ADIB –Standard

Security Certificates and Domain Lifecycle Management Standard

STD-ITD-571

Date: 30th November 2023
Version: 4.0

Version Control & Change Management

Version	Issue Date	Details of Change	Reason for change
4.0	November, 2023	Update Review & Monitoring section	Updated to align with the current practice
3.0	November, 2022	Added controls: - certificate validity shall not exceed 2 years - External certificates to be used for all public facing services.	Updated process to align with best practices
2.0	Publishing Date	Document reviewed. No change required.	Process annual review
1.0	Publishing Date	Document created	To provide controls SSL certificates and public domains

Prepared by	Approved by	Reviewed by
Governance Team	Head of IT Compliance and Security Architecture Head of Technology GRC	IT Governance Team

Document Contents

1. Overview

The objective of Security certificate and Domain Lifecycle Management Standard is to provide controls for all relevant stakeholders involved in assessment, acquisition, configuration & installation, review & monitoring of SSL certificates and domains.

2. Applicability

The SSL Certificate and Domain Lifecycle Management Standard is applicable to entire ADIB Technology and its subsidiaries.

3. Standard Owner

Security Certificate Lifecycle Management: Head of Technology GRC
Domain Management Lifecycle: Head of Technology GRC

4. Standard Statements and Description

4.1. Security Certificate Lifecycle Management

- Application owner identifies the requirement for Security certificate.
- Appropriate change request shall be raised and tracked.
- SSL certificate shall be obtained from Internal CA or trusted External CA
- SSL certificate shall be purchased based on the validity (Duration of Certificate) requirements requested by the business owners. The certificate validity shall not exceed 2 years.
- Application owners shall not use Wild Card certificates for public facing services.
- Based on application owner request, the Technology GRC shall review the requirement for the Security certificate and recommend whether SSL/Business user/Client/Internal certificate needs to be obtained
- Systems Team reviews and ensures chosen CA for SSL certificate/Business user/Client supports RSA/ECC encryption algorithms or any algorithm which allows 2048-bit key length.
- Systems Team reviews and ensures chosen CA for SSL certificate/Business user/Client supports minimum of SHA 2 hashing algorithms.
- External certificates to be used for all the public facing services.
- Internal certificate/Self signed can be obtained only for internal applications alone.
- Business user certificates can be initiated on a need basis.
- Application owner shall be responsible for the security of the private key associated with the SSL Certificates. In case, change of responsibilities or termination of employment, the application owner shall handover the private keys to his/her line Manager.
- During Certificate Signing Request (CSR) for purchase or renewal of SSL, the requestor should provide Licenses@adib.com as contact email rather than their personal or work email address.
- CSR file shall not be overwritten after generating a certificate reference number online.

4.2. Domain Lifecycle Management

- Application owner identifies the requirement for Domain registration.
- Appropriate change request shall be raised and tracked.
- Based on application owner request, Technology Compliance team shall review the requirement for domain registration
- Domain names should only be purchased from trusted domain and hosting providers.
- During purchase or renewal of domains, the requestor should provide Licenses@adib.ae as contact email rather than their personal or work email address.

4.3. Review and Monitoring

- SSL Certificates and Public Domain records shall be maintained by SecOps team to discover, monitor, and generate alerts before expiration using the certificate management tool.
- The application owner is responsible for taking required action upon receiving alerts.
- Alerts shall be created in certificate management tool at least once in a month before 3 months of SSL certificate and domain registration expiry date and twice in a week before 1 month of SSL certificate expiry date in the Certificate Management Tool

4.4. Definitions

- **SSL (Secure Sockets Layer)** is the standard security technology for establishing an encrypted link between a web server and a browser. This link ensures that all data passed between the web server and browsers remain private and integral. SSL is an industry standard and is used by millions of websites in the protection of their online transactions with their customers.
- **SSL Certificates** are required to create an SSL connection with a web server.
- **CSR (Certificate Signing Request)** is a small, encoded text file containing information about the organization and the domain you wish to secure. It is required for the activation of a digital SSL certificate and, as a rule, is generated on the server where the certificate is to be installed. A CSR is submitted to the Certificate Authority and used to generate the certificate.
- **Domain names** are used to identify one or more IP addresses.
- **Certification Authority (CA)** is an entity that issues digital certificates.

5. Exceptions

Any deviation to the standard shall be documented along-with associated risks and shall be approved by Head of Technology GRC.