KSL Cryptographic Standard

Classification	INTERNAL
Document Reference	ITS0101
Document Version	1.0
Document Status	Final

Revision History

Version	Date	Change Number	Summary of Changes
1.0	19 Jun 2023	NA	First copy

Document Review

Date of Next Scheduled Review
1st Jun 2024

Authors

Name	Title
Ong Boon Hwee	Assistant Manager, IT Security
Foo Tze Uei	Manager, IT Governance, Risk, Compliance
Jonathan Ong	General Manager, Cyber Security

Contents

1. Objective

1.1 Introduction

KSL uses cryptography in its business applications to protect confidential and secret information from unauthorised disclosure (data privacy and data confidentiality), unauthorised modification (data authentication and data integrity), and even for non-repudiation (entity authentication).

1.2 Purpose

In today context, business risk drives the need for cryptographic solutions to establish and maintain sound security posture and practices. Use of inappropriate or out-dated cryptographic standard would be a threat to any application or software employing any form of cryptography solution, which unnecessarily increases the information security risk.

1.3 Background

Cryptography is a branch of mathematics based on the transformation of data into cipher text from plaintext and vice versa. It relies upon two basic components: an algorithm (or methodology) and a cryptographic key. The cryptographic key is the parameter used in the transformation.

This document describes:

- acceptable cryptographic algorithms and key strengths
- standards in deploying commonly used cryptographic solutions

2. Scope of Coverage & Applicability

All KSL systems/services/data regardless of hosted on-premises or private/public cloud that uses cryptography in its business applications should comply with this cryptographic management standard. Entities or business systems that are unable to fully adopt this standard should seek approval for IT technology deviations from IT GRC.

3. Target Audience

This document is intended for staff:

a. who deploy or implement cryptographic solutions in systems;

b. who evaluate, recommend and procure commercial cryptographic hardware/software;

c. who manage and update cryptographic (hardware/software) modules on a periodic basis.

4. Approved Cryptographic Algorithm/Function

S/N	Type	Approved Algorithm/Function	Exception / Limitation
4.1	Symmetric Key	The minimum key length for following approved symmetric algorithms should be: AES: 128-bit or higher; RC5: 128-bit. The recommended modes of operation for block ciphers are: Electronic Code Book (ECB); Cipher Block Chaining (CBC); Cipher Feedback Mode (CFB); Output Feedback Mode (OFB); Galois/Counter Mode (GCM); or Counter with CBC-MAC mode (CCM).	3DES: No applications should be using 3DES by end of 2023. It can only be allowed for compatibility or supportability reasons. A risk assessment shall be conducted and recorded in the risk register.
4.2	Asymmetric Key (including key establishment)	RSA: 2048-bit or above; DH: 2048-bit or above; ECDH: 224-bit or above;	Nil

4.3	Hash Function	The approved hash functions are SHA-2 (224, 256, 384, 512 bits), or stronger.	SHA-1 shall not be used for any new implementation for digital signing or within any internet facing system. Use of SHA-1 for other purposes is solely allowed for compatibility or supportability reasons. A risk assessment is to be conducted and recorded in the risk register.
4.4	Digital Signature	RSA: 2048-bit; DSA: 2048-bit ECDSA: 224-bit	For interoperability, digital signature implementation should adopt the PKCS #7 standards.
4.5	Message Authentication Code (MAC)	HMAC-MD5; HMAC-SHA1; or approved block cipher algorithms and hash functions.	MAC provides message origin authentication, not confidentiality. If confidentiality is required then the message shall require encryption. Eg OSPF authentication message-digest.
4.6	Random Number Generator	Approved Pseudorandom number generator (PRNG) algorithms are defined in FIPS 186-2, ANSI X.931 and ANSI X9.62.	Nil

5. Cryptographic Solutions

5.1 Network Security

1. IPSec is an approved protocol for encrypted network traffic. It should be used for securing data over insecure channels (including leased lines, MPLS, Metro-Ethernet and the Internet). E.g. VPN.

2. Internet Key Exchange version 2 (IKEv2) is the current supported protocol for IPSEC VPN tunnels.

3. Internet Key Exchange version 1 (IKEv1) had been deprecated. Use of IKEv1 is solely allowed for compatibility or supportability reasons. A risk assessment is required to be conducted and recorded in the risk register.

5.2 Transport/Session Layer Security

1. Transport Layer Security (TLS) version 1.2 or higher shall be used for new implementations after Oct 2023.
    i. TLS 1.0 and 1.1 can be used for compatibility or supportability reasons. Justification for compatibility or supportability reasons must be documented.
    ii. For TLS 1.0 and 1.1, a risk assessment is to be conducted and recorded in the risk register. The risk assessment should include the plan to migrate to an approved algorithm. Target date for migration should be before end Oct 2023.
    iii. Cipher suites that are composed entirely of the approved cryptographic algorithms mentioned in Section 4 above should be used. Specifically, only cipher suites that are listed in Appendix A-1 are allowed for TLS implementation.
    iv. Security Sockets Layer (SSL) 3.0 or earlier shall not be used.

5.3 External Certificate Authorities (CA)

1. The Certificate Authority (CA) Certificate Policy and Certificate Practice Statements (CPS) should conform to industry recommendation.

5.4 Secure Internet Electronic Mail

1. The two primary Secure Internet Electronic Mail implementations are based on OpenPGP and Secure Multipurpose Internet Mail Extensions (S/MIME) standards.

5.5 Cryptographic Implementations in Development Projects/UAT

1. Cryptographic APIs should confirm to the above approved cryptographic algorithms.

Appendix A-1 - Cipher Suites for TLS Implementation

Only cipher suites listed in the table below are allowed, they are grouped by certificate types and TLS protocol versions. Cipher suites with forward secrecy and GCM block cipher mode are recommended to be configured as higher priority.

S/N	Cipher Suite Name	Key Exchange	Encryption	Hash Function for HMAC	Hash Function for PRF
TLS 1.2 Cipher Suites for RSA Server Certificates					
1	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	ECDHE	AES_128_GCM	N/A	SHA-256
2	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256	ECDHE	AES_128_CBC	N/A	SHA-256
3	TLS_RSA_WITH_AES_256_GCM_SHA384	RSA	AES_256_GCM	N/A	SHA-384
4	TLS_RSA_WITH_AES_128_GCM_SHA256	RSA	AES_128_GCM	N/A	SHA-256
5	TLS_RSA_WITH_AES_256_CCM	RSA	AES_256_CCM	N/A	SHA-256
6	TLS_RSA_WITH_AES_128_CCM	RSA	AES_128_CCM	N/A	SHA-256
7	TLS_RSA_WITH_AES_256_CBC_SHA256	RSA	AES_256_CBC	SHA-256	SHA-256
8	TLS_RSA_WITH_AES_128_CBC_SHA256	RSA	AES_128_CBC	SHA-256	SHA-256
TLS 1.2 Cipher Suites for ECDSA Server Certificates					
1	TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384	ECDHE	AES_256_CBC	SHA-384	SHA-384
2	TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384	ECDHE	AES_256_GCM	N/A	SHA-384
3	TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256	ECDHE	AES_128_GCM	N/A	SHA-256
4	TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256	ECDHE	AES_128_CBC	SHA-256	SHA-256

This page is intentionally left blank