the requirements set forth in "Guidance for Cryptographic Algorithm and Key-Size Selection" in NIST SP 800-57 Part 1. SHA-3 should be preferred, but SHA-2 is also acceptable, but refer to the latest standard. Key lengths should meet or exceed those deemed "Acceptable" in "Transitioning the Use of Cryptographic Algorithms and Key Lengths" NIST SP 800-131A or the latest superseding standard.

n. Key Agreement and Authentication

o. Key exchange must use one of the following protocols: Diffie-Hellman (including ECDH), or Internet Key Exchange (IKE), version 2.

p. Public keys used to establish trust must be verified (either manually or through a cryptographically signed message) prior to use.

q. Any server used for authentication must have a valid certificate signed by a trusted provider. All applications or servers using SSL or TLS must have

a valid certificate signed by a trusted provider. Use of ephemeral keys is not adequate for this purpose.