Ref. RFQ No. EA/03-19-2026

Statement of Work (SOW)

Public SSL/TLS Certificate Procurement

1. Project Overview

The purpose of this RFP is to procure publicly trusted SSL/TLS certificates from an internationally recognized Certificate Authority (CA) to secure the organization's internet-facing systems, applications, APIs, and services. The selected vendor shall provide certificates, management support, validation services, and lifecycle assistance to ensure compliance with global security standards and best practices.

Scope of Work

The selected bidder shall provide the following:

1- The solution must support issuance of the certificate below but not limited to

- Extended Validation (EV) SSL Certificates
- Organization Validation (OV) SSL Certificates
- Domain Validation (DV) SSL Certificates
- Wildcard Certificates
- Multi-Domain / SAN Certificates
- Code Signing Certificates (optional if required)
- Client Authentication Certificates (optional if required)

2- The certificates must meet or exceed the following technical specifications:

Requirement	**Specification**
Encryption Strength	Minimum 256-bit encryption
Key Length	RSA 2048-bit minimum or ECC equivalent
Hash Algorithm	SHA-256 or stronger
Browser Compatibility	Compatible with all major browsers and OS platforms

Requirement	Specification
Root Trust	Must be trusted by Microsoft, Apple, Google, Mozilla root stores
SAN Support	Must support Subject Alternative Names
Wildcard Support	Must support subdomain wildcard issuance
API Access	REST API or automation interface for issuance and management
Revocation	CRL and OCSP support
Re-issuance	Unlimited re-issuance during certificate validity period
Validation Speed	Domain validation within minutes; OV/EV within defined SLA
Certificate Format	PEM, DER, PFX, CER, CRT support,
TLS Support	TLS 1.2 and TLS 1.3 compatibility
Support Etisalat Multiple Domain	Must support different domain name related to Etisalat organization
TLS/SSL Certificate Tools	Free Tools to be installed in End User PC for troubleshooting and validation of Certificates, repairing, changing the format and key password of the Certificate

3- The solution must offer centralized certificate management covering end-to-end certificate administration, including user management, lifecycle alerts and notifications, expiry reminders (minimum 30/15/7 days), revocation, automated renewal options, and an inventory reporting dashboard.

4- The CA must support the points below but limited to.

- Be compliant with CA/Browser Forum requirements
- Support Web Trust or equivalent compliance audit
- Maintain publicly trusted root certificates
- Provide incident response procedures for compromised certificates

- Provide Certificate Transparency (CT) log support

5- The solution provider must be an authorized reseller or the official CA provider
6- The solution provider must provide references from enterprise customers
7- The solution provider must demonstrate capability to support enterprise-scale deployments
8- The solution provider must provide proof of CA accreditation and trust chain

---

9- The solution provider should provide Support as per below Requirements.

- 24×7 technical support
- Dedicated account manager (preferred)
- SLA-based response times
- Implementation guidance and documentation
- Support for certificate installation and troubleshooting (remote)

10- Strong **and Modern TLS Security Requirements**
The solution must support current industry-standard TLS security, including TLS 1.2/1.3 only, modern cipher suites, and Perfect Forward Secrecy. Legacy and weak algorithms/ciphers must not be supported.

- Secure Key Management
Private keys must always remain under the customer's control. The CA must not access or generate customer private keys. Support for secure CSR generation (including HSM-based key protection) is required.
- Robust Certificate Validation and Issuance Controls
The solution must provide reliable revocation and verification mechanisms (e.g., OCSP stapling), Certificate Transparency logging with alerts for mis-issued certificates, and CAA enforcement to prevent unauthorized certificate issuance.
- Centralized Management, Monitoring, and Compliance
The solution must include discovery of all certificates, real-time inventory, expiry monitoring, security compliance checks (e.g., SSL Labs A rating), and support for modern web security standards such as HSTS.

- - Must ensure all certificates achieve SSL Labs rating A or A+. - Must support HTTP Strict Transport Security (HSTS). - No SHA-1/MD5, no RSA key exchange, no deprecated algorithms