무엇이 다른가? ❶ - 지난 15년간의 주요 실적 및 신뢰도

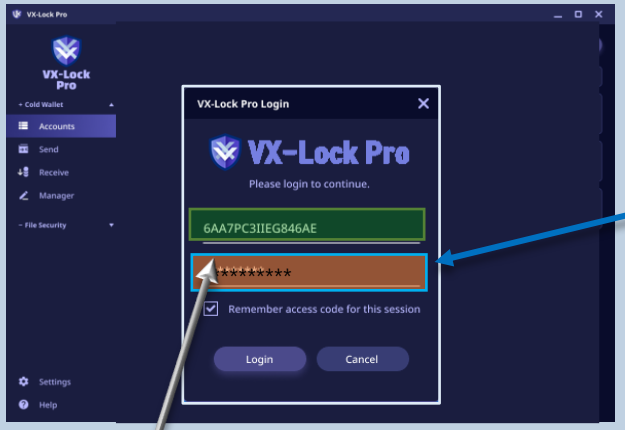
Military Grade Security (군사 등급 보안 제품)

- 2006년 말레이시아 총리실 산하 CGSO(정부 보안 담당 최고 공무원)의 기술 승인 취득
- 2008년 저장소의 파일 및 데이터 보호를 위한 Safe-All 특수 USB 드라이브 제품 한국 출시

- 타 부처와의 보안 통신을 위해 말레이시아 수상 산하 내각용 보안 이메일 시스템 통신 승인 및 배포
- MAMPU(말레이시아 중앙정보국)로부터 정부 기관에서 가장 신뢰성 있는 암호화 공급자로 인증 및 승인
- 2014년 TAQNIA(사우디 아라비아 왕립 개발투자 회사)와 보안 ID 발급 시스템의 POC 프로젝트 진행
- MasterCard 공인 전자 지갑 및 플랫폼용 개발업체 선정
- SGPMX(싱가포르 귀금속 거래소)용 전자 지갑 플랫폼 개발
- 말레이시아 기관 및 필리핀 경찰 정보국에 SypherSafe 보안 이동 통신 시스템 개발 및 공급

VX-Lock

무엇이 다른가? ❷ - ECC 320 bit 암호화 ID 및 접속 코드에 의한 로그인 보안



Text를 입력하여 만든 ID처럼 보이나, 이는 식별을 용이하기 위한 것일 뿐, ECC 320 bit로 암호화되어 임포팅된 보안 ID

① 보안 ID를 이용한 사용자/디바이스 인증 – 스마트폰의 경우, 전화번호, 이메일 등 유니크한 개인 정보와 IMEI 등 Device 정보를 ECC 320 bit로 암호화 후 임포팅

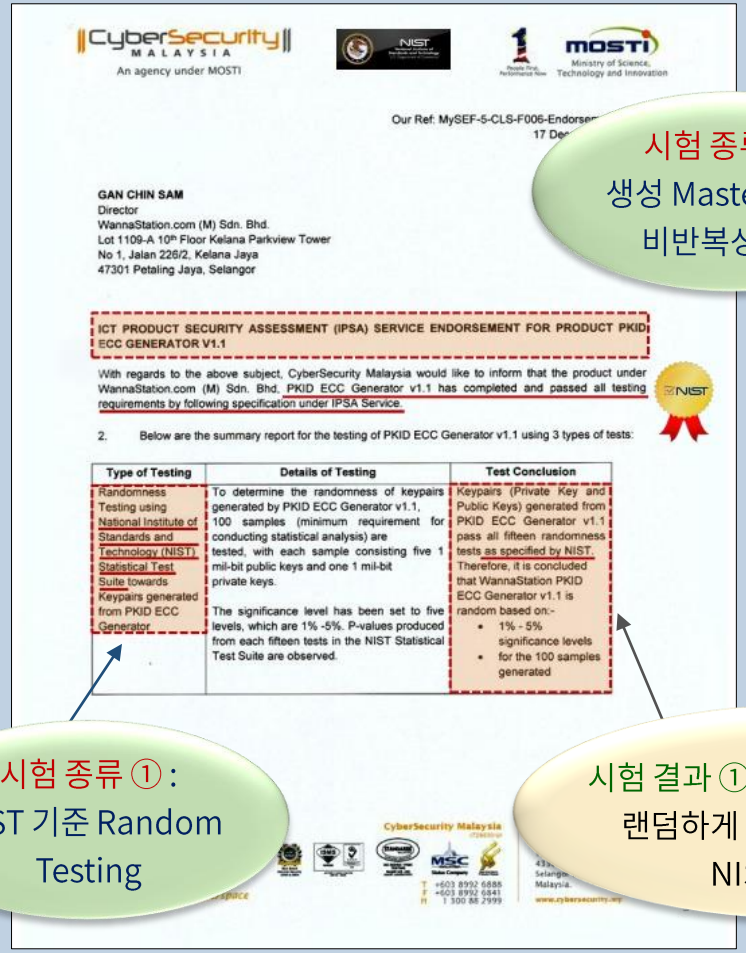
② 부인 방지 및 불법 복제 사용 차단 - 로그인 시 PKID로 사용자 및 디바이스 진위 확인과 사용자 위장/디바이스 불법 복제를 차단하는 전무후무한 기술

③ 2중의 네트워크 암호화 – AES 256 bit + SHA-3 256 bit 동시 적용 암호화 기술 구현

NIST National Institute of Standards and Technology | Common Criteria

VX-Lock

무엇이 다른가? ❸ - NIST 인증 보안 ID(PKID) 기술 적용



CyberSecurity MALAYSIA
An agency under MOSTI

MOSTI Ministry of Science, Technology and Innovation

Our Ref: MySEF-5-CLS-F006-Endorse
17 De

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

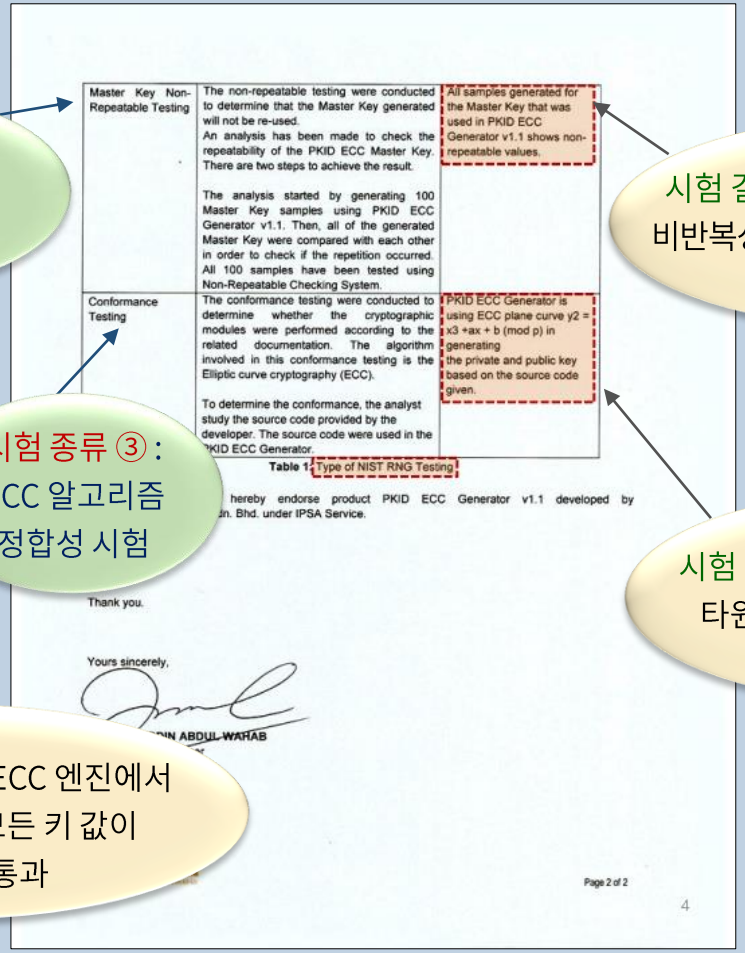
With regards to the above subject, CyberSecurity Malaysia would like to inform that the product under WannaStation.com (M) Sdn. Bhd. PKID ECC Generator v1.1 has completed and passed all testing requirements by following specification under IPSA Service.

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
n. Bhd. under IPSA Service.

Thank you.

Yours sincerely,

IN ABDUL WAHAB

Page 2 of 2

4

시험 종류 ② : 생성 Master Key의 비반복성 시험

시험 종류 ③ : ECC 알고리즘 정합성 시험

시험 종류 ① : NIST 기준 Random Testing

시험 결과 ① : PKID ECC 엔진에서 랜덤하게 생성된 모든 키 값이 NIST 기준 통과

시험 결과 ② : 모든 샘플 Master Key의 비반복성 입증 → 개별 생성 Master key의 보안성 담보 입증

시험 결과 ③ : ECC PKID 생성기가 타원곡선 이론 공식에 부합하여 기능함을 입증

VX-Lock

무엇이 다른가? ❹ - CC 인증 보안 ID 생성 엔진 기술 적용

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

ECC 알고리즘 기반 공개 키 ID 생성 엔진 기술 인증

VX-Lock