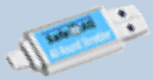
¿Cómo nos diferenciamos? ❶ - Referencias y Credenciales mayores de 15 años

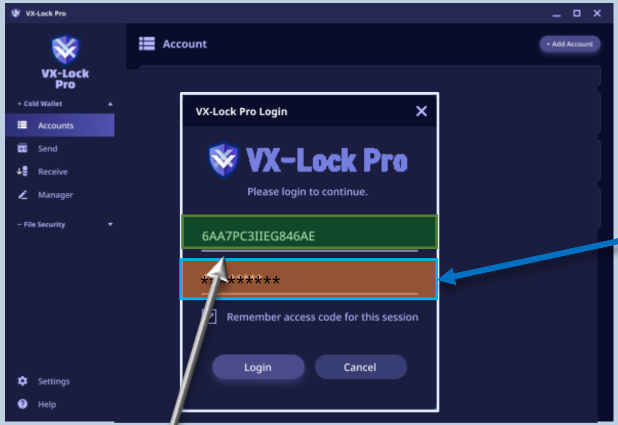
Military Grade Security (Seguridad de Grado Militar)

- Respaldo de tecnología por parte del Director de Seguridad del Gobierno (CGSO) del Departamento del Primer Ministro en Malasia, 2006
- Safe-All, la unidad USB especial para proteger archivos y datos almacenados se lanzó en la República de Corea, 2008



- Respaldo e implementación de la comunicación del Sistema de correo electrónico seguro para el Gabinete de Malasia bajo el Departamento del Primer Ministro para la comunicación segura con otros Ministerios
- Acreditación y respaldo de MAMPU como el proveedor de cifrado más confiable para todas las agencias gubernamentales bajo la Política Nacional de Criptografía
- Proyecto POC de Sistema de Emisión de Identificación Segura con TAQNIA (Empresa Saudita de Desarrollo e Inversión en Tecnología) en 2014
- Desarrollador de incorporación calificado de MasterCard para billetera electrónica y plataforma
- Desarrollador de la plataforma E-Wallet para la Bolsa de Metales Preciosos de Singapur (SGPMX): desarrollo continuo del sistema de comercio electrónico y backend
- Desarrollo y suministro del sistema de comunicación móvil seguro SypherSafe a varias agencias de Malasia y la inteligencia policial de Filipinas para su comunicación móvil altamente sensible

¿Cómo nos diferenciamos? ❷ - Seguridad de inicio de sesión y cifrado de red dual



VX-Lock Pro Login

VX-Lock Pro

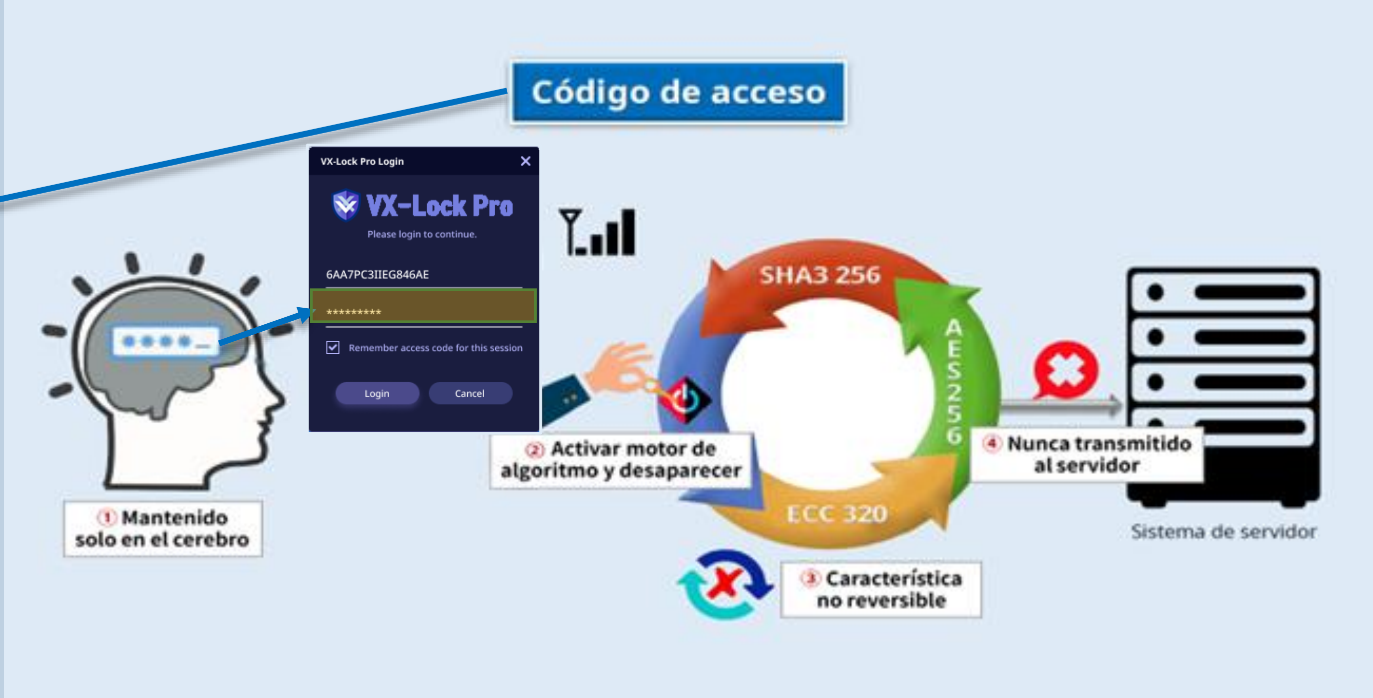
Please login to continue.

6AA7PC3IIEG846AE

****

☐ Remember access code for this session

Aunque la identificación de usuario parece texto sin formato, es una identificación segura encriptada con ECC de 320 bits e importada.



VX-Lock Pro Login

VX-Lock Pro

Please login to continue.

6AA7PC3IIEG846AE

****

☑ Remember access code for this session

Código de acceso
Login
Cancel
SHA3 256
AES256
ECC 320
① Mantenido solo en el cerebro
② Activar motor de algoritmo y desaparecer
③ Característica no reversible
④ Nunca transmitido al servidor
Sistema de servidor

① Autenticación de usuario / dispositivo con ID segura - Cifrado de información privada única como número de teléfono, dirección de correo electrónico, IMEI, etc. ⇨ Generación de ID segura ⇨ Importación para autenticación segura

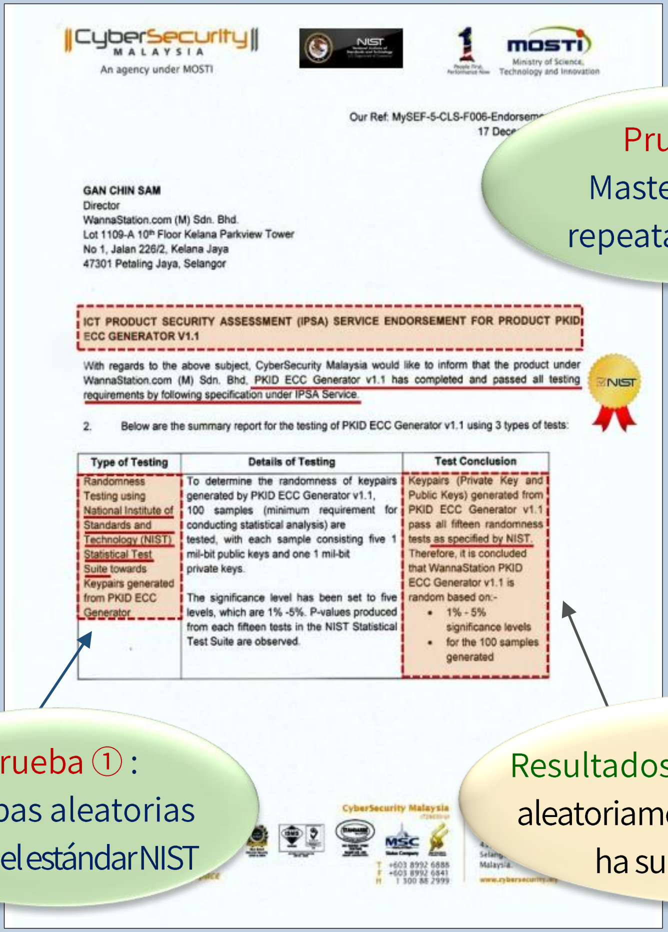
② No repudio y anticopia: tecnología de punta contra dispositivos y usuarios falsos intrínsecamente haciendo que el usuario inicie sesión con Secure ID (PKID)

③ Cifrado de red dual: utilizando AES 256 bit y SHA-3 256 bit al mismo tiempo

NIST National Institute of Standards and Technology | Common Criteria

VX-Lock

¿Cómo nos diferenciamos? ❸ - Con ID segura (PKID) garantizada por NIST



CyberSecurity MALAYSIA
An agency under MOSTI

NIST

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.

NIST

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

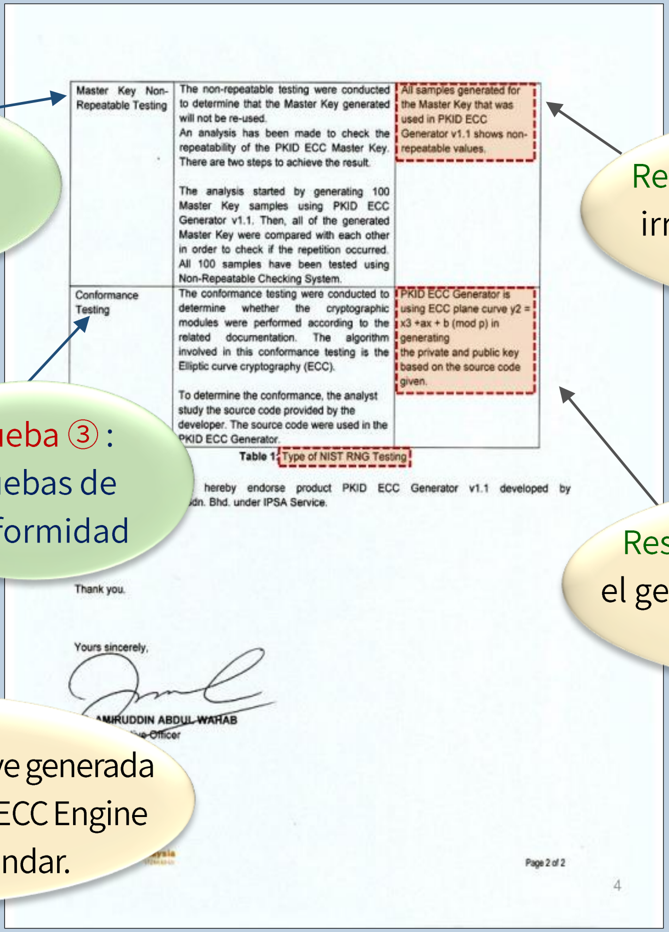
T +603 8992 6888
F +603 8992 6841
H 1 300 88 2999

Selang
Malaysia.
www.cybersecurity.my

Prueba ①:
Pruebas aleatorias según el estándar NIST

Resultados ①: Cada clave generada aleatoriamente por PKID ECC Engine ha superado su estándar.

Prueba ②:
Masterkey Non-repeatable Testing



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 (mod 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,

AMIRUDDIN ABDUL WAHAB
ive Officer

Page 2 of 2

4

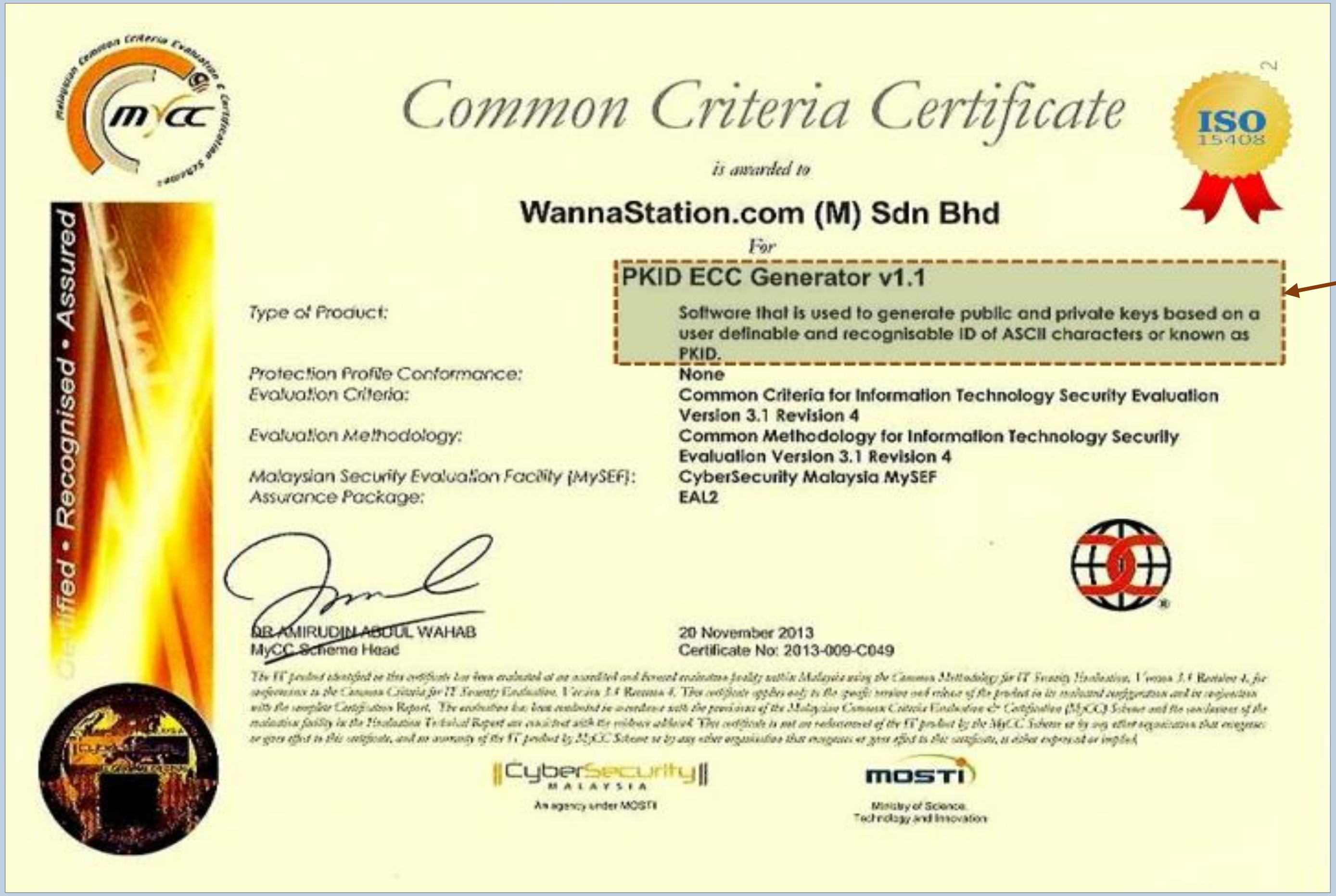
Resultados ② Cada Masterkey era irrepetible y su seguridad estaba garantizada.

Prueba ③:
Pruebas de conformidad

Resultados ③: Se encontró que el generador ECC PKID cumple con el algoritmo ECC..

VX-Lock

¿Cómo nos diferenciamos? ❹ - Con PKID Generation Tech garantizado por CC



Malaysian Common Criteria Evaluation & Certification Scheme

MyCC

Common Criteria Certificate

ISO 15408

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

Certified • Recognised • Assured

DR AMIRUDIN ABDUL WAHAB
MyCC Scheme Head

20 November 2013
Certificate No: 2013-009-C049

The IT product identified in this certificate has been evaluated at an accredited and licensed evaluation facility within Malaysia using the Common Methodology for IT Security Evaluation, Version 3.1 Revision 4, for conformance to the Common Criteria for IT Security Evaluation, Version 3.1 Revision 4. This certificate applies only to the specific version and release of the product in its evaluated configuration and in conjunction with the complete Certification Report. The evaluation has been conducted in accordance with the provisions of the Malaysian Common Criteria Evaluation & Certification (MyCC) Scheme and the conclusions of the evaluation facility in the Evaluation Technical Report are consistent with the evidence adduced. This certificate is not an endorsement of the IT product by the MyCC Scheme or by any other organisation that recognises or gives effect to this certificate, and no warranty of the IT product by MyCC Scheme or by any other organisation that recognises or gives effect to this certificate, is either expressed or implied.

CyberSecurity MALAYSIA
An agency under MOSTI

MOSTI
Ministry of Science, Technology and Innovation

Tecnología de la generación de ID de clave pública basada en el algoritmo ECC