KEMENTERIAN SAINS, TEKNOLOGI DAN INOVASI
MINISTRY OF SCIENCE, TECHNOLOGY AND INNOVATION

CyberSecurity MALAYSIA
Agensi di bawah MOSTI

BORANG PENYERAHAN ALGORITMA

Algorithm Submission Form

SENARAI ALGORITMA KRIPTOGRAFI TERPERCAYA NEGARA (MySEAL)

MAKLUMAT SERAHAN *Submission Information*	
☐ Individu *Individual*	☐ Organisasi *Organisation*

A. MAKLUMAT PENYERAH

Submitter Information

MAKLUMAT PENYERAH *Submitter Information*	
NAMA PENYERAH UTAMA *Principal Submitter's Name*	
NO TELEFON PEJABAT *Office Tel No*	
NO TELEFON MUDAH ALIH *Mobile No*	
NO FAKSIMILI *Fax No*	
ALAMAT E-MEL *E-mail Address*	
ALAMAT SURAT MENYURAT *Postal Address*	

NAMA PENYERAH TAMBAHAN (jika berkenaan) *Name of Auxiliary Submitter(s)* *(if any)*	
NAMA PEREKA CIPTA / PEMBANGUN ALGORITMA *Name of Algorithm Inventor(s) / Developer(s)*	
NAMA PEMILIK ALGORITMA (jika berlainan daripada penyerah utama) *Name of Algorithm's Owner* *(if different from the submitter)*	
TANDATANGAN PENYERAH *Signature of Submitter*	

MAKLUMAT ORGANISASI (untuk serahan organisasi sahaja) *Organisation Information (for organisation submission only)*	
ORGANISASI *Organisation*	
ALAMAT *Address*	

B. MAKLUMAT ALGORITMA

Algorithm Information

NAMA ALGORITMA *Name of algorithm*	
PRIMITIF ALGORITMA KRIPTOGRAFI *Cryptographic Algorithm Primitive*	☐ *Symmetric* ☐ *Block Cipher* ☐ *Block Cipher* ☐ *Lightweight Block Cipher* ☐ *Stream Cipher* ☐ *Synchronous stream cipher* ☐ *Self- Synchronous stream cipher* ☐ *Asymmetric* ☐ *Encryption* ☐ *Key agreement* ☐ *Digital signature* ☐ *Cryptographic Hash Function* ☐ *Cryptographic hash function* ☐ *Lightweight hash function*
CADANGAN TAHAP KESELAMATAN *Proposed Security Level*	☐ 40 – bit ☐ 80 – bit ☐ 128 – bit ☐ 192 – bit ☐ 256 – bit ☐ Lain-lain. Sila nyatakan. *Other(s). Please specify* _____
CADANGAN PLATFORM *Proposed Environment*	☐ Perkakasan *Hardware* ☐ Perisian *Software*

C. MAKLUMAT TAMBAHAN

Additional Information

PENGGUNAAN *Implementation*	☐ *Bluetooth* ☐ *Global System for Mobile communications (GSM)* ☐ *Radio-Frequency Identification (RFID)* ☐ *Smart cards* ☐ *Mobile devices* ☐ *Sensor network* ☐ *Microcontroller* ☐ *Microprocessor* ☐ *Field-programmable gate array (FPGA)* ☐ Lain-lain. Sila nyatakan. *Other(s). Please specify* _____

PENYATAAN PENYERAH

STATEMENT BY THE SUBMITTER

I/We do hereby understand that my/our submitted algorithm may not be selected for inclusion in MySEAL. I/We also understand and agree that after the close of the submission period, my/our submission may not be withdrawn. I/We further understand that I/we will not receive financial compensation from MySEAL project for my/our submission.

Diserahkan oleh (Tandatangan & Cop): *Submitted by (Signature & Stamp):* Tarikh: *Date:*	Diterima oleh (Tandatangan & Cop): *Received by (Signature & Stamp):* Tarikh: *Date:*

SENARAI SEMAK

Checklist

Bil ***No***	**Perkara / Dokumen diperlukan** ***Document(s) needed***	**Disertakan oleh Penyerah (√)** ***Supplied by Submitter (√)***	**Disemak oleh Penerima (√)** ***Checked by Receiver (√)***	**Catatan** ***Notes***
1	Profil Syarikat *Company Profile*			
2	Laporan analisis *Analysis Report* *Symmetric Block Cipher* ☐ Ujian statistik NIST *NIST statistical tests* ☐ *Linear cryptanalysis* ☐ *Differential cryptanalysis* ☐ Lain-lain. Sila nyatakan. *Other(s). Please specify*. _____ *Symmetric Stream Cipher* ☐ Ujian statistik NIST *NIST statistical tests* ☐ *Algebraic attack* ☐ *Correlation attack* ☐ *Distinguishing attack* ☐ *Guess-and-Determine attack* ☐ Lain-lain. Sila nyatakan. *Other(s). Please specify.* _____			

Bil ***No***	**Perkara / Dokumen diperlukan** ***Document(s) needed***	**Disertakan oleh Penyerah (√)** ***Supplied by Submitter (√)***	**Disemak oleh Penerima (√)** ***Checked by Receiver (√)***	**Catatan** ***Notes***
	Asymmetric Cryptographic Algorithm ☐ *Hard Mathematical Problems and assumptions* ☐ *Security Model and its proof* *Cryptographic Hash Function* ☐ *Pre-image resistance* ☐ *Second pre-image resistance* ☐ *Collision resistance*			
3	Laporan prestasi algoritma mengikut keupayaan perkakasan dan/atau perisian *Implementation and performance reports on hardware and/or software*			
4	Laporan reka bentuk *Justification on design principles*			
5	Vektor ujian *Test vectors*			
6	Penyata / perjanjian / pendedahan Harta Intelek *Intellectual Property statements / agreements / disclosures*			