POLICY ON THE USE OF CRYPTOGRAPHIC CONTROLS

Code:	8A.10/ISO2700:2013/A10.1.1/A10.2/A18.1.5
Version:	v 1.11
Date of version:	11/09/2024
Created by:	Casey Eldib, James Paul & Brad Unal
Approved by:	Metin Unal
Confidentiality level:	Confidential

CHANGE HISTORY

Date	Version	Created by	Description of change
24/04/2017	1.0		Basic document outline
28/04/2017	1.2	Brian Grant	Vormetric cryptographic key and control details added
02/05/2017	1.3	James Paul	Reviewed
18/07/2017	1.4	James Paul	Updated
18/07/2018	1.5	Fiona Nicholls	Reviewed/updated
03/09/2019	1.6	Di Parker	Reviewed/updated
13/09/2020	1.7	Mark Needham	Reviewed/updated
09/09/2021	1.8	Mark Needham	Reviewed/updated
07/09/2022	1.9	Mark Needham	Reviewed/updated
11/09/2023	1.10	Mark Needham	Reviewed/updated
11/09/2024	1.11	Mark Needham	Reviewed/updated

TABLE OF CONTENTS

1. PURPOSE, SCOPE AND USERS

The purpose of this document is to define rules for the use of cryptographic controls, as well as the rules for the use of cryptographic keys, in order to protect the confidentiality, integrity, authenticity and non-repudiation of information.

Insufficient encryption or encryption key management can lead to compromise and disclosure of secure sensitive data. Employees of OracleCMS must be familiar with minimum standards for encryption, and the protection of encryption keys, in order to prevent unauthorised disclosure and subsequent fraudulent use. The Company's minimum standards limit the use of encryption to those algorithms that have received substantial public review, and have been proven to work effectively.

This policy applies to any encryption keys, and to the person responsible for any encryption key, including but not limited to:

● encryption keys issued by the OracleCMS

● encryption keys used for OracleCMS business

● encryption keys used to protect data owned by the OracleCMSThe public keys contained in digital certificates are specifically exempted from this policy.

This document is applied to the entire Information Security Management System (ISMS) scope, i.e. to al} systems and information used within the ISMS scope.

Users of this document are IT department of OracleCMS.

2. REFERENCE DOCUMENTS

- ISO/IEC 27001 standard, clauses A.IO.I.I, A.10.1.2, A.18.1,5
- Information Security Policy
- Information Classification Policy — separate policy document

3. Use of cryptography

3.1 Control Requirements

According to the Information Classification Policy, as well as legal and contractual obligations, the organization must protect individual systems or information by means of the following cryptographic controls:

Name of system / type of information	Cryptographic tool	Encryption algorithm	Key Size

Microsoft SQL Database Server - Oracle ESX14 - Oracle CMS	Vormetric Transparent Encryption (VT E) Ver 5.2	Symmetrical AES	256
Vormetric Data Security Manager	Proprietary internal Masker Key virtual HSM	Symmetrical AES	256

Owners of individual assets to which cryptographic controls are applied are responsible for appropriate application of individual cryptographic controls.

Chief Technology Officer is responsible for prescribing the following rules regarding key management

- generating private and public cryptographic keys
- activation and distribution of cryptographic keys defining the time limit for the use of keys and their regular updating (in accordance with risk assessment)
- archiving inactive keys which are necessary for encrypted electronic archives
- destruction of keys

Keys are managed by their owners in line with the abovementioned rules.

Cryptographic master keys will be protected in the Vormetric Data Security Manager (DSM) which is a FIPS 140-2 Level 1 compliant key policy and security management platform. Access to the environment will not allow access to the underlying keys, which are never exposed outside of the DSM.

Access to the DSM includes separation of duties whereby Blue Apache Managed Service Provider with SLA performs System Administration while security policy for key and encryption is configured and managed by CTO. Authentication for these roles is enforced through Oracle CMS' Active Directory.

Data Encryption key exchange between the DSM and the VT E agent is performed using ECC and data encryption keys are obfuscated in server memory when not in use to prevent exposure of the DE key.

Key material is securely backed with a wrapper key up on a weekly basis or when key rotation is applied and can only be recovered as required. Key recovery, using the wrapper key, requires not less than two custodians, preventing unauthorized recovery of key material by any one custodian,

On key rotation, historical keys are archived within the DSM and are also included in DSM key backup to assure archived key material can be applied/recovered for historical or archive encrypted data.

3.2 Encryption Algorithm Requirements

Ciphers in use must meet or exceed the set defined as "AES-compatible" or "partially AES-compatible" according to the IETF/IRTF Cipher Catalog, or the set defined for use in the United States National Institute of Standards and Technology (NIST) publication FIPS 140-2, or any superseding documents according to the date of implementation. The use of the Advanced Encryption Standard (AES) is strongly recommended for symmetric encryption.

Algorithms in use must meet the standards defined for use in NIST publication FIPS 140-2 or any superseding document, according to date of implementation. The use of the RSA and Elliptic Curve Cryptography (ECC) algorithms is strongly recommended for asymmetric encryption

3.3 Hash Function Requirements

OracleCMS Hash Functions must adhere to NIST framework requirements

3.4 Key Agreement and Authentication

● Key exchanges must use one of the following cryptographic protocols: Diffie-Hellman, IKE, or Elliptic curve Diffie-Hellman (ECDH).

● End points must be authenticated prior to the exchange or derivation of session keys.

● Public keys used to establish trust must be authenticated prior to use. Examples of authentication include transmission via cryptographically signed message or manual verification of the public key hash.

● All servers used for authentication (for example, RADIUS or TACACS) must have installed a valid certificate signed by a known trusted provider.

● All servers and applications using SSL or TLS must have the certificates signed by a known, trusted provider.

3.5 Key Generation

● Cryptographic keys must be generated and stored in a secure manner that prevents loss, theft, or compromise.

● Key generation must be seeded from an industry standard random number generator (RNG).

3.6 Secret Key Encryption Keys

Keys used for secret key encryption, also called symmetric cryptography, must be protected as they are distributed to all parties that will use them. During distribution, the symmetric encryption keys must be encrypted using a stronger algorithm with a key of the longest key length for that algorithm authorised in this Policy. If the keys are for the strongest algorithm, then the key must be split, each portion of the key encrypted with a different key that is the longest key length authorised and the each encrypted portion is transmitted using different transmission mechanisms. The goal is to provide more stringent protection to the key than the data that is encrypted with that encryption key.

Symmetric encryption keys, when at rest, must be protected with security measures at least as stringent as the measures used for distribution of that key.

3.7 Public Key Encryption Keys

Public key cryptography, or asymmetric cryptography, uses public-private key pairs. The public key is passed to the certificate authority to be included in the digital certificate issued to the end user. The digital certificate is available to everyone once it issued. The private key should only be available to the end user to whom the corresponding digital certificate is issued.

3.7.1 Company Public Key Infrastructure (PKI) Keys

The public-private key pairs used by OracleCMS' public key infrastructure (PKI) are generated on the Key Management Service to an individual end user. The private key associated with an end user's identity certificate, which are only used for digital signatures, will never leave the Key Management Service. The private key associated with any encryption certificates, which are used to encrypt email and other documents, must be escrowed in compliance with OracleCMS policies. Access to the private keys stored on OracleCMS issued Key Management Service will be protected by a username, password and 2 factor authentication known only to the individual to whom the access of the Key Management Service is issued.

3.7.2 Other Public Key Encryption Keys

Other types of keys may be generated in software on the end user's computer and can be stored as files on the hard drive or on a hardware token. If the keys are generated in software, the end user is required to create at least one backup of these keys and store any backup copies securely. The user is also required to create an escrow copy of any private keys used for encrypting data and deliver the escrow copy to the local Information Security representative for secure storage. All backups, including escrow copies, shall be protected with a password or passphrase that is compliant with OracleCMS Password Policy.

3.7.2 Commercial or Outside Public Key Infrastructure (PKI) keys

In working with business partners, the relationship may require the end users to use public-private key pairs that are generated in software on the end user's computer. In these cases, the public-private key pairs are stored in files on the hard drive of the end user. The private keys are only protected by the strength of the password or passphrase chosen by the end user. For example, when an end user requests a digital certificate from a commercial PKI, such as VeriSign or Thawte, the end user's web browser will generate the key pair and submit the public key as part of the certificate request to the CA. The private key remains in the browser's certificate store where the only protection is the password on the browser's certificate store. A web browser storing private keys will be configured to require the user to enter the certificate store password anytime a private key is accessed.

3.6 Hardware Token Storage

Hardware tokens storing encryption keys will be treated as sensitive company equipment, as described in the OracleCMS Acceptable Use Policy, when outside OracleCMSoffices. In addition, all hardware tokens, smartcards, USB tokens, etc., will not be stored or left connected to any end user's computer when not in use. For end users traveling with hardware tokens, they will not be stored or carried in the same container or bag as any computer.

3.6 Personal Identification Numbers (PINs), passwords and passphrases

All PINs, passwords or passphrases used to protect encryption keys must meet complexity and length requirements described in OracleCMS Password Policy

3.7 Loss and Theft

The loss, theft, or potential unauthorized disclosure of any encryption key covered by this policy must be reported immediately to a Director, who will direct the end user in any actions that will be required regarding revocation of certificates or public-private key pairs.

4. MANAGING RECORDS KEPT ON THE BASIS OF THIS DOCUMENT

Record name	Store location	Person responsible for storage	Controls for record protection	Time retention
Vormetric Data Security Manager Administration Guide (Key Management Administration)	OracleCMS-456 Spencer Street, VIC	CTO	VDS Guide is PDF read only and not modifiable. Guide is updated by Vormetric on release of new software versions.	Instructions that are no longer valid are stored for a period of 3 years

Only MD/CTO can grant other employees' access to the any of the abovementioned records.

5. VALIDITY AND DOCUMENT MANAGEMENT

This document is valid as of 11/09/2024

The owner of this document is CTO, who must check and, if necessary, update the document at least once every six months.

When evaluating the effectiveness and adequacy of this document, the following criteria must be considered:

- number of incidents related to loss, compromise or destruction of cryptographic keys
- number of systems to which cryptographic controls are applied contrary to this Policy

Managing Director

Metin Unal