



An agency under MOSTI

### Malaysian Validation Programs Overview

Hazlin Abdul Rani

CyberSecurity Malaysia Malaysia

Copyright © 2017 CyberSecurity Malaysia

#### 





#### INTRODUCTION





### CyberSecurity Malaysia

- Company Limited-by-Guarantee under the supervision of Ministry of Science Technology and Innovation (MOSTI)
- 🖵 Est. 1997
- A National Body to monitor the National e-Security aspect
- Provides specialised cybersecurity services and continuously identifies possible areas that may be detrimental to national security and public safety



#### **OUR SERVICES**





security

### SECURITY ASSURANCE - ICT PRODUCT EVALUATION





#### ICT Product Evaluation / Assessment





### MALAYSIA CRYPTOGRAPHY MODULE VALIDATION SCHEME





# Cryptography Module Validation Scheme (MyCMV)

- Currently being developed by ISCB, CyberSecurity Malaysia
- Complement two other existing schemes
  - Malaysian Common Criteria Evaluation & Certification (MyCC) Scheme
  - ICT Product Security Assessment (IPSA) Certification Scheme
- Validate cryptographic module cryptography algorithm conformance test



#### MyCMV Timeline

11<sup>th</sup> Malaysian Development Plan (RMK11), 2016 - 2020

Before RMK11	2016	2017	2018	2019
<ul> <li>Research – FIPS140, Cryptrec, NESSIE etc</li> <li>Consultant</li> <li>Training</li> </ul>	<ul> <li>Apply for lab accreditati on</li> <li>Developing MyCMV Scheme</li> <li>MySEAL initiatives</li> </ul>	<ul> <li>Lab accreditati on</li> <li>Continue developing MyCMV Scheme</li> <li>1<sup>st</sup> phase MySEAL</li> </ul>	<ul> <li>Pilot test MyCMV</li> <li>2<sup>nd</sup> phase MySEAL</li> </ul>	<ul> <li>Finalised MyCMV Scheme</li> <li>Launch MyCMV Scheme</li> </ul>
			<	



#### **Propose Structure**









### MySEAL Project

#### <u>SENARAI ALGORITMA KRIPTOGRAFI TERPERCAYA NEGARA /</u> National Trusted Cryptography Algorithm List

- The MySEAL project is a multi-year effort, running from 2016-2020, which will be used as a requirement and guideline on the usage of cryptographic algorithms in all trusted cryptography products in Malaysia
- specifically designed to provide a list of cryptographic algorithms suitable for implementation within Malaysian context that supports Dasar Kriptografi Negara (DKN)
- MySEAL Focus Group & MySEAL Evaluation Committee

https://myseal.cybersecurity.my



# MySEAL Project

#### Existing algorithm

#### New algorithm

Published as a standard or in other national cryptography algorithm project



ISO/IEC, NIST, CRYPTREC, NESSIE



Has not been published as a standard



Local & International participants



Symmetric, Asymmetric, Hash function, Key Generation



https://myseal.cybersecurity.my



## Crypto Validation Facility

- Cryptography Evaluation Lab (MyCEL)
- In the process of CST lab accreditation by NVLAP





#### Challenges

- No local expertise in FIPS140 & ISO19790
- Accredited crypto evaluation facility
- Evaluator / validator for cryptography module







An agency under MOSTI

# Thank you

#### **Corporate Office**

CyberSecurity Malaysia, Level 5, Sapura@Mines No. 7 Jalan Tasik The Mines Resort City 43300 Seri Kembangan Selangor Darul Ehsan, Malaysia.

T : +603 8992 6888 F : +603 8992 6841 H : +61 300 88 2999

www.cybersecurity.my info@cybersecurity.my

#### **Northern Regional Office**

CyberSecurity Malaysia, Level 19, Perak Techno-Trade Centre Bandar Meru Raya, Off Jalan Jelapang 30020 Ipoh, Perak Darul Ridzuan, Malaysia

T: +605 528 2088 F: +605 528 1905



www.facebook.com/CyberSecurityMalaysia



twitter.com/cybersecuritymy





CERTIFIED TO ISO/IEC 27001:20 CERT. NO. : AR 4656

ISMS







Copyright © 2017 CyberSecurity Malaysia