我们有何不同？ ❶ - 过去 15 年的参考资料和证书

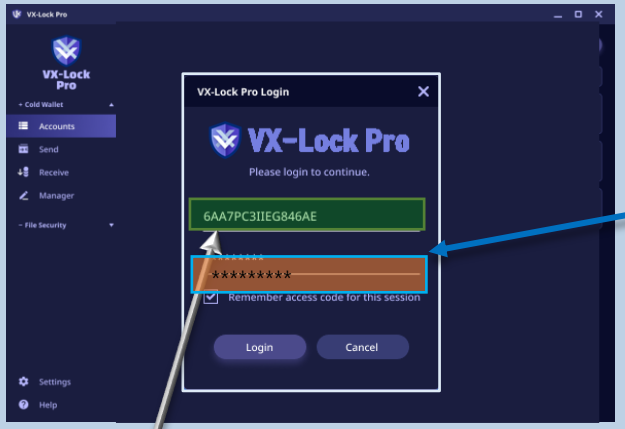
Military Grade Security (军用级安全)

- 2006 获得马来西亚总理府下属CGSO（首席政府安全官）的技术批准
- 2008 推出 Safe-All 专用 USB 驱动器产品，用于在韩国存储文件和数据保护
- 为马来西亚总理办公室批准和分发安全电子邮件系统通信，以便与其他部委进行安全通信。
- 经马来西亚中央情报局 (MAMPU) 认证和批准为政府机构最值得信赖的加密货币提供商
- 2014年与TAQNIA（沙特阿拉伯皇家发展投资公司）合作的安全ID发行系统POC项目
- 被选为万事达卡认证电子钱包和平台的开发商
- 为 SGPMX（新加坡贵金属交易所）开发电子钱包平台
- 为马来西亚机构和菲律宾警察情报局开发和供应 SypherSafe 安全移动通信系统




VX-Lock

我们有何不同？ ❷ - 登录安全和双重网络加密



看起来像是输入文字创建的ID，
但这只是为了方便识别，是用E
CC 320位加密的导入**安全ID**

① 使用安全ID的用户/设备身份验证–加密唯一的私人信息，例如电话号码， 电子邮件地址，IMEI等。⇨ 生成安全ID⇨导入以进行安全身份验证

② 不可抵赖和防复制–通过使用安全ID（PKID）进行用户登录，从本质上抵制伪造设备和用户的最新技术

③ 双网络加密–同时使用AES 256位和SHA-3 256位

NIST National Institute of Standards and Technology | Common Criteria

VX-Lock

我们有何不同？ ❸ - 具有 NIST 保证的 Secured ID (PKID)

CyberSecurity MALAYSIA
An agency under MOSTI

NIST

MOSTI
Ministry of Science, Technology and Innovation

Our Ref: MySEF-5-CLS-F006-Endor...
17...

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

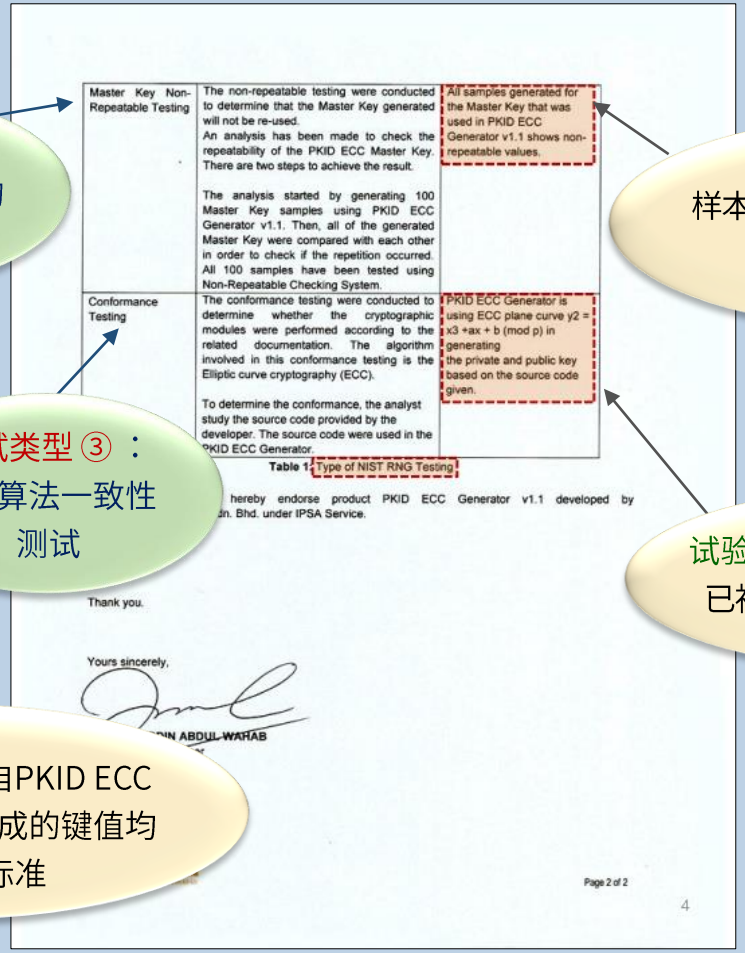
ICT PRODUCT SECURITY ASSESSMENT (IPSA) SERVICE ENDORSEMENT FOR PRODUCT PKID ECC GENERATOR V1.1

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
www.cybersecurity.my



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,

...IN ABDUL WAHAB

Page 2 of 2

4

测试类型①：
NIST标准随机
测试

试验结果①：来自PKID ECC
引擎的所有随机生成的键值均
通过NIST标准

测试类型②：
每个生成的主密钥的
不可重复性测试

试验结果②：
样本主密钥的不可重复性证明→
单独创建的主密钥的
安全性保证

测试类型③：
ECC算法一致性
测试

试验结果③：ECC PKID生成器
已被证明可以按照其曲线运行

VX-Lock

我们有何不同？ ❹ - 使用 CC 保证的 PKID 生成技术

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

基于ECC算法的公钥ID生成技术