


Schedule

Issue date: 14 July 2025
Valid Until: -



NO: SAMM 856

Page: 1 of 3

LABORATORY LOCATION/ CENTRAL OFFICE:	TUV Austria Cybersecurity Lab Sdn. Bhd. A-11-01, Empire Office Tower, Jalan SS 16/1, Ss 16, 47500 Subang Jaya, Selangor. , 47500, SELANGOR MALAYSIA
	
ACCREDITED SINCE :	14 JULY 2025
FIELD(S) OF TESTING:	SOFTWARE TESTING

This laboratory has demonstrated its technical competence to operate in accordance with MS ISO/IEC 17025:2017 (ISO/IEC 17025:2017).

This laboratory's fulfillment of the requirements of ISO/IEC 17025 means the laboratory meets both the technical competence requirements and management system requirements that are necessary for it to consistently deliver technically valid test results and calibrations. The management system requirements in ISO/IEC 17025 are written in language relevant to laboratory operations and operate generally in accordance with the principles of ISO 9001 (see Joint ISO-ILAC-IAF Communiqué dated April 2017).

CENTRAL LOCATION:	TUV Austria Cybersecurity Lab Sdn. Bhd. A-11-01, Empire Office Tower, Jalan SS 16/1, Ss 16, 47500 Subang Jaya, Selangor. , 47500, Selangor
FIELD(S) OF TESTING :	SOFTWARE TESTING,

SCOPE OF TESTING : SOFTWARE TESTING

Material / Product Tested	Type Of Test / Properties Measured / Range Of Measurement	Standard Test Methods / Equipment / Techniques
Application	Injection Flaws - - Log inspection	method: method:
Drivers, Operating Systems And Applications	technology -" Security techniques -" Evaluation criteria for IT-•	Part 2: Security functional requirements Part 3: Security assurance
	technology -" Security techniques -" Evaluation criteria for IT-•	requirements
	technology -" Security techniques -" Evaluation criteria for IT-•	Common Methodology for
	technology -" Security techniques -" Evaluation criteria for IT-•	Information Technology Security

Schedule

Issue date: 14 July 2025
Valid Until: -



NO: SAMM 856

Page: 2 of 3

Material / Product Tested	Type Of Test / Properties Measured / Range Of Measurement	Standard Test Methods / Equipment / Techniques
	technology -" Security techniques - " Evaluation criteria for IT-•	Evaluation (CEM v3.1)
	technology -" Security techniques - " Evaluation criteria for IT-•	The Common Criteria Evaluation
	technology -" Security techniques - " Evaluation criteria for IT-•	for the following Assurance Level:
	technology -" Security techniques - " Evaluation criteria for IT-•	EAL1: Functionally Tested e
	technology -" Security techniques - " Evaluation criteria for IT-•	EAL2: Structurally Tested e
	technology -" Security techniques - " Evaluation criteria for IT-•	EAL3: Methodically Tested e
	technology -" Security techniques - " Evaluation criteria for IT-•	and Checked
	technology -" Security techniques - " Evaluation criteria for IT-•	EAL4: Methodically Designed,
	technology -" Security techniques - " Evaluation criteria for IT-•	Tested and Reviewed
Firmware And Software	Technology Security Evaluation	Part 1 Introduction and e
Ict Products And	security under the MyCC Scheme in	Technology Security Evaluation
Mobile	Application Layer	Mobile application penetration test
Network	SSL/TLS Certificate, Cipher Algorithms	Network penetration test method:
Penetration	Malicious File Execution -	None
	- Application installer reverse engineering	None
	and Protocols	None
Protection Profile And	Information Security Evaluation of IT	Common Criteria for Information
Review	Broken Authentication and Session	None
	Management	Open Web Application
	Cross-Site Scripting (XSS)	Security Project (OWASP)
	Insecure Direct Object Reference	None
	Security Misconfiguration	None
	Sensitive Data Exposure	None
	Missing Functional Level Access Control	None
	Cross-Site Request Forgery (CSRF)	None
	Using Components with Known	None
	Vulnerabilities	None
	Unvalidated Redirects and Forwards	None
Source Code	Injection Flaws	Source code review test method:
Such As Low Level	Criteria ISO/IEC 15408, -œInformation	general model

Scan this QR Code or visit <https://accreditation.ism.gov.my/public/listing/cab/samm-ct/3005671> for the current scope of accreditation

Schedule

Issue date: 14 July 2025
Valid Until: -



NO: SAMM 856

Page: 3 of 3

Material / Product Tested	Type Of Test / Properties Measured / Range Of Measurement	Standard Test Methods / Equipment / Techniques
Systems Which Include	accordance with information	(CC v3.1) including:
Testing	Insecure Direct Object Reference	Open Web Application -
	Cross Site Request Forgery (CSRF)	security Project (OWASP)
	Information Leakage and Improper Error	None
	Handling	None
	Broken Authentication and Session	None
	Management	None
	Insecure Cryptographic Storage	None
	Insecure Communications	None
	Failure to Restrict URL Access	None
	- Application permission review	Open Web Application
	- User interface limitation bypass	Security Project (OWASP)
	- User interface limitation bypass	Open Android Security
	Server Layer (API)	Assessment Methodology
	- Access control	(OASAM)
	Authentication	None
	Session management -	None
	Error management -	None
	Input validation -	None
	Transport Layer	None
	Device Layer	None
	Obsolete Version, EOL (End of Life)	Open Source Security Testing
	findings	Methodology Manual
	Patch-related findings for Operating	(OSSTMM)
	Systems, Applications and Services	None
	Best practices and Configuration findings	None
	for Known Services	None
	Authentication based findings	None
Web	Cross Site Scripting (XSS) Flaws	Web application penetration test

Scan this QR Code or visit <https://accreditation.ism.gov.my/public/listing/cab/samm-ct/3005671> for the current scope of accreditation