Wannastation.com (M) Sdn. Bhd.

PKID ECC Generator v1.1

PKID ECC Generator v1.1 Security Target v1.0

(PKIDECCGEN-ST-v1.0-071013)

7 October 2013

DOCUMENT HISTORY

Version Number	Version Date	Change Details
0.1	29 April 2013	Initial version
0.2	20 May 2013	Updates on TOE physical scope, Security Functional Requirement etc.
0.3	19 July 2013	Updates after receive EOR1 from evaluator.
0.4	16 August 2013	Updates after receive EOR5
0.5	12 September 2013	Updates : -Scope includes manual key-in but not automatic detection, server is standalone and not connected to any network (EOR6) -Added assumptions and security objective for objective environment. -Update FCS_CKM.1 (B) SFR
1.0	7 October 2013	Initial Release

Table of Contents

1 Document introduction

1.1 DOCUMENT CONVENTIONS

The following conventions have been applied in this document:
Security Functional Requirements – Part 2 of the CC defines the approved set of operations that may be applied to functional requirements: assignment, selection, and iteration.
1. The **refinement** operation is used to add detail to a requirement, and thus further restricts a requirement. Refinement of security requirements is denoted by **bold underline text**.
2. The **selection** operation is used to select one or more options provided by the CC in stating a requirement. Selections are denoted by *italicized text* in square brackets, [*selection value*].
3. The **assignment** operation is used to assign a specific value to an unspecified parameter, such as the length of a password. Assignment is indicated by showing the value in square brackets, [**assignment value**] in **bold**.
4. The **iteration** operation is used when a component is repeated with varying operations. Iteration is denoted by showing the iteration name in parenthesis following the component identifier, (iteration name).

1.2 TERMINOLOGY

Table 1: Terminology

Acronym	Meaning
CC	Common Criteria
FIPS PUB	Federal Information Processing Standards Publication
EAL	Evaluation Assurance Level
PP	Protection Profile
SAR	Security Assurance Requirements
SFR	Security Functional Requirements
ST	Security Target
TOE	Target of Evaluation
TSC	TSF Scope of Control
TSF	TOE Security Function
OSP	Organizational Security Policy
TSS	TOE Summary Specification

1.3 REFERENCES

- Common Criteria Part 1 Version 3.1 Revision 4
- Common Criteria Part 2 Version 3.1 Revision 4
- Common Criteria Part 3 Version 3.1 Revision 4
- Common Methodology for Information Technology Security Evaluation (CEM) version 3.1 Revision 4

1.4 DOCUMENT ORGANIZATION

This ST contains:

- TOE Description: Pr*ovides an overview o*f the TOE security functions and describes the physical and logical scope for the TOE
- TOE Security Problem Definition: Describes the threats, organizational security policies, and assumptions that pertain to the TOE and the TOE environment.
- TOE Security Objectives: Identifies the security objectives that are satisfied by the TOE and the TOE environment.
- TOE Security Functional Requirements: Presents the Security Functional Requirements (SFRs) met by the TOE
- TOE Security Assurance Requirement: Presents the Security Assurance Requirements (SARs) met by the TOE
- TOE Summary Specification: Describes the security functions provided by the TOE to satisfy the security requirements and objectives

2 INTRODUCTION

2.1 ST AND TOE REFERENCE

Table 2: ST and TOE Reference

ST Title	PKID ECC Generator v1.1 Security Target
ST Version	1.0
TOE Identification	PKID ECC Generator v1.1
CC Identification	Common Criteria Version 3.1 Revision 4
Assurance Level	EAL2
ST Author	WannaStation.com (M) Sdn. Bhd.
Keyword	Key Generator

2.2 TOE OVERVIEW

2.2.1 Usage and major security features of the TOE.

PKID ECC Generator v1.1 is a system that generates public and private keys based on a user definable and recognizable ID of ASCII characters (PKID).. Using the Key Generation Module, the system uses proprietary technology to create a public and private key which has distinctive and unique attributes of each user. A user may choose a PKID unique to himself or herself, such as PC/Notebook MAC address, IMEI number and email address. A chosen PKID will become the seed to generate a public and private key through a sophisticated series of key generation processes. The generated public and private keys are tied to the chosen PKID. Using algorithm based on elliptic curve encryption algorithm, much smaller key size can be used and desirable as it allows the application on PC, smart phones or mobile communication devices for multi-function security applications. Depending on the PKID, the public and private keys generated by the TOE can be used on various platforms:

Table 3: Input and Output Platform

PKID	Output Platform
PC/Notebook MAC address	PC/Notebook (for audio file encryption/decryption)
IMEI number	Mobile phone (for file encryption/decryption, not SMS)
Email address	PC/Notebook (for file encryption/decryption)

This system is also unique as during customization of the system, input from the client organization will be used to generate Master Key in order to customize the PKID ECC Generator for that specific client. This is particularly important to ensure that no one can duplicate the system without having the same input from the client.

The system will enforce authentication before the administrator can use the system using the Authentication Module. Administrator can perform management functions such as changing of password, generation of public/private keys and exporting keys using the Admin Module.

2.2.2 TOE Type

PKID ECC Generator v1.1 is a system for the generation of public and private keys that is created based on a user definable and recognizable ID of ASCII characters.

2.2.3 Required non-TOE hardware, software and firmware

Table 4: Required non-TOE hardware, software and firmware

Item	Description
Hardware	-A machine running Windows 2003 Server with min Intel Xeon 2.33Ghz processor and min 2GB RAM. -DVD/CD drive and Blank recordable CDs (for storing generated

	Master Key)
Software	-Microsoft Visual C++ version 6.0. -CD Burner software (for burning Master Key to CD) -Document to PDF converter software that works by creating a virtual printer that prints to PDF files (for printing private and public key access codes). -PDF Viewer software.

2.3 TOE DESCRIPTION

This section primarily addresses the physical and logical components of the TOE included in the evaluation.

2.3.1 Physical scope of the TOE

The TOE physically consists of:

- Software: PKID ECC Generator v1.1
- Guidance:
    a) PKID ECC Generator v1.1 Preparative Guidance – guide for setting of the Master Key and customization of the TOE.
    b) PKID ECC Generator v1.1 Administrator Guide – guide for operating the TOE.

The TOE involves 2 components (refer Figure 1) :

1. Customization of the PKID ECC Generator

   During customization of the generator, input from the client organization will be used to generate Master Key in order to customize the PKID ECC Generator for that specific client.

2. Customized PKID ECC Generator

   After customization in step 1, the customized generator is able to generate public and private key which has distinctive and unique attributes of each user based on a user definable and recognizable ID of ASCII characters (PKID) inputted either by manual key-in or automatic detection. However, the TOE scope covered for this evaluation is manual key-in and the TOE resides in a standalone server which is not connected to any network. A chosen PKID by each user will become the seed to generate the keys. The generated public and private keys are tied to the chosen PKID.

   The scope also covers the output produced by the Key Generation Module which are the private key, public key and its access code. Taking MAC address for the PKID as an example, files encrypted using the public key generated for a MAC address can only be decrypted using the corresponding private key on the PC/Notebook with the same MAC address. To be able to use the keys for

encryption and decryption, users shall use client application provided by the developer which supports these features.

Note1: client application is not included in the TOE scope. However, they are used for testing the encryption/decryption using public and private keys generated by the PKID ECC Generator.

Note 2: The revocation and recovery of keys are not covered in the TOE scope.

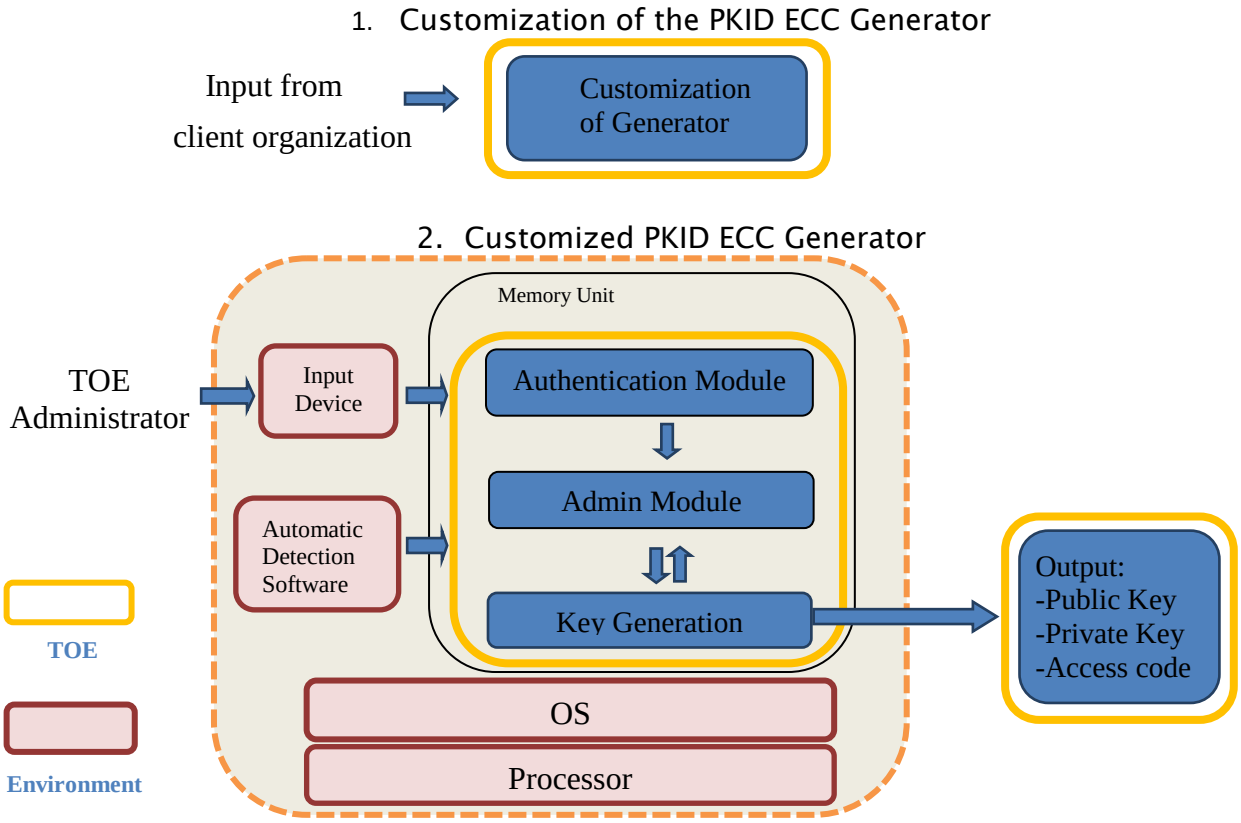

Figure 1: TOE Components

Note: Automatic Detection Software is software provided by Wannastation.com (M) Sdn. Bhd to be used for PKID inputted by automatic detection. However input by automatic detection is not in TOE scope.

2.3.2 Logical scope of the TOE

The logical scope of TOE is described based on several security functional requirements as below.

Table 5: TOE Security Function map to TOE Scope

Security Function	TOE Scope Description
Authentication	During Customization of the PKID ECC Generator, authentication is required to import Master Key into the generator. In the Customized PKID ECC Generator, the TOE can be accessed only after the user (TOE Administrator) had been successfully authenticated.
Security Management	Management of functions during customization of the generator and in the customized generator itself.
Cryptographic Support	During Customization of the PKID ECC Generator, input from the client organization will be used to generate Master Key in order to customize the generator for that specific client. In the Customized PKID ECC Generator, generation of public and private keys (together with access code) is using specified encryption algorithm.

3 CONFORMANCE CLAIMS

3.1 COMMON CRITERIA CLAIMS

The following conformance claims are made for the TOE and ST:

- The ST and the TOE are Common Criteria conformant to **Common Criteria version 3.1 Revision 4.**
- The ST and the TOE are conformant to Common Criteria **Part 2.**
- The ST and the TOE are conformant to Common Criteria **Part 3.**
- The TOE conforms to **EAL2** .
- The ST and TOE claims no conformance to a Protection Profile.

3.2 PP CONFORMANCE CLAIMS RATIONALE

The conformance claim of this ST does not claim conformance to any Protection Profile. Hence, there are no elements to be covered in the conformance claim rationale.

4 TOE SECURITY PROBLEM DEFINITION

4.1 ASSUMPTION

These assumptions are made to ensure the security of the TOE and its deployed environment.

Table 6: Assumptions

A.PHY	The TOE and its environment are physically secure and managed by authorized TOE Administrator.
A.ADMIN	Authorized TOE Administrator is non-hostile, keeps the Master Key CD in a secure place and follows guidance documentation accordingly; however, TOE Administrators is not free from human error and mistakes.
A.INPUT	Input(PKID) received from user as the seed for the generation of public and private keys is in good condition and has not been tampered with.
A.DESTRUCT	The TOE environment will destroy cryptographic keys generated by the TOE.
A.CLIENT	Client application (not in TOE scope) will handle correct operation of encryption and decryption using keys generated by the TOE.
A.REVOKE	The TOE environment will handle revocation of the cryptographic keys.
A.SECURE	The operating system where the TOE executed and all third party applications installed are trusted and do not perform malicious actions to compromise the operation of TOE. The TOE resides in a standalone server which is not connected to any network.

4.2 THREATS

Table 7: Threats

T.DUPLICATE	An attacker can duplicate the TOE and generate keys for users on behalf of the TOE administrator.
T.KEYS	An attacker can generate a random list of public and private keys and use the keys on behalf of the user.
T. UNAUTHORIZED	An unauthorized person may attempt to bypass the TOE access controls.

4.3 ORGANIZATIONAL SECURITY POLICIES

The Organizational Security Policies (OSP) is imposed by an organization to secure the TOE and its environment.

Table 8: OSP

OSP.ROLE	Only authorized individuals assigned by the organization have access to the TOE.

5 TOE SECURITY OBJECTIVES

5.1 SECURITY OBJECTIVE FOR THE TOE

The TOE provides security functionality to solve a certain part of the problem defined by the security problem definition. This part wise solution is called the security objectives for the TOE and consists of a set of objectives that the TOE should achieve in order to solve its part of the problem.

Table 9: TOE Security Objectives

O.CUSTOMIZE	The TOE's key generator shall be customized based on input received from the client organization.
O.UNIQUE	The TOE shall utilize ASCII characters as an input to generate unique public and private keys for each user.
O.AUTH	The TOE shall authenticate the Administrator before providing access to the TOE.
O.FUNCTION	The TOE shall provide the administrator with several management functions.

5.2 SECURITY OBJECTIVE FOR THE OPERATIONAL ENVIRONMENT

The security objectives for the TOE operational environment as following:

Table 10: Security objectives for the TOE operational environment

OE.PHY	The TOE and its environment shall be physically secure.
OE.ADMIN	Authorized TOE Administrator shall be non-hostile, keeps the Master Key CD in a secure place and follows guidance documentation accordingly; however, TOE Administrators is not free from human error and mistakes.
OE.INPUT	Input received from user as the seed for the generation of public and private keys shall be in good condition and has not been tampered with.

OE.DESTRUCT	The TOE environment shall destroy cryptographic keys generated by the TOE.
OE.CLIENT	Client application (not in TOE scope) shall handle correct operation of encryption and decryption using keys generated by the TOE.
OE.REVOKE	The TOE environment shall handle revocation of the cryptographic keys.
OE.SECURE	The operating system where the TOE executed and all third party applications installed shall be trusted and shall not perform malicious actions to compromise the operation of TOE. The TOE shall reside in a standalone server which is not connected to any network.

5.3 SECURITY OBJECTIVES RATIONALE

This section provides mapping between TOE Security Objectives to threat and the tracings from Security Objectives to Threats, Assumptions and Policies.

Table 11 : Mappings of Security Objectives and Objectives for Environment to Threats/Assumptions/Policy

	T.DUPLICATE	T.KEYS	T. UNAUTHORIZED	A.PHY	A.ADMIN	A.INPUT	A.DESTRUCT	A.CLIENT	A.REVOKE	A.SECURE	OSP.ROLE
O.CUSTOMIZE	X										
O.UNIQUE		X									
O.AUTH			X								X
O.FUNCTION			X								
OE.PHY				X							
OE.ADMIN					X						
OE.INPUT						X					
OE.DESTRUCT							X				
OE.CLIENT								X			
OE.REVOKE									X		
OE.SECURE										X	

5.3.1 Security objectives rationale for the TOE

Table 12: Mapping of TOE Security Objective to Threats and Organization Policy

Threats/OSP	Security Objectives	Rationale
T.DUPLICATE An attacker can duplicate the TOE and generate keys for users on behalf of the TOE administrator.	O.CUSTOMIZE The TOE's key generator shall be customized based on input received from the client organization.	This security objective counters the threat because it prevents an attacker from duplicating the TOE and then generating keys for users on behalf of the TOE administrator.
T.KEYS An attacker can generate a random list of public and private keys and use the keys on behalf of the user.	O.UNIQUE The TOE shall utilize ASCII characters as an input to generate unique public and private keys for each user.	This security objective counters the threat because generated public and private keys are unique for each user.
T. UNAUTHORIZED An unauthorized person may attempt to bypass the TOE access controls and gain access to the TOE.	O.AUTH The TOE shall authenticate the Administrator before providing access to the TOE. O.FUNCTION The TOE shall provide the administrator with several management functions.	This security objective counters the threat because TOE will prevent unauthorized person to access the TOE functions. Only TOE authorized administrator shall have access to the TOE.
OSP.ROLE Only authorized individuals assigned by the organization have access to the TOE.	O.AUTH The TOE shall authenticate the Administrator before providing access to the TOE.	This security objective counters the OSP because individuals who are not authorized administrators cannot access the TOE.

5.3.2 Security objectives rationale for the Operational Environment

Table 13: Mapping of Security Objective for the Operational Environment to Threats/ Organizational Security Policy/Assumption

Assumptions	Security Objectives	Rationale
A.PHY The TOE and its environment are physically secure and managed by authorized TOE Administrator.	**OE.PHY** The TOE and its environment shall be physically secure.	This security objective counters assumption because the TOE and its environment shall be physically secure.
A.ADMIN Authorized TOE Administrator is non-hostile, keeps the Master Key CD in a secure place and follows guidance documentation accordingly; however, TOE Administrators is not free from human error and mistakes.	**OE.ADMIN** Authorized TOE Administrator shall be non-hostile, keeps the Master Key CD in a secure place and follows guidance documentation accordingly; however, TOE Administrators is not free from human error and mistakes.	This security objective counters assumption because authorized TOE Administrator shall be non-hostile, keeps the Master Key CD in a secure place and follows guidance documentation accordingly; however, TOE Administrators is not free from human error and mistakes.
A.INPUT Input(PKID) received from user as the seed for the generation of public and private keys is in good condition and has not been tampered with.	**OE.INPUT** Input(PKID) received from user as the seed for the generation of public and private keys shall be in good condition and has not been tampered with.	This security objective counters assumption because input(PKID) received from user as the seed for the generation of public and private keys shall be in good condition and has not been tampered with.
A.DESTRUCT The TOE environment will destroy cryptographic keys generated by the TOE.	**OE.DESTRUCT** The TOE environment shall destroy cryptographic keys generated by the TOE.	This security objective counters assumption because the TOE environment shall destroy cryptographic keys generated by the TOE.
A.CLIENT Client application (not in TOE scope) will handle correct operation of encryption and decryption using keys generated by the TOE.	**OE.CLIENT** Client application (not in TOE scope) shall handle correct operation of encryption and decryption using keys generated by the TOE.	This security objective counters assumption because client application (not in TOE scope) shall handle correct operation of encryption and decryption using keys generated by the TOE.
A.REVOKE	**OE.REVOKE**	This security objective counters assumption

The TOE environment will handle revocation of the cryptographic keys.	The TOE environment shall handle revocation of the cryptographic keys.	because the TOE environment shall handle revocation of the cryptographic keys.
A.SECURE The operating system where the TOE executed and all third party applications installed are trusted and do not perform malicious actions to compromise the operation of TOE. The TOE resides in a standalone server which is not connected to any network.	**OE.SECURE** The operating system where the TOE executed and all third party applications installed shall be trusted and shall not perform malicious actions to compromise the operation of TOE. The TOE shall reside in a standalone server which is not connected to any network.	This security objective counters assumption because the operating system where the TOE executed and all third party applications installed shall be trusted and shall not perform malicious actions to compromise the operation of TOE. The TOE shall reside in a standalone server which is not connected to any network.

6 EXTENDED COMPONENTS DEFINITION

There are no extended components defined for this TOE.

7 SECURITY REQUIREMENTS

7.1 OVERVIEW

This section contains the security functional requirements (SFRs) for the TOE. The summary of SFRs is listed in following table.

Table 14: Security Functional Requirements for the TOE

Component	Component Name
Class FIA : Identification and Authentication	
FIA_UAU.2	User authentication before any action
FIA_UAU.2 (Customize)	User authentication before any action (Customize)
FIA_SOS.1	Verification of secrets
Class FMT : Security Management	
FMT_SMF.1	Specification of management functions
FMT-SMF.1 (Customize)	Specification of management functions (Customize)
Class FCS : Cryptographic support	
FCS_CKM.1 (A)	Cryptographic key generation (Master Key)
FCS_CKM.1 (B)	Cryptographic key generation (Public and private key)
FCS_CKM.2 (A)	Cryptographic key distribution (Master Key)
FCS_CKM.2 (B)	Cryptographic key distribution (Public and private key)

7.2 TOE SECURITY FUNCTIONAL REQUIREMENTS

Class FIA: Identification and Authentication

FIA_UAU.2 User authentication before any action

Hierarchical to:	FIA_UAU.1 Timing of authentication
Dependencies:	FIA_UID.1 Timing of identification
FIA_UAU.2.1	The TSF shall require each user to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that user.
Notes:	None.

FIA_UAU.2 (Customize) User authentication before any action

Hierarchical to:	FIA_UAU.1 Timing of authentication
Dependencies:	FIA_UID.1 Timing of identification
FIA_UAU.2.1	The TSF shall require each user to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that user.
Notes:	None.

FIA_SOS.1 Verification of secrets

Hierarchical to:	No other components.
Dependencies:	No dependencies.
FIA_SOS.1.1	The TSF shall provide a mechanism to verify that secrets meet [**minimum 8 characters**].
Notes:	None.

Class FMT : Security Management

FMT_SMF.1 Specification of management functions

Hierarchical to:	No other components.
Dependencies:	No dependencies.

FMT_SMF.1.1	The TSF shall be capable of performing the following management functions: [**change administrator password, generate public and private keys, export keys**].
Notes:	None.

FMT_SMF.1 (Customize) Specification of management functions

Hierarchical to:	No other components.
Dependencies:	No dependencies.
FMT_SMF.1.1	The TSF shall be capable of performing the following management functions: [**set Master Key access code**].
Notes:	None.

Class FCS : Cryptographic support

FCS_CKM.1 (A) Cryptographic key generation (Master Key)

Hierarchical to:	No other components.
Dependencies:	[FCS_CKM.2 Cryptographic key distribution, or FCS_COP.1 Cryptographic operation] FCS_CKM.4 Cryptographic key destruction
FCS_CKM.1.1	The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm [**non-repeatable**] and specified cryptographic key sizes [**320 bit**] that meet the following: [**none**].
Notes:	None.

FCS_CKM.1 (B) Cryptographic key generation (Public and private key)

Hierarchical to:	No other components.
Dependencies:	[FCS_CKM.2 Cryptographic key distribution, or FCS_COP.1 Cryptographic operation] FCS_CKM.4 Cryptographic key destruction
FCS_CKM.1.1	The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm **[standard**

	Elliptical Curve Cryptography using plane curve] and specified cryptographic key sizes [**320 bit**] that meet the following: [**NIST Statistical Test Suite**].
Notes:	NIST Statistical Test Suite is for testing the randomness of the cryptographic keys generated by the TOE.

FCS_CKM.2 (A) Cryptographic key distribution (Master Key)

Hierarchical to:	No other components.
Dependencies:	[FDP_ITC.1 Import of user data without security attributes, or FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation] FCS_CKM.4 Cryptographic key destruction
FCS_CKM.2.1	The TSF shall distribute cryptographic keys in accordance with a specified cryptographic key distribution method [**Master Keys injected into generator**] that meets the following: **[none**].
Notes:	None.

FCS_CKM.2 (B) Cryptographic key distribution (Public and private key)

Hierarchical to:	No other components.
Dependencies:	[FDP_ITC.1 Import of user data without security attributes, or FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation] FCS_CKM.4 Cryptographic key destruction
FCS_CKM.2.1	The TSF shall distribute cryptographic keys in accordance with a specified cryptographic key distribution method [**designated folders for storing newly generated keys and for exported keys whereby user lost the keys**] that meets the following: **[none]**.
Notes:	The keys stored in the designated folders will then be copied to storage medium such as CD, thumbdrive etc. The process of copying the keys and the storage medium is not in the scope of evaluation.

7.3 TOE SECURITY ASSURANCE REQUIREMENTS

This ST claims compliance to the assurance requirements from the CC EAL2 assurance package. This EAL was chosen based on the security problem definition and the security objectives for the TOE. The chosen assurance level is consistent with the claimed threat environment.

The following table summarized the TOE assurance requirements drawn from CC Part 3.

Table 15: TOE assurance requirements

Assurance Class	Assurance components
ADV: Development	ADV_ARC.1 Security architecture description
	ADV_FSP.2 Security-enforcing functional specification
	ADV_TDS.1 Basic design
AGD: Guidance documents	AGD_OPE.1 Operational user guidance
	AGD_PRE.1 Preparative procedures
ALC: Life-cycle support	ALC_CMC.2 Use of a CM system
	ALC_CMS.2 Parts of the TOE CM coverage
	ALC_DEL.1 Delivery procedures
ASE: Security Target evaluation	ASE_CCL.1 Conformance claims
	ASE_ECD.1 Extended components definition
	ASE_INT.1 ST introduction
	ASE_OBJ.2 Security objectives
	ASE_REQ.2 Derived security requirements
	ASE_SPD.1 Security problem definition
	ASE_TSS.1 TOE summary specification

Assurance Class	Assurance components
ATE: Tests	ATE_COV.1 Evidence of coverage
	ATE_FUN.1 Functional testing
	ATE_IND.2 Independent testing – sample
AVA: Vulnerability assessment	AVA_VAN.2 Vulnerability analysis

7.4 SECURITY REQUIREMENTS RATIONALE

7.4.1 Tracing of SFR to TOE security objectives

The functional and assurance requirements presented in this ST are mutually supportive and their combinations meet the stated security objectives. The security requirements were derived according to the general model presented in Part 1 of the Common Criteria. Table 16 illustrates the mapping between the security requirements and the security objectives.

Table 16: Mappings of SFR and TOE Security Objectives

	O.CUSTOMIZE	O.UNIQUE	O.AUTH	O.FUNCTION
FIA_UAU.2			X	
FIA_UAU.2 (Customize)	X			
FIA_SOS.1			X	
FMT_SMF.1				X
FMT_SMF.1 (Customize)	X			
FCS_CKM.1 (A)	X			
FCS_CKM.1 (B)		X		
FCS_CKM.2 (A)	X			
FCS_CKM.2 (B)		X		

Table 17: Rationale for SFR mapped to TOE Security Objectives

TOE Security Objectives	SFRs	Rationale
O.CUSTOMIZE The TOE's key generator shall be customized based on input received from the client organization.	FCS_CKM.1 (A)	Based on input received from client organization, Master Key is generated for the customization of the key generator. This SFR specifies the key generation algorithm and key size to be used for the Master Key generation. It traces back to this objective.
	FCS_CKM.2 (A)	This SFR specifies how the generated Master Key will be distributed. It traces back to this objective.
	FMT_SMF.1 (Customize)	This SFR identifies that the management functions available during customization of the TOE is set Master Key access code. It traces back to this objective.
	FIA_UAU.2 (Customize)	This SFR requires successful authentication for importing Master Key into the generator for customization. It traces back to this objective.
O.UNIQUE The TOE shall utilize ASCII characters as an input to generate unique public and private keys for each user.	FCS_CKM.1 (B)	This SFR specifies the key generation algorithm and key size to be used. It traces back to this objective.
	FCS_CKM.2 (B)	This SFR specifies how the generated keys will be distributed. It traces back to this objective.
O.AUTH The TOE shall authenticate the Administrator before providing access to the TOE.	FIA_UAU.2	This SFR requires administrator to be successfully authenticated before allowed access to the TOE. It traces back to this objective.
	FIA_SOS.1	This SFR requires verification of password supplied by the administrator to be min 8 characters. It traces back to this objective.
O.FUNCTION The TOE shall provide the administrator with several management functions.	FMT_SMF.1	This SFR identifies that the management functions available in the TOE is change administrator password and generate public and private keys. It traces back to this objective.

7.4.2 SFR dependency rationale

This section provides a demonstration that all of the functional requirements of the Security Functional Requirements included within the TOE have been satisfied.

Table 18: SFR dependency rationale

SFR	Dependency	Justification
FIA_UAU.2	FIA_UID.1	Justification for not meeting FIA_UID.1 No identification is needed because authentication is for the username created for TOE Administrator during customization.
FIA_UAU.2 (Customize)	FIA_UID.1	Justification for not meeting FIA_UID.1 No identification is needed because authentication is for Master Key's access code.
FIA_SOS.1	None	No dependencies to satisfy.
FMT_SMF.1	None	No dependencies to satisfy.
FMT_SMF.1 (Customize)	None	No dependencies to satisfy.
FCS_CKM.1 (B)	a) [FCS_CKM.2 Cryptographic key distribution or FCS_COP.1 Cryptographic operation] b) FCS_CKM.4 Cryptographic key destruction	Satisfied with FCS_CKM.2 (B) Justification for not meeting FCS_CKM.4 The dependency for FCS_CKM.4 is not met because the cryptographic algorithms are only used for generation of keys. The TOE does not conduct key destruction.

FCS_CKM.2 (B)	a) [FDP_ITC.1 Import of user data without security attributes or FDP_ITC.2 Import of user data with security attributes or FCS_CKM.1 Cryptographic key generation] b) FCS_CKM.4 Cryptographic key destruction	Satisfied with FCS_CKM.1 (B). Justification for not meeting FCS_CKM.4 The dependency for FCS_CKM.4 is not met because the cryptographic algorithms are only used for generation of keys. The TOE does not conduct key destruction. It is provided by the environment.
FCS_CKM.1 (A)	a) [FCS_CKM.2 Cryptographic key distribution or FCS_COP.1 Cryptographic operation] b) FCS_CKM.4 Cryptographic key destruction	Satisfied with FCS_CKM.2 (A) Justification for not meeting FCS_CKM.4 The dependency for FCS_CKM.4 is not met because the TOE does not conduct key destruction. It is provided by the environment.
FCS_CKM.2 (A)	a) [FDP_ITC.1 Import of user data without security attributes or FDP_ITC.2 Import of user data with security attributes or FCS_CKM.1 Cryptographic key generation] b) FCS_CKM.4 Cryptographic key destruction	Satisfied with FCS_CKM.1 (A) Justification for not meeting FCS_CKM.4 The dependency for FCS_CKM.4 is not met because the TOE does not conduct key destruction. It is provided by the environment.

7.4.3 SAR justification

The security assurance requirements that was selected for the TOE is from the CC EAL2 package. This EAL was chosen based on the security problem definition and the security objectives for the TOE. The chosen assurance level is consistent with the claimed threat environment.

8 TOE SUMMARY SPECIFICATION

This section provides the TOE summary specification, a high-level definition of the security functions claimed to meet the functional and assurance requirements.

PKID ECC Generator v1.1 is a system that generates public and private keys based on a user definable and recognizable ID of ASCII characters (PKID). The TOE resides in a standalone server which is not connected to any network.

8.1 AUTHENTICATION

During customization of the PKID ECC Generator, the generated Master Key from the CD shall be imported into the generator which resulting in a customized generator for that client. To import, the Master Key access code is required to be entered for authentication. This covers FIA_UAU.2 (Customize).

In the customized PKID ECC Generator, the TOE provides the capability to prevent access by unauthorized user. TOE administrator is able to access TOE by providing the password. The TOE requires authorized administrator to be authenticated first before allowing any other actions on behalf of that authorized administrator. This covers FIA_UAU.2. The TOE also provides a mechanism to verify that passwords entered are min 8 characters. This covers FIA_SOS.1.

Security Functional Requirements Satisfied:

- FIA_UAU.2 (Customize)
- FIA_UAU.2
- FIA_SOS.1

8.2 SECURITY MANAGEMENT

During customization of the PKID ECC Generator, after Master Key is generated using specified cryptographic key generation as stated in 8.3 a), an access code is set for the generated Master Key. This covers FMT_SMF.1 (Customize).

In the customized PKID ECC Generator, after being successfully authenticated, the TOE administrator is capable of performing the following functions:

a) Change administrator password
   Current password needs to be supplied before specifying the new password.

b) Generate public and private keys
   The administrator takes input (PKID) from the user and generates the public and private key (together with access code) for the user.

c) Export keys
   The administrator is capable of exporting the keys upon request such as the case where users lost the keys.

This covers FMT_SMF.1.

Security Functional Requirements Satisfied:

- FMT_SMF.1 (Customize)
- FMT_SMF.1

8.3 CRYPTOGRAPHIC SUPPORT

The TOE is unique as during customization of the system, input from the client organization will be used to generate Master Keys in order to customize the PKID ECC Generator for that specific client. This is particularly important to ensure that no one can duplicate the system without having the same input from the client.

Master Key shall be generated using specified cryptographic key generation which is non-repeatable with key size of 320 bit. This covers FCS_CKM.1 (A).

The generated Master Key from the CD shall be imported into the generator which resulting in a customized generator for that client. This covers FCS_CKM.2 (A). To import, the Master Key access code is required to be entered for authentication.

In the Customized PKID ECC Generator, TOE authorized administrator is able to generate public and private keys (together with access code) for the user. The generated keys are unique for each user. Generation of public and private keys shall be using specified encryption algorithm which is Standard Elliptical Curve Cryptography using plane curve with cryptographic key-size of 320 bit that meets the NIST Statistical Test Suite. This covers FCS_CKM.1 (B).

The generated public and private keys are tied to the chosen PKID. For example, files encrypted using the public key generated for a MAC address can only be decrypted using the corresponding private key on the PC/Notebook with the same MAC address. The scope also covers the output produced by the Key Generation Module which are the private key, public key and access code. Files (not SMS) encrypted using the public key generated for an IMEI number can only decrypted using the corresponding private key on the mobile phone with the same IMEI number. Files encrypted using the public key generated for an email address can only decrypted using the corresponding private key for the email address. Users shall use client application provided by the developer which supports these features. (As already stated in *Section 2.3.1 Physical Scope of the TOE*, client application is not included in the TOE scope).

The TOE will store the newly generated public and private keys in designated folder. Exported keys (refer item c under Section 8.2 Security Management) will also be stored in designated folder. These keys are ready for copying and distribution to the users. This covers FCS_CKM.2 (B).

Security Functional Requirements Satisfied:

- FCS_CKM.1 (A)
- FCS_CKM.2 (A)
- FCS_CKM.1 (B)
- FCS_CKM.2 (B)