How We Differ? ❶ - References & Credentials over the past 15 years

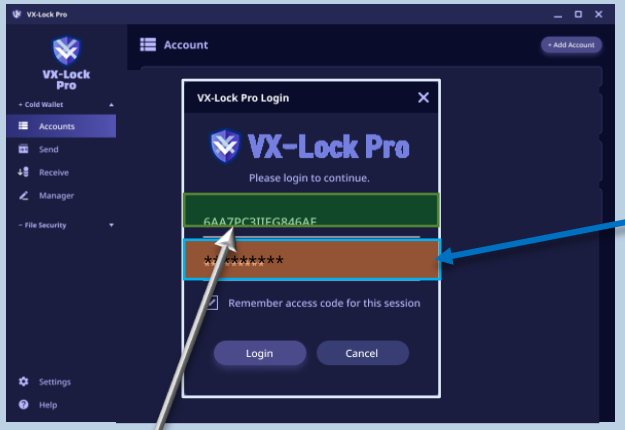
Military Grade Security

- Technology Endorsement by Chief Government Security Officer (CGSO) under Prime Minister's Department in Malaysia, 2006
- Safe-All, Special USB Drive for Securing File & Data in storage was released provided in Republic of Korea, 2008
- Endorsement and Deployment of Secure Email System's communication for Cabinet of Malaysia under Prime Minister Department for secure communication with other Ministries
- MAMPU's Accreditation & Endorsement as Most Trusted Encryption Provider to All Government Agencies under the National Cryptography Policy
- POC Project of Secure ID Issuance System with TAQNIA(Saudi Technology Development and Investment Company) in 2014
- MasterCard Qualified Onboarding Developer for e-wallet & platform
- E-Wallet platform developer for Singapore Precious Metals Exchange (SGPMX) – ongoing eMobile Trading & Backend System's development
- Development & supply of SypherSafe Secure Mobile communication System to various Malaysia agencies & Philippines Police Intelligence for their highly sensitive mobile communication

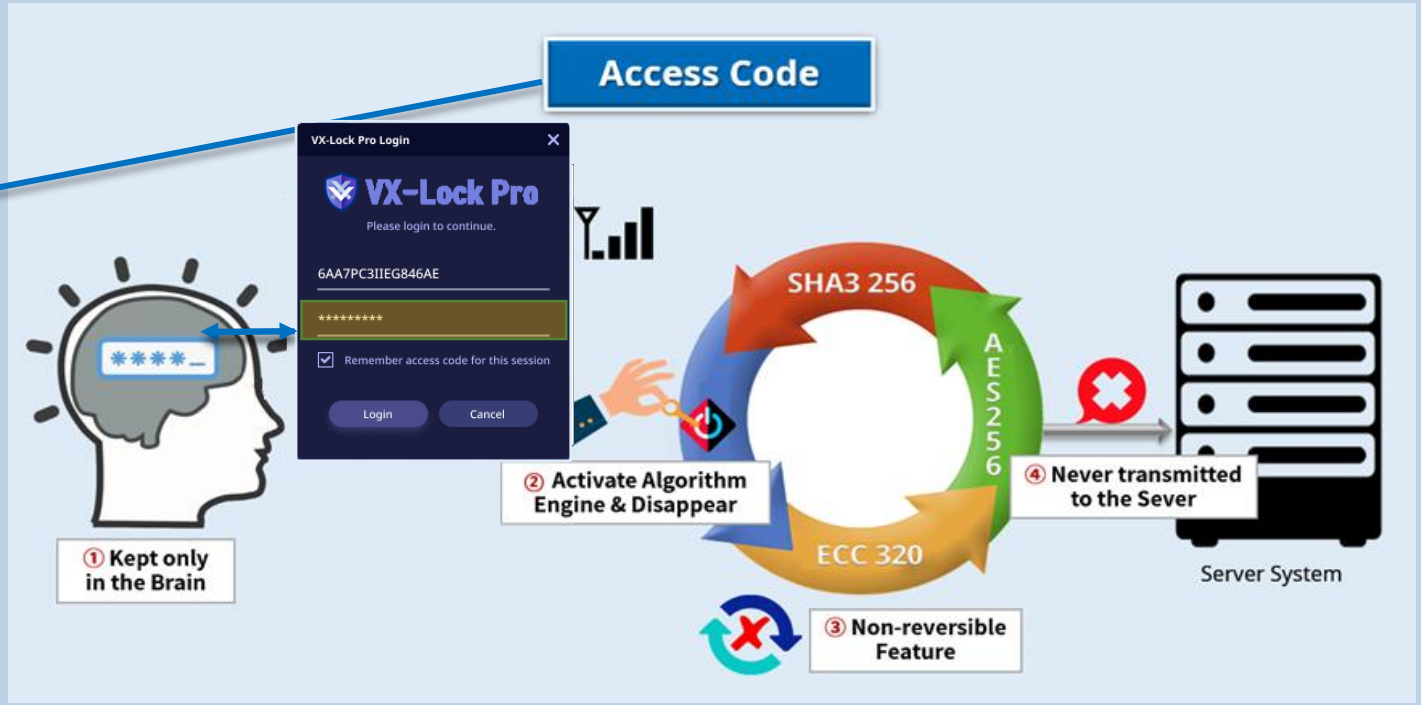



VX-Lock

How We Differ? ❷ - Login Security & Dual Network Encryption



Although the User ID looks like plain texts, it is a secure ID encrypted with ECC 320 bit and imported.



① User/Device Authentication with Secure ID – Encrypting unique private info such as phone number, e-mail address, IMEI and etc. ⇨ Generating Secure ID ⇨ Importing for Secure Authentication

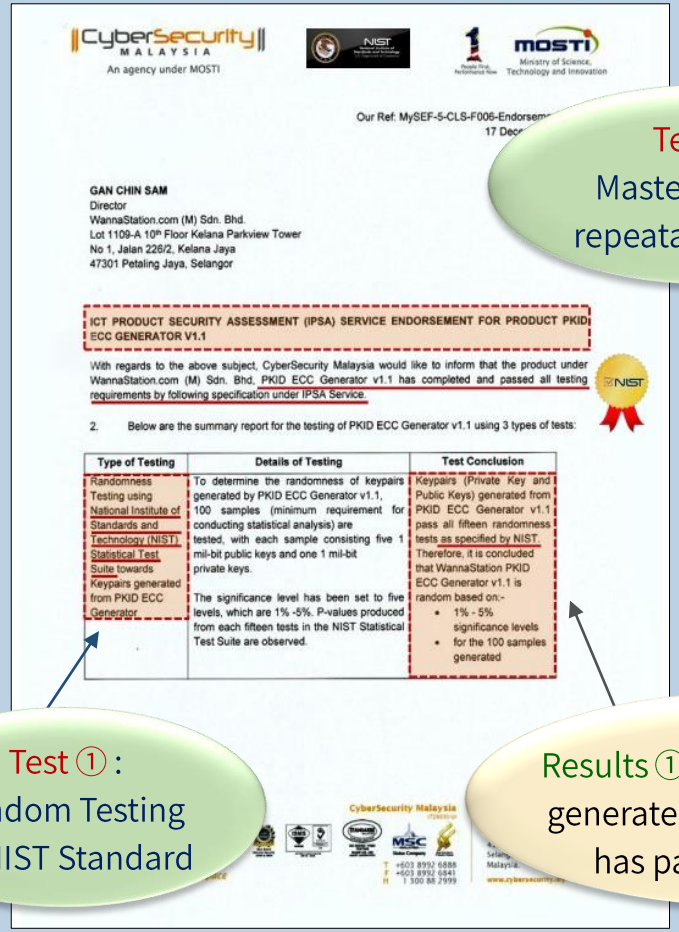
② Non-Repudiation & Anti-Copy – Strongest Tech against Fake Device & User intrinsically by making the user login with Secure ID(PKID)

③ Dual Network Encryption – Utilizing both AES 256 bit and SHA-3 256 bit at the same time

NIST National Institute of Standards and Technology | Common Criteria

VX-Lock

How We Differ? ❸ - With Secured ID(PKID) guaranteed by NIST



CyberSecurity MALAYSIA
An agency under MOSTI

MOSTI Ministry of Science, Technology and Innovation

Our Ref: MySEF-5-CLS-F006-Endorsem
17 Dec

GAN CHIN SAM
Director
WannaStation.com (M) Sdn. Bhd.
Lot 1109-A 10th Floor Kelana Parkview Tower
No 1, Jalan 226/2, Kelana Jaya
47301 Petaling Jaya, Selangor

ICT PRODUCT SECURITY ASSESSMENT (IPSA) SERVICE ENDORSEMENT FOR PRODUCT PKID ECC GENERATOR V1.1

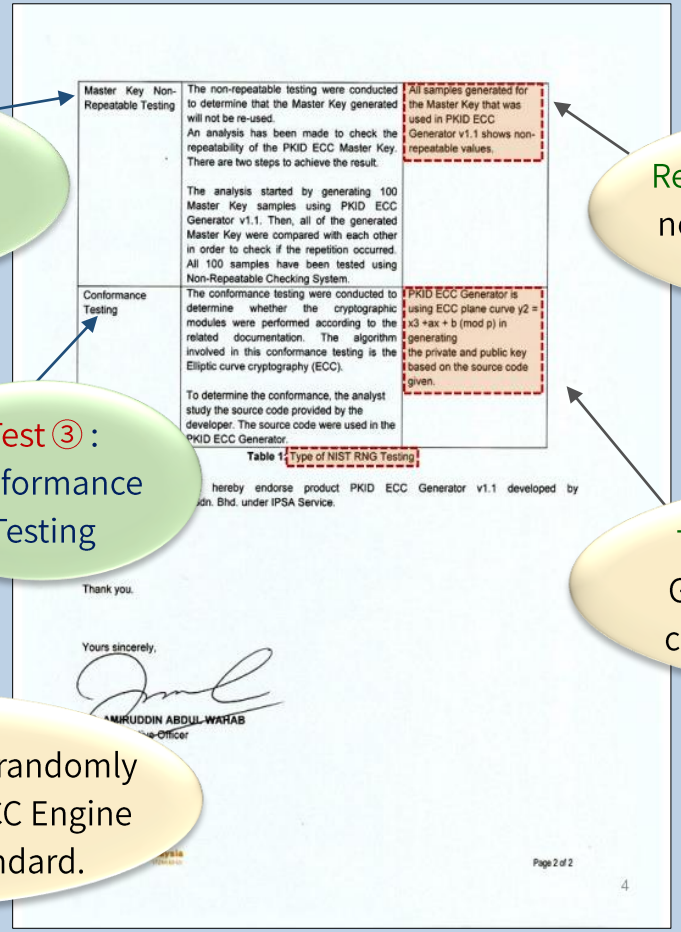
With regards to the above subject, CyberSecurity Malaysia would like to inform that the product under WannaStation.com (M) Sdn. Bhd. PKID ECC Generator v1.1 has completed and passed all testing requirements by following specification under IPSA Service.

2. Below are the summary report for the testing of PKID ECC Generator v1.1 using 3 types of tests:

Type of Testing	Details of Testing	Test Conclusion
Randomness Testing using National Institute of Standards and Technology (NIST) Statistical Test Suite towards Keypairs generated from PKID ECC Generator	To determine the randomness of keypairs generated by PKID ECC Generator v1.1, 100 samples (minimum requirement for conducting statistical analysis) are tested, with each sample consisting five 1 mil-bit public keys and one 1 mil-bit private keys. The significance level has been set to five levels, which are 1% -5%. P-values produced from each fifteen tests in the NIST Statistical Test Suite are observed.	Keypairs (Private Key and Public Keys) generated from PKID ECC Generator v1.1 pass all fifteen randomness tests as specified by NIST. Therefore, it is concluded that WannaStation PKID ECC Generator v1.1 is random based on:- • 1% - 5% significance levels • for the 100 samples generated

CyberSecurity Malaysia

T +603 8992 6888
F +603 8992 6841
H 1 300 88 2999



Master Key Non-Repeatable Testing	The non-repeatable testing were conducted to determine that the Master Key generated will not be re-used. An analysis has been made to check the repeatability of the PKID ECC Master Key. There are two steps to achieve the result. The analysis started by generating 100 Master Key samples using PKID ECC Generator v1.1. Then, all of the generated Master Key were compared with each other in order to check if the repetition occurred. All 100 samples have been tested using Non-Repeatable Checking System.	All samples generated for the Master Key that was used in PKID ECC Generator v1.1 shows non-repeatable values.
Conformance Testing	The conformance testing were conducted to determine whether the cryptographic modules were performed according to the related documentation. The algorithm involved in this conformance testing is the Elliptic curve cryptography (ECC). To determine the conformance, the analyst study the source code provided by the developer. The source code were used in the PKID ECC Generator.	PKID ECC Generator is using ECC plane curve $y2 = x3 + ax + b \pmod p$ in generating the private and public key based on the source code given.

Table 1: Type of NIST RNG Testing

hereby endorse product PKID ECC Generator v1.1 developed by
dn. Bhd. under IPSA Service.

Thank you.

Yours sincerely,

MIRUDDIN ABDUL WAHAB
ve Officer

Page 2 of 2

4

Test ② : Masterkey Non-repeatable Testing

Test ③ : Conformance Testing

Test ① : Random Testing by NIST Standard

Results ① : Every key randomly generated by PKID ECC Engine has passed its standard.

Results ② : Every Masterkey was non-repeatable and its security was guaranteed.

Test Results ③ : ECC PKID Generator was found to be conforming ECC Algorithm.

VX-Lock

How We Differ? ❹ - With PKID Generation Tech guaranteed by CC

Common Criteria Certificate

is awarded to

WannaStation.com (M) Sdn Bhd

For

PKID ECC Generator v1.1

Type of Product: Software that is used to generate public and private keys based on a user definable and recognisable ID of ASCII characters or known as PKID.

Protection Profile Conformance: None

Evaluation Criteria: Common Criteria for Information Technology Security Evaluation Version 3.1 Revision 4

Evaluation Methodology: Common Methodology for Information Technology Security Evaluation Version 3.1 Revision 4

Malaysian Security Evaluation Facility (MySEF): CyberSecurity Malaysia MySEF

Assurance Package: EAL2

DR AMIRUDIN ABDUL WAHAB
MyCC Scheme Head

20 November 2013
Certificate No: 2013-009-C049

CyberSecurity MALAYSIA
An agency under MOSTI

MOSTI
Ministry of Science, Technology and Innovation

Tech. of Generating Public Key ID based on ECC algorithm