TERM OF REFERENCE

PROVISION FOR DEVELOPMENT OF NATIONAL TRUSTED CRYPTOGRAPHIC ALGORITHM LIST (MYSEAL) CONFORMANCE TESTING TOOL (MCTT) SYSTEM FOR CYBERSECURITY MALAYSIA.

TABLE OF CONTENTS

1.0 OBJECTIVE

1.1 Cryptography Development Department, a department in CyberSecurity Malaysia is entrusted to perform conformance testing towards all implementation using any cryptographic algorithms that are listed in "Algoritma Kriptogafi Sedia Ada" (AKSA) National Trusted Cryptographic Algorithm List (MySEAL). This test is used to ensure the implementation of the cryptographic algorithms complies with the requirements of a specifications and conditions, regulations and standards along with its documentation.

1.2 With the above, Cryptography Development Department has taken an initiative to develop MySEAL Conformance Testing Tool (MCTT) system which is a web-based conformance testing tool that exclusively designed for all cryptographic algorithms listed in AKSA MySEAL. MCTT will improve the efficiency of the department in conducting the conformance testing.

2.0 BACKGROUND

2.1 MySEAL, National Trusted Cryptographic Algorithm List or "Senarai Algoritma Kriptografi Terpercaya Negara" is a project to develop a portfolio of national trusted cryptographic algorithms which specifically designed to provide a list of cryptographic algorithms suitable for implementation within Malaysia context that supports "Dasar Kriptografi Negara" (NCP). While NCP serves as a guiding document for Malaysia to achieve cryptographic sovereignty, MySEAL will support in the scientific areas of cryptography and cryptanalysis. For a cryptographic algorithm to be listed into MySEAL, it needs to comply with the criteria which have been developed based on accepted international standards and requirements defined by MySEAL Focus Group committee. This committee is spearheaded by CyberSecurity Malaysia and supported by members from Malaysian institutions.

2.2 The MySEAL project will be used as a requirement and guideline on the usage of cryptographic algorithms in all trusted cryptography products in Malaysia. Currently, the total number of cryptographic algorithms listed in AKSA MySEAL is fifty-eight (58) cryptographic algorithms which are consists of twelve (12) Symmetric Block Cipher algorithms, three (3) Stream Cipher algorithms, eleven (11) Asymmetric Cryptographic algorithms, twenty (20) Cryptographic Hash Function algorithms, three (3) Cryptographic Key Generation algorithms, and nine (9) Deterministic Random Bit Generators.

2.3 MCTT is aimed to minimize the time consumed in accomplishing the conformance test as much as possible. By developing this centralized conformance testing tool, it will be more convenient to the testers in conducting conformance test towards all listed cryptographic algorithms. This is due to the automation of generating: -

- 2.3.1 the input test vectors
- 2.3.2 the output (Ciphertext) of all fifty-eight (58) cryptographic algorithms listed in AKSA MySEAL
- 2.3.3 the conformance test result by comparing both output from MCTT and vendor's application using hashing algorithm

3.0 SCOPE OF WORK

The basic flow of MySEAL Conformance Testing Tool (MCTT) is illustrated as in Figure 1.

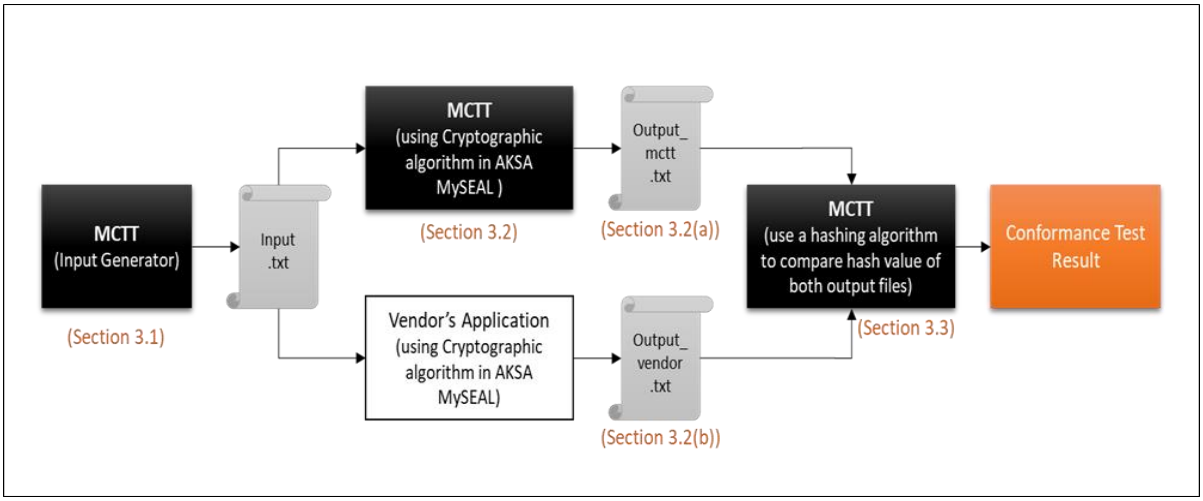

Figure 1: Basic Flow of MCTT

There are three (3) main functions in MCTT: -

3.1 Test Vector Generator

The first function in MCTT is to generate a thousand (1,000) test vectors for all fifty-eight (58) cryptographic algorithms listed in AKSA MySEAL. Test vector is a set of inputs or parameters provided to a system in order to test that system. The output of this function will be the input for the vendor's application that using any cryptographic algorithm listed in AKSA MySEAL.

3.2 Cryptographic Algorithm Function

The second function in MCTT is to process the input file that contains test vectors generated by the first function which has been mentioned in item 3.1. This function will be able to perform encryption and decryption process for all fifty-eight (58) cryptographic algorithms that was listed in AKSA MySEAL. This function will generate an output file, where generally it will contain information on ciphertext or hash value. Then it will be compared to the output file that will be provided by the vendor. The comparison process will be done in the third function in MCTT which will be described in item 3.3.

3.3 Conformance Test Result Generator

The third function will be used to generate a hash value of any file by using a hash function. To complete a conformance testing towards an application or implementation that using any cryptographic algorithm listed in AKSA MySEAL, the output file that has been generated (refer to 3.2(a) in Figure 1) needs to be compared with the output that was provided by the vendor (refer to 3.2(b) in Figure 1). The comparison is used to check whether they are identical or not. The effective ways to do this is by comparing their hash values. Both of their hash values should be the same if both of the output files are containing the same contents.

3.4 Proposal shall comply with all the provisions of this Request for Proposal (RFP). Any proposal not complying therewith may be disregarded. The Bidder is required to submit a proposal that shall include the following:

ITEM NOS.	CYBERSECURITY MALAYSIA's SCOPE OF WORKS, TECHNICAL SPECIFICATIONS & REQUIREMENTS	*CYBERSECURITY MALAYSIA's RQMT LEVEL (See Note 1)*	*PLEASE TICK IF BIDDER* COMPLY *(See Note 2)*	*BIDDER'S REMARKS (INCLUDING DETAILS/REASONS AND ATTACHMENT) IF BIDDER DOES NOT COMPLY*	*BIDDER'S REMARKS IF ANY (INCLUDING DETAILS AND ATTACHMENT) IN SUPPORTING THEIR COMPLIANCE STATEMENT*
A	**GENERAL REQUIREMENTS**				
1.0	**SCOPE OF WORKS**				
1.1	Bidder **MUST** fully comply with the scope of works, which include the design, development, testing, commissioning, handover and acceptance of the development of MySEAL Conformance Testing Tool (MCTT) System specified in Bill of Quantities and Price Schedules.	M			
1.2	The proposed solution of MySEAL Conformance Testing Tool (MCTT) System shall be delivered (including appropriate packaging) to CyberSecurity Malaysia, Selangor, Malaysia.	M			
1.3	Bidder's partial compliance to the said scope of works shall be disqualified.	M			
2.0	**BIDDER PAST EXPERIENCES**				
2.1	Bidder **MUST** possess a minimum of two (2) years relevant experiences in development and implementation of any cryptographic algorithm or relevant services.	M			
2.2	Bidder to provide list of relevant project experience or similar exercise.	M			
3.0	**WARRANTY REQUIREMENTS**				
3.1	The warranty shall include preventive and corrective maintenance for the proposed solution.	M			
3.2	The proposed solution shall have minimum of one (1) year standard warranty from the date of commissioning and acceptance by CyberSecurity Malaysia.	M			
3.3	Bidder **MUST** provide preventive maintenance of the system on quarterly basis for one (1) year. Report should be provided after each maintenance activity.	M			

ITEM NOS.	CYBERSECURITY MALAYSIA's SCOPE OF WORKS, TECHNICAL SPECIFICATIONS & REQUIREMENTS	*CYBERSECURITY MALAYSIA's RQMT LEVEL (See Note 1)*	*PLEASE TICK IF BIDDER* COMPLY *(See Note 2)*	*BIDDER'S REMARKS (INCLUDING DETAILS/REASONS AND ATTACHMENT) IF BIDDER DOES NOT COMPLY*	*BIDDER'S REMARKS IF ANY (INCLUDING DETAILS AND ATTACHMENT) IN SUPPORTING THEIR COMPLIANCE STATEMENT*
4.0	**DOCUMENTATION REQUIREMENTS**				
4.1	All documentation shall be in English. Bidder shall be responsible for any translation cost incurred (if any) in regard to the submission of the documentation required by this RFP.	M			
4.2	CyberSecurity Malaysia reserves the right to reproduce all or part of the document submitted by the bidder for internal use.	G			
4.3	Bidder shall provide logical and physical architecture design of the proposed solution including the functionality, system testing, user acceptance testing, list of cryptographic algorithm sources, user manual and any other related information to the proposed solution.	M			
4.4	The bidder shall present the proposed solution in oral presentation and RFP documentation to CyberSecurity Malaysia as part of evaluation process in this tender. (if required)	M			
5.0	**DELIVERY REQUIREMENTS**				
5.1	Bidder is required to propose reasonable and workable project timeline. However, the Project **must not exceed six (6) months** after receipt of CyberSecurity Malaysia Letter Of Acceptance (LOA). Please refer to Item 4.0 of Terms of Reference (TOR).	M			
5.2	CyberSecurity Malaysia has the right to reject any kind of bugs during or after installation. The replacement shall be done without extra charge.	M			
5.3	Upon completion of the development works, bidder is required to submit: i) User Requirement Document; ii) Development reports includes, but is not limited to bugs fixing; iii) Project Progress Meeting Documentation, including Minutes of Meeting and Slides presentation; iv) User Acceptance Test (UAT) approved by both parties; v) System design document; vi) Admin and user manual; *Note:* *i) All documents, reports or materials prepared/developed by the Vendor specifically in relation to or for the purpose of this Proposal, shall unless otherwise expressly agreed, belong to CyberSecurity Malaysia (CSM);* ii) *Once the party agreed to the terms of the proposed solution, a separate term will be negotiated between the parties for the development, then the source code shall be transferred to CSM once payment has been made.*	M			

ITEM NOS.	CYBERSECURITY MALAYSIA's SCOPE OF WORKS, TECHNICAL SPECIFICATIONS & REQUIREMENTS	*CYBERSECURITY MALAYSIA's RQMT LEVEL (See Note 1)*	*PLEASE TICK IF BIDDER* COMPLY *(See Note 2)*	*BIDDER'S REMARKS (INCLUDING DETAILS/REASONS AND ATTACHMENT) IF BIDDER DOES NOT COMPLY*	*BIDDER'S REMARKS IF ANY (INCLUDING DETAILS AND ATTACHMENT) IN SUPPORTING THEIR COMPLIANCE STATEMENT*
6.0	**BIDDER RESPONSIBILITY**				
6.1	Bidder shall conduct any rectification or modification on MCTT (without extra charges) if there are any issues arise from Security Assessment conducted by CyberSecurity Malaysia before deployment of the MCTT.	M			
6.2	Bidder shall propose minimum hardware specification to be used for the development of the proposed solution as CyberSecurity Malaysia will provide such requirements using our existing infrastructure platforms. This information will be provided to successful bidder upon the receipt of CyberSecurity Malaysia Letter of Acceptance (LOA). The bidder shall focus on the development works on MCTT using open-source software or libraries.	M			
6.3	Bidder is subjected to all existing government guidelines, procedures and regulations pertaining to the procurement and conduct of professional services.	M			
6.4	Bidder shall confirm that their proposal is based on the entire provision of the above scope of works/terms of reference. Bidder's partial compliance to the said scope of works/terms of reference shall be disqualified.	M			
6.5	Bidder shall review this document and take full responsibility for obtaining the necessary information from CyberSecurity Malaysia as may be required to meet the specifications and requirements.	M			
6.6	Bidder shall review and fulfil all specifications and requirements before committing to sign the purchase agreement.	I			
6.7	Any of the outputs, findings, assessments and any other documents pertaining to the development and implementation of the Project shall not be abused or used by the Bidder for profit based or otherwise.	G			
6.8	In the interest of national security, all discussions and decisions made by will remain confidential and should not be disclosed to any other person or organisation.	I			
6.9	Bidder is expected to sign the Non-Disclosure Agreement (NDA) with CyberSecurity Malaysia to ensure unnecessary disclosure of information on the subject area before, during and after delivery of the consultancy services.	M			
6.10	No media briefings can be undertaken or press releases issued by the Bidder or any of the Project team members.	M			

ITEM NOS.	**CYBERSECURITY MALAYSIA's SCOPE OF WORKS, TECHNICAL SPECIFICATIONS & REQUIREMENTS**	*CYBERSECURITY MALAYSIA's RQMT LEVEL (See Note 1)*	*PLEASE TICK IF BIDDER* **COMPLY** *(See Note 2)*	*BIDDER'S REMARKS (INCLUDING DETAILS/REASONS AND ATTACHMENT) IF BIDDER DOES NOT COMPLY*	*BIDDER'S REMARKS IF ANY (INCLUDING DETAILS AND ATTACHMENT) IN SUPPORTING THEIR COMPLIANCE STATEMENT*
B	**TECHNICAL SPECIFICATIONS & REQUIREMENTS**				
1.0	**PURPOSE**				
1.1	To provide solution of MySEAL Conformance Testing Tool (MCTT) System as per specifications and features as below:	M			
2.0	**MySEAL CONFORMANCE TESTING TOOL (MCTT) SYSTEM**				
2.1	Bidder shall ensure the implementation of MCTT is a web-based solution with appropriate access control, system logs and implementing secure by design principal	M			
2.2	**Phase 1 – Development Phase** Bidder shall ensure three (3) main functions in MCTT System are successfully developed:	M			
	(i) Test Vector Generator • Bidder shall ensure the MCTT is able to generate an output file which contains of at least 1000 test vectors • Bidder shall ensure that any required format of the test vector is set by CyberSecurity Malaysia • Bidder shall ensure that the output file is compatible with the cryptographic algorithm function	M			
	(ii) Cryptographic Algorithm Function • Bidder shall ensure this function is able to process all of 58 cryptographic algorithms which are listed as below: - **1. 12 Symmetric Block Ciphers** AES-128, AES-192, AES-256, Camellia-128, Camellia-192, Camellia-256, CLEFIA-128, CLEFIA-192, CLEFIA-256, PRESENT-80, PRESENT-128, and HIGHT **2. 3 Symmetric Stream Ciphers** ChaCha20-256, KCipher-2, Rabbit	M			

ITEM NOS.	CYBERSECURITY MALAYSIA's SCOPE OF WORKS, TECHNICAL SPECIFICATIONS & REQUIREMENTS	CYBERSECURITY MALAYSIA's RQMT LEVEL (See Note 1)	PLEASE TICK IF BIDDER COMPLY (See Note 2)	BIDDER'S REMARKS (INCLUDING DETAILS/REASONS AND ATTACHMENT) IF BIDDER DOES NOT COMPLY	BIDDER'S REMARKS IF ANY (INCLUDING DETAILS AND ATTACHMENT) IN SUPPORTING THEIR COMPLIANCE STATEMENT
	3. 11 Asymmetric Cryptographic DSA, ECDSA, RSA-PSS, PSEC-KEM, RSA-KEM, ECIES-KEM, RSA-OAEP, NTRU, ECDH, and DH **4. 20 Cryptographic Hash Function** SHA-384, SHA-512, SHA-512/224, SHA-512/256, SHA3-224, SHA3-256, SHA3-384, SHA3-512, SHAKE128, SHAKE256, SPONGENT-88, SPONGENT-128, SPONGENT-160, SPONGENT-224, SPONGENT-256, PHOTON-80/20/16, PHOTON-128/16/16, PHOTON-160/36/36, PHOTON-224/32/32, and PHOTON-256/32/32 **5. 3 Cryptographic Key Generation** Miller-Rabin Primality Test, Elliptic curve Primality Certificate, and Shawe-Taylor's Algorithm **6. 9 Deterministic Random Bit Generator** HMAC-SHA-384-DRBG, HMAC-SHA-512-DRBG, SHA-512/224-DRBG, SHA-512/256-DRBG5, SHA-384-DRBG, SHA-512-DRBG, AES-128-CTR-DRBG, AES-192-CTR-DRBG, and 3-Key-TDEA-CTR-DRBG				
	• Bidder shall ensure that this function is able to produce a text file which contains the output of the cryptographic algorithm function	M			
	• Bidder shall ensure that the algorithm is develop correctly and conform to its corresponding standards.	M			
	• If the bidder used any cryptographic library to develop this function, bidder shall ensure that the source of the library is well stated in the comment's section.	M			
	(iii) <u>Conformance Test Result Generator</u>				
	• Bidder shall ensure the function is able to hash two (2) different input files using a standard hashing algorithm	M			
	• Bidder shall ensure the function is able to compare the hash value of two (2) different input files	M			
	• Bidder shall ensure the function is able to determine whether two (2) different input files are identical or not	M			
	• Bidder shall ensure the function is able to generate the conformance testing result	M			

ITEM NOS.	CYBERSECURITY MALAYSIA's SCOPE OF WORKS, TECHNICAL SPECIFICATIONS & REQUIREMENTS	CYBERSECURITY MALAYSIA's RQMT LEVEL (See Note 1)	PLEASE TICK IF BIDDER COMPLY (See Note 2)	BIDDER'S REMARKS (INCLUDING DETAILS/REASONS AND ATTACHMENT) IF BIDDER DOES NOT COMPLY	BIDDER'S REMARKS IF ANY (INCLUDING DETAILS AND ATTACHMENT) IN SUPPORTING THEIR COMPLIANCE STATEMENT
2.3	**Phase 2 – Testing Phase** Bidder shall perform System Testing (ST) and User Acceptance Testing (UAT) once MCTT have been implemented with proper documentation on logical and physical architecture of the proposed solution.	M			
2.4	Bidder **MUST** have engineer/developer with sufficient experience in developing cryptographic implementation and preferably with suitable certification. Bidder to provide Curriculum-vitae (CV) of engineer/developer involved.	M			
C	**SUPPORT AND MAINTENANCE REQUIREMENT**				
1.0	**VENDOR ASSISTANCE REQUIREMENT**				
1.1	Bidder is required to have an established technical support set-up in Malaysia.	M			
1.2	Bidder must possess technical support personnel. Bidder to specify the number of personnel.	G			
1.3	Bidder is required to specify on any special requirement in order to provide on-site support.	G			
1.4	Bidder **MUST** provide onsite corrective technical support for a period of one (1) year with 9 x 5. (Exclude weekend and public holiday.)	M			
1.5	Bidder **MUST** provide two (2) hours response time and one (1) working day resolution time for minor issue and five (5) working days resolution time for major issue.	M			
1.6	Bidder **MUST** provide the Service Level Agreement (SLA).	M			

Note 1 : CyberSecurity Malaysia's Requirement Level: -

M – Mandatory Requirement : These are ESSENTIAL/CRITICAL requirements that MUST be fully complied by Bidder.
G – General Requirement : These are DESIRABLE requirements and Bidder is required to comply.
I – For Info Only : These are information for the Bidder to take note and acknowledge.

Note 2 : A blank (i.e. no tick in this column) shall be taken as Bidder being in non-compliance for that particular line item unless otherwise specified.

4.0 PROJECT DELIVERABLES & TIMELINE

The Bidder shall propose a reasonable and workable project timeline. However, the project shall **not exceed 6 months** after receipt of CyberSecurity Malaysia Letter Of Acceptance (LOA).

The example of propose timeline will be as follows:

	Activity	*Timeline
1.	Letter of Award (LOA) is issued by CyberSecurity Malaysia	T1
2.	Signing of relevant contract & documents (including review of documents from Legal)	T2 = T1 + 2 w
3.	Phase 1 – Development Phase	T3= T1 + a w
4.	Phase 2 – Testing Phase	T4= T1 + b w
5.	Phase 3 – Security Assessment Phase	T5=T1 + c w

* Timeline by which activity shall be completed ('T1' is the date of LOA. 'w' means time period of a week, 'a', 'b', and 'c' is the propose timeline)

5.0 SUBMISSION OF PROPOSAL

5.1 The Bidder shall submit the proposal as per specified in **Item 3; Scope of Work.**

6.0 POINT OF CONTACT

The bidder shall nominate an executive level within their organization, whom shall be a full-time employee of the organization, to be the working together with Project Owner from CyberSecurity Malaysia. The appointed person shall be the single point of contact between the bidder and CyberSecurity Malaysia.

--- END OF DOCUMENT---