Mobile Billing System Security Target

Common Criteria: EAL1

Version 1.2

25-MAY-11

Document management

Document identification

Document ID	IDV_EAL1_ASE
Document title	IDOTTV Mobile Billing System Security Target
Product version	Mobile Billing System (version 1.4) consists of: - Mobile Billing Webtool (version 1.4) - Mobile Billing Applet (version 1.0) - Mobile Billing Server (version 1.0)

Document history

Version	Date	Description
0.1	11-SEP-10	Release for internal review
0.2	08-DEC-10	Updated to address EOR001
0.3	24-JAN-11	Updated to address CAR
0.4	28-MAR-11	Updated to address minor changes for Product Version.
1.0	09-MAY-11	Initial Release
1.1	24-MAY-11	Minor update on Glossary
1.2	25-MAY-11	Minor update.

Table of Contents

1 Security Target introduction (ASE_INT)

1.1 ST and TOE identification

ST Title	IDOTTV Mobile Billing System Security Target
ST Version	1.2, 25-MAY-11
TOE Reference	Mobile Billing System (version 1.4) consists of: - Mobile Billing Webtool (version 1.4) - Mobile Billing Applet (version 1.0) - Mobile Billing Server (version 1.0)
TOE Version	Version 1.4
Assurance Level	EAL1
CC Identification	Common Criteria for Information Technology (IT) Security Evaluation, Version 3.1, July 2009, incorporating: • Part One – Introduction and General Model, Revision Three, July 2009; • Part Two – Security Functional Components, Revision Three, July 2009; and • Part Three – Security Assurance Components, Revision Three, July 2009.

1.2 Document organization

This document is organized into the following sections:

- Section 1 provides the introductory material for the ST as well as the TOE description including the physical and logical scope of the TOE.
- Section 2 provides the conformance claims for the evaluation.
- Section 3 defines the security objectives for the environment.
- Section 4 contains the functional and assurance requirements derived from the Common Criteria, Part 2 and 3, respectively that must be satisfied by the TOE.

- Section 5 provides a summary of the TOE specification, identifying the IT security functions provided by the TOE
- Section 6 provides the glossary for the ST.

1.3 TOE overview

1.3.1 TOE type and usage

Mobile Billing System consists of a mobile application (Mobile Billing Applet Version 1.0) that facilitates secured, confidential and paperless billing service between service provider and customers which is installed on a user's mobile device and the Mobile Billing Server (Version 1.0). Instead of relying on paper and intermediaries, Mobile Billing delivers bill statement and requested usage information directly to mobile devices. It also features a mobile payment function that enables customers to make bill payment via mobile device.

The TOE is comprised of three key components:

- **Mobile Billing Applet.** A java-based mobile application developed specifically for the Blackberry mobility platform. The application provides a subscriber with the basis for integrating with the mobile billing server.
- **Mobile Billing Server.** An application that provides:
    - connectivity to the billing systems of telecommunications providers,
    - a connection to the mobile billing applet application that provides subscribers with system connectivity.
    - Storing data for the TOE.
- **Mobile Billing Webtool**. a web-based interface for both subscribers and telecommunication administrators to login and manage their accounts or the system.

The TOE is ***Mobile Billing System version 1.4*** and is referred to as ***Mobile Billing System*** in this document.

1.3.2 TOE security functions

The following table highlights the range of security functions and features implemented by the TOE.

Security function	Description
Identification and Authentication	The TOE provides identification and authentication of users of the TOE.
Security Management	The TOE provides security management through the use of the Web Administration Interface as well as through the applet installed on mobile devices.
User Data Protection	The TOE provides its own access control between subjects and objects covered by the Access Control SFP.
Secure Communication	The TOE is able to protect the billing information from disclosure and modification when the scanned data is sent from Mobile Billing server to the applet application.

1.4 TOE description

1.4.1 Physical scope of the TOE

The TOE comprises the Mobile Billing System. This consists of the applet that is installed on any Java-enabled mobile device as well as the Mobile Billing Server. A typical installation of the TOE can be found in Figure 1 below.

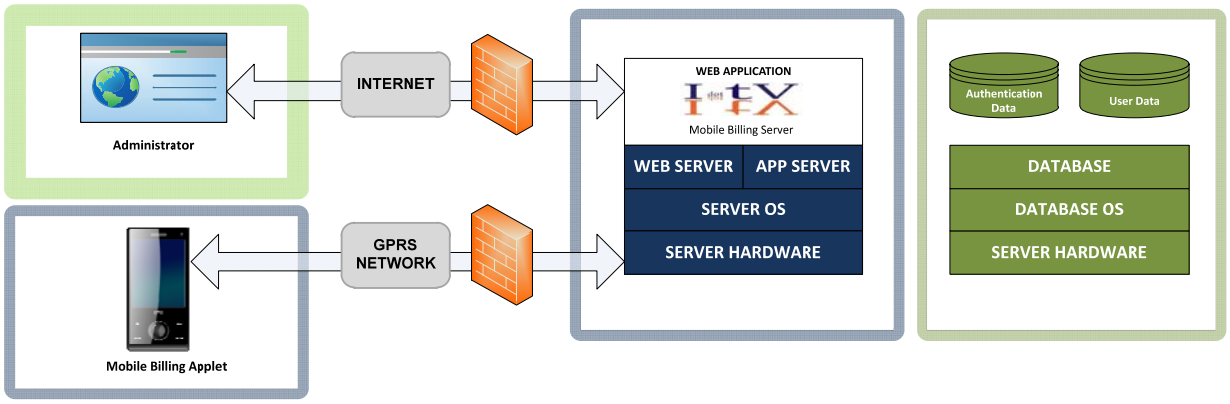

Figure 1 – Mobile Billing System Deployment

Telecommunication administrator will login to the TOE through a web admin interface. For subscribers, they will download and install the applet and access their billing information through the application.

The mobile application can be installed on any Java Enabled mobile devices. The Mobile Billing Server runs Apache HTTP Server Version 2.0 on a Linux operating system.

1.4.2 Logical scope of the TOE

The logical boundaries of the TOE include the functions of the TOE interfaces. These functions include identification and authentication, security management, User Data Protection and secure communication.

- **Identification & Authentication.** When a user issues a request to the TOE to access the billing information, the TOE requires that the user identify and authenticate themselves before performing any TSF mediated action on behalf of the user. The TOE checks the credentials presented by the user upon the login page against the authentication information in the database.

- **User Data Protection.** The access control function permits a user to access the billing information only if a userID or role of the user has permission to access the information. Access rules are stored in Access Control Lists associated with each object in the TSC.

- **Security Management.** The TOE contains various user management functions to ensure efficient and secure management of the TOE:

  The TOE maintains four roles within the TOE to ensure that the functions are restricted to only those users that need to have access to privileged functions. The roles maintained by the TOE are: Telecommunication Employee, Telecommunication Administrator, Mobile Subscriber and Super Administrator. The functions above, and indeed, aspects of these functions, are restricted based on these roles.

- **Secure Communication.** The TOE provides a secure communication channel between the applet application and the Mobile Billing server when billing information is sent from the server.

2 Conformance Claim (ASE_CCL)

The ST and TOE are conformant to version 3.1 (Revision 3) of the Common Criteria for Information Technology Security Evaluation.

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

- Part 2 conformant. Conformant with Common Criteria for Information Technology Security Evaluation Part 2: Security functional requirements, version 3.1, Revision 3.
- Part 3 conformant. Conformant with Common Criteria for Information Technology Security Evaluation Part 3: Security assurance requirements, version 3.1, Revision 3. Evaluation is EAL1.

3 Security objectives (ASE_OBJ)

3.1 Overview

The security objectives at an EAL1 level of assurance include concise statements of the objectives to be achieved by the supporting environment.

3.2 Security objectives for the environment

Identifier	Objective statements
OE.ENVIRONMENT	Those responsible for the TOE must ensure that appropriate authentication and authorisation controls for all users and administrators in the underlying environment (including the Operating System, RDBMS, and Web Server)
OE.ADMIN	The owners of the TOE must ensure that the super administrators and telecommunication administrator who manages the TOE is not hostile and is competent.
OE.PHYSICAL	Those responsible for the TOE must ensure that the IT environment provides the TOE with appropriate physical security, commensurate with the value of the IT assets protected by the TOE.
OE.DATABASE	Those responsible for the TOE must ensure that the databases in the TOE environment have been correctly configured according to the principle of least privilege.
OE.MANAGEMENT	Those responsible for the TOE must ensure that all management of the TOE is performed through the management interfaces of the TOE and not through the underlying environment.
OE.NETWORK	Those responsible for the TOE must ensure that appropriate network layer protection, that there is a firewall in place that only permits access through required ports for external users to access the web-server.
OE.PATCH	Those responsible for the TOE must ensure that the underlying operating system, web-server, application server and DBMSs and are patched and hardened to protect against known vulnerabilities and security configuration

	issues.
OE.COMMUNICATION	Those responsible for the TOE must ensure that the web-server has SSL certificates installed and are valid (not revoked or expired), are sourced from a trusted entity.

4 Security requirements (ASE_REQ)

4.1 Overview

This section defines the security requirements satisfied by the TOE. Each requirement has been extracted from version 3.1 of the Common Criteria, part 2 providing functional requirements and part 3 providing assurance requirements.

4.2 SFR conventions

Part 2 of the Common Criteria defines an approved set of operations that may be applied to security functional requirements. Following are the approved operations and the document conventions that are used within this ST to depict their application:

- **Assignment.** The assignment operation provides the ability to specify an identified parameter within a requirement. Assignments are depicted using bolded text and are surrounded by square brackets as follows [**assignment**].

- **Selection.** The selection operation allows the specification of one or more items from a list. Selections are depicted using bold italics text and are surrounded by square brackets as follows [***selection***].

- **Refinement.** The refinement operation allows the addition of extra detail to a requirement. Refinements are indicated using bolded text, for **additions**, and strike-through, for ~~deletions~~.

- **Iteration.** The iteration operation allows a component to be used more than once with varying operations. Iterations are depicted by placing a letter at the end of the component identifier as follows FDP_IFF.1a and FDP_IFF.1b.

4.3 Security functional requirements

4.3.1 Overview

The security functional requirements are expressed using the notation stated in Section 4.2 and summarized in the table below.

Identifier	Title
FCS_COP.1	Cryptographic operation
FDP_ACC.1	Subset access control
FDP_ACF.1	Security attribute based access control
FIA_UAU.2	User authentication before any action
FIA_UID.2	User identification before any action
FMT_MSA.1	Management of security attributes
FMT_MSA.3	Static attribute initialisation
FMT_MTD.1	Management of security functions behaviour
FMT_SMF.1	Specification of Management Functions
FMT_SMR.1	Security roles
FTP_ITC.1	Inter-TSF trusted channel

4.3.2 FCS_COP.1 Cryptographic Operation

Hierarchical to:	No other components.
FCS_COP.1.1	The TSF shall perform [**secure hashing**] in accordance with a specified cryptographic algorithm [**MD5**] and cryptographic key sizes [**none**] that meet the following: [**FIPS 180-2**].
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
Notes:	This cryptographic operation does not use key. The password of the users is hashed and compare with the values stored in the authentication data database.

4.3.3 FDP_ACC.1 Subset access control

Hierarchical to:	No other components.
FDP_ACC.1.1	The TSF shall enforce the [**Access Control SFP**] on [**Subjects:** **a) Telecommunication Employees, Telecommunication administrator, super administrator and mobile subscriber** **Objects:** **a) Billing information** **Operations:** **a) Retrieving of user billing information for viewing**]
Dependencies:	FDP_ACF.1 - Security attribute based access control
Notes:	Mobile Subscriber can only see their billing information using Mobile Billing Applet. Telecommunication Administrator and Super Administrator can see all the billing information using Mobile Billing Webtool. For Telecommunication Employee, it will be up to the Telecommunication Administrator or Super

	Administrator to configure the access.

4.3.4 FDP_ACF.1 Security attribute based access control

Hierarchical to:	No other components.
FDP_ACF.1.1	The TSF shall enforce the [**Access Control SFP**] to objects based on the following: [**Subject attribute:** **a) ID of the user** **b) corresponding user role/level** **Object attributes:** **a) Access Control List**]
FDP_ACF.1.2	The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: [**The operation is allowed, if:** **a) The Access Control List for an object permits the user ID to access that object; OR** **b) The Access Control List for an object permits the User Role to access that Object.**]
FDP_ACF.1.3	The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: [**the Telecommunication administrator role and super administrator role can access all records**].
FDP_ACF.1.4	The TSF shall explicitly deny access of subjects to objects based on the following additional rules: [**None**].
Dependencies:	FDP_ACC.1 Subset access control FMT_MSA.3 Static attribute initialisation
Notes:	None.

4.3.5 FIA_UAU.2 User authentication before any action

Hierarchical to:	FIA_UAU.1 Timing of authentication
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.
Dependencies:	FIA_UID.1 Timing of identification
Notes:	None.

4.3.6 FIA_UID.2 User identification before any action

Hierarchical to:	FIA_UID.1 Timing of identification
FIA_UID.2.1	The TSF shall require each user to be successfully identified before allowing any other TSF-mediated actions on behalf of that user.
Dependencies:	No dependencies.
Notes:	None.

4.3.7 FMT_MSA.1 Management of security attributes

Hierarchical to:	No other components.
FMT_MSA.1.1	The TSF shall enforce the [**Access Control SFP**] to restrict the ability to [***write or delete***] the security attributes [**None**].
Dependencies:	[FDP_ACC.1 Subset access control, or FDP_IFC.1 Subset information flow control] FMT_SMR.1 Security roles FMT_SMF.1 Specification of Management Functions
Notes:	Subscribers will have access to their own account bills using Mobile Billing Applet and telecommunication administrators can see all the information of users using the Mobile Billing Webtool.

4.3.8 FMT_MSA.3 Static attribute initialisation

Hierarchical to:	No other components.
FMT_MSA.3.1	The TSF shall enforce the [**Access Control SFP**] to provide [***restrictive***] default values for security attributes that are used to enforce the SFP.
FMT_MSA.3.2	The TSF shall allow ~~the~~ [**none**] to specify alternative initial values to override the default values when an object or information is created.
Dependencies:	FMT_MSA.1 Management of security attributes FMT_SMR.1 Security roles
Notes:	None.

4.3.9 FMT_MTD.1 Management of TSF data

Hierarchical to:	No other components
FMT_MTD.1.1	The TSF shall restrict the ability to [***modify***] the [**User Password**] to [**individual users (that is related to the password)**].
Dependencies:	FMT_SMR.1 Security roles FMT_SMF.1 Specification of Management Functions
Notes:	None.

4.3.10 FMT_SMF.1 Specification of Management Functions

Hierarchical to:	No other components.
FMT_SMF.1.1	The TSF shall be capable of performing the following management functions: [**a) creation of administrative users with default passwords** **b) changing of passwords** **c) management of Access Control lists**]

Dependencies:	No dependencies.
Notes:	None.

4.3.11 FMT_SMR.1 Security Roles

Hierarchical to:	No other components.
FMT_SMR.1.1	**a)** The TSF shall maintain the roles [**Telecommunication Employees, Telecommunication administrator, super administrator and mobile subscriber**].
FMT_SMR.1.2	The TSF shall be able to associate users with roles.
Dependencies:	FIA_UID.1 Timing of identification
Notes:	None.

4.3.12 FTP_ITC.1 Inter-TSF trusted channel

Hierarchical to:	No other components.
FTP_ITC.1.1	The TSF shall provide a communication channel between itself and another **remote instance of the TOE** ~~trusted IT product~~ that is logically distinct from other communication channels and provides assured identification of its end points and protection of the channel data from modification or disclosure.
FTP_ITC.1.2	The TSF shall permit [***the TSF***] to initiate communication via the trusted channel.
FTP_ITC.1.3	The TSF shall initiate communication via the trusted channel for [**Transfer of user data**].
Dependencies:	None
Notes:	None.

4.4 Dependency analysis

SFR	Dependency	Inclusion
FCS_COP.1	[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	None as there are no key used for MD5 therefore there is no need for key generation as well as key destruction.
FDP_ACC.1	FDP_ACF.1 Security attribute based access control	FDP_ACF.1
FDP_ACF.1	FDP_ACC.1 Subset access control FMT_MSA.3 Static attribute initialisation	FDP_ACC.1 FMT_MSA.3
FIA_UAU.2	FIA_UID.1 Timing of identification	FIA_UID.2
FIA_UID.2	No dependencies	N/A
FMT_MSA.1	[FDP_ACC.1 Subset access control, or FDP_IFC.1 Subset information flow control] FMT_SMR.1 Security roles FMT_SMF.1 Specification of Management Functions	FDP_ACC.1 FDP_ACF.1 FMT_SMF.1 FMT_SMR.1
FMT_MSA.3	FMT_MSA.1 Management of security attributes FMT_SMR.1 Security roles	FMT_MSA.1 FMT_SMR.1

SFR	Dependency	Inclusion
FMT_MTD.1	FMT_SMR.1 Security roles FMT_SMF.1 Specification of Management Functions	FMT_SMF.1 FMT_SMR.1
FMT_SMF.1	No dependencies	N/A
FMT_SMR.1	FIA_UID.1 Timing of identification	FIA_UID.2
FTP_ITC.1	No dependencies	N/A

4.5 TOE security assurance requirements

The assurance package for the evaluation of the TOE is Evaluation Assurance Level 1 (EAL1).

EAL1 provides a basic level of assurance by a limited security target and an analysis of the SFRs in that ST using a functional and interface specification and guidance documentation, to understand the security behavior.

The analysis is supported by a search for potential vulnerabilities in the public domain and independent testing (functional and penetration) of the TSF.

EAL1 also provides assurance through unique identification of the TOE and of the relevant evaluation documents.

This EAL provides a meaningful increase in assurance over unevaluated IT.

Assurance class	Assurance components
ADV: Development	ADV_FSP.1 Basic functional specification
AGD: Guidance documents	AGD_OPE.1 Operational user guidance
	AGD_PRE.1 Preparative procedures
ALC: Life cycle support	ALC_CMS.1 TOE CM coverage
	ALC_CMC.1 Labelling of the TOE
ASE: Security Target evaluation	ASE_CCL.1 Conformance claims
	ASE_ECD.1 Extended components definition
	ASE_INT.1 ST Introduction
	ASE_OBJ.1 Security objectives for the operational environment
	ASE_REQ.1 Stated security requirements
	ASE_TSS.1 TOE summary specification
ATE: Tests	ATE_IND.1 Independent testing - conformance
AVA: Vulnerability assessment	AVA_VAN.1 Vulnerability survey

4.6 Assurance measures

Assurance requirement	Assurance measures	Demonstration
ADV_FSP.1 Basic functional specification	Development	The development assurance measure provides all the necessary design documentation to support the analysis of the TOE for an evaluation at EAL1. The functional specification provides a detailed description of the security functions of the TOE.
AGD_OPE.1 Operational user guidance	Guidance documents	The operational user guidance documentation provides the guidance for end users, administrators and other parties who will utilise the TOE. These documents provide all the necessary instructions and direction for ensuring that the TOE is installed, configured, used and administered in a secure manner.
AGD_PRE.1 Preparative procedures		
ALC_CMC.1 Labelling of the TOE	Life cycle support	Configuration management measures provide the assurance that the TOE and supporting evidence can be uniquely identified.
ALC_CMS.1 TOE CM coverage		
ASE_CCL.1 Conformance claims	Security Target evaluation	Security Target evaluation assurance measures ensure that the claim to EAL1 can be accurately appraised.
ASE_ECD.1 Extended components definition		
ASE_INT.1 ST Introduction		
ASE_OBJ.1 Security objectives for the operational environment		

Assurance requirement	Assurance measures	Demonstration
ASE_REQ.1 Stated security requirements		
ASE_TSS.1 TOE summary specification		
ATE_IND.1 Independent testing - conformance	Tests	The tests assurance measure ensures that the TOE has been appropriately tested for the claimed set of security functions. The test plans for the TOE identifies the set of security functions that are to be tested, the procedures for establishing the test environment and also for conducting the test cases. The results of the tests are also recorded to provide evidence of test results.
AVA_VAN.1 Vulnerability survey	Vulnerability assessment	The TOE will be made available for vulnerability analysis and penetration testing.

5 TOE summary specification (ASE_TSS)

5.1 Overview

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

The TOE security functions include the following:

- User Data Protection
- Identification and Authentication
- Security Management
- Secure Communication

5.1.1 User Data Protection

The TOE enforces an access control policy on billing information. After a mobile subscriber identifies and authenticates to the mobile billing server via the mobile billing applet, the mobile billing server will check all access to the billing information from the user. The TOE will permit a user to access a protected resource only if a userID or role/level of the user has permission to perform the requested action on the resource (**FDP_ACC.1, FDP_ACF.1**). For the Telecommunication Administrator, Telecommunication Employee and the Super Administrator, they authenticate themselves through the Mobile Billing Webtool (web portal).

The TOE maintains access control lists for each object within an organisation. Each ACL maps users and roles to the operations that they are permitted to perform on the object. For the mobile subscriber, their userID, IMEI (***International Mobile Equipment Identity*** is a unique 17 or 15 digit code used to identify an individual mobile station to a GSM or UMTS network), IMSI (***International Mobile Subscriber Identity*** is a unique 15-digit code used to identify an individual user on a GSM network and a TAC code which is issued to the user during registration will be used to identify the user when they are accessing the billing information. This is to ensure that only the user with the registered sim card and phone can access the information.

There are 4 users maintained by the TOE. They are the Mobile Subscriber, Telecommunication Administrator, Telecommunication Employee and the Super Administrator (**FMT_SMR.1**). Each type of user will have different access rights to billing information. For mobile subscriber, they can only access

their own billing information whereas telecommunication administrator can access all information. All users will have a unique user ID.

5.1.2 Identification and Authentication

When a user issues a request to the TOE to access a his/her billing information, the TOE requires that the user (being a Mobile Subscriber, Telecommunication Administrator, Telecommunication Employee or Super Administrator) identify and authenticate themselves before performing any TSF mediated action (**FIA_UID.2, FIA_UAU.2**). The TOE checks the credentials presented by the user upon the login page against the authentication information in the database.

Mobile Subscriber will login through the interface orovided by the Mobile Billing applet on their mobile device. For the Telecommunication Administrator, Telecommunication Employee and the Super Administrator, they will login through the Mobile Billing Webtool (web portal).

All users presented passwords are hashed before being used to authenticate the user or when users change their passwords (**FMT_MTD.1/Password**) and is being written to the database. This is all done by the Mobile Billing Server (**FCS_COP.1**).

5.1.3 Security Management

The TOE contains various management functions to ensure efficient and secure management of the TOE (**FMT_SMF.1**):

Mobile Subscriber

1. Checking their own account statement

Telecommunication Administrator

1. Authenticate to the Mobile Billing Server and as well as performing management functions according to their roles through the Mobile Billing Webtool

2. Only telecommunication administrator and super administrators can change passwords, reset passwords and change the access levels of the telecommunication employees

3. Reset Password for user that forgot its password.

Super Administrator

1. Authenticate to the Mobile Billing Server and as well as performing management functions according to their roles through the Mobile Billing Webtool

2. Only telecommunication administrator and super administrators can change passwords, reset passwords and change the access levels of the telecommunication employees

3. Create administrator users for the telecommunication company

Telecommunication Employees

1. Authenticate to the Mobile Billing Server and as well as performing management functions according to their level that is allocated to them by the telecommunication administrators or super administrator through the Mobile Billing Webtool

The TOE allows no one to change the default values of the TSF data and security attributes of the TOE as well as the ACL (**FMT_MSA.3, FMT_MSA.1**).

5.1.4 Secure Communication

The TOE uses SSL to protect billing information flowing among the TOE components (Mobile Billing server and the applet installed on mobile devices) from disclosure (**FTP_ITC.1**). The initiation of the secure SSL channel is done by the Mobile Billing Applet on the Mobile Subscriber's mobile device. Whenever user launches the applet and proceed to authenticate themselves, the Mobile Billing Applet will do a handshake protocol with the Mobile Billing Server and after this, a session key will be generated and will be used to encrypt the user data sent/retrieved to and from the Mobile Billing Server.

6 Glossary

Term	Description
Authentication Data	It is information used to verify the claimed identity of a user.
FIPS 180-2	It is a Federal Information Processing Standards Publications (FIPS PUBS) are issued by the National Institute of Standards and Technology for Secure Hash Standard
MD5	MD5 (Message-Digest algorithm 5) is a cryptographic hash function with a 128-bit hash value.
Mobile Subscriber	Mobile Subscriber access the TOE through the Mobile Billing applet on their mobile phones.
SSL	The TLS is a protocol that allows client/server applications to communicate across a network in a way designed to prevent eavesdropping and tampering.
Super Administrator	Super Administrators are from IDOTTV. They are responsible for the correct operation of the Mobile Billing Server (installation, configuration and maintenance).
Telecommunication Administrator	Administrators are from the telecommunication operator who subscribe to the mobile billing service for their mobile users. They are responsible for the subscription of mobile users and their data and they administer these though the web portal provided by IDOTTV.
TSC	TSC (TSF Scope of Control) The set of interactions that can occur with or within a TOE and are subject to the rules of the TSP.
TSF data	Data created by and for the TOE, that might affect the operation of the TOE
User data	Data created by and for the user that does not affect the operation of the TSF.