GB

NATIONAL STANDARD OF THE

PEOPLE'S REPUBLIC OF CHINA

ICS 35.040

L 80

GB/T 20273-2019

Replacing GB/T 20273-2006

Information Security Technology - Security Technical Requirements for Database Management System

信息安全技术

数据库管理系统安全技术要求

Issued on: August 30, 2019 **Implemented on: March 1, 2020**

Issued by: State Administration for Market Regulation;

Standardization Administration of the People's Republic of China.

Table of Contents

Information Security Technology - Security Technical Requirements for Database Management System

1 Scope

This Standard stipulates the description of database management system evaluation target; the definition, security objectives and requirements of security issues of different evaluation assurance levels of database management system; the fundamental principles between the definition of security issues and security objectives, and between security objectives and security requirements.

This Standard is applicable to the test, evaluation and procurement of database management system. It may also be applied to the guidance of the research and development of database management system.

NOTE: Level-EAL2, Level-EAL3 and Level-EAL4 security requirements stipulated in this Standard are applicable to not only the security evaluation of database management system based on GB/T 18336.1-2015, GB/T 18336.2-2015 and GB/T 18336.3-2015, but also GB/T 17859-1999-based database security evaluation of second-level database system audit protection, third-level security label protection, fourth-level structural protection. Please refer to A.1 in Appendix A for relevant correspondences.

2 Normative References

The following documents are indispensable to the application of this document. In terms of references with a specified date, only versions with a specified date are applicable to this document. In terms of references without a specified date, the latest version (including all the modifications) is applicable to this document.

GB/T 18336.1-2015 *Information Technology - Security Techniques - Evaluation Criteria for IT Security - Part 1: Introduction and General Model*

GB/T 18336.2-2015 *Information Technology - Security Techniques - Evaluation Criteria for IT Security - Part 2: Security Functional Components*

GB/T 18336.3-2015 *Information Technology - Security Techniques - Evaluation Criteria for IT Security - Part 3: Security Assurance Components*

GB/T 25069-2010 *Information Security Technology - Glossary*

GB/T 28821-2012 *Technical Requirements of Relational Database Management System*

4 Description of Evaluation Target

4.1 An Overview of Evaluation Target

In this Standard, target of evaluation (TOE) refers to management software and database object that it manages included in the database management system (DBMS).

Management software included in DBMS shall provide database language, which defines, operates and manages database object; provide database control language and maintain data integrity of DBMS operation through data model semantic constraints; provide database backup, restore and recovery mechanism, guarantee the availability of database when there are breakdowns in DBMS operation. Relational database management system (RDBMS) shall provide transaction management mechanism, guarantee the atomicity, consistency, isolation and durability (ACID) of transactions in multi-user database concurrent operations.

DBMS mainly includes the following constituent parts:

a) Database: constituted of physical files, such as: data file that stores user data and TOE security functionality (TSF) data; log file that stores database transaction processing process; control file that maintains the integrity of DBMS operations, etc. The database object being stored includes: model object, non-model object, database dictionary object, etc.

b) Database instance: include components like query engine, transaction manager, data storage manager, etc. Implement basic functions: the definition, management, query, update and control of database object.

c) Database language and its access interface: provide database language and database development interface specifications, such as: structured query language (SQL), open database connectivity (ODBC), JAVA database connectivity (JDBC), etc.; allow authorized users to define database structure through database development interface, access and modify database object data, demonstrate relevant configuration parameters of DBMS operation, and execute various maintenance operations on user data and relevant data of DBMS operation.

d) DBMS operation maintenance auxiliary means: provide DBMS operation maintenance auxiliary means or interfaces, such as: initiation and shutdown of database instance; online, offline, opening and closing of database or data file; database checkpoint control; database log archiving; external data import, etc.

user/authorized administrator's functions like parallel sessions.

NOTE: DBMS software and the security of its management data assets are not isolated. Under the production environment, the IT environment of DBMS operation (operating system, network system and hardware, etc.), together with DBMS, establish a security system of TOE. In the description of TOE, security target (ST) author clearly indicates and identifies the correlation between the architecture of DBMS evaluation, and the various components of IT environment.

4.3 Evaluation Target Deployment Mode

If any internal and external entity of DBMS needs to obtain data assets of TOE management, firstly, it shall satisfy corresponding security policies of TOE and the operating environment. TOE operating environment target might include multiple security control components, which involve multiple security policies, such as: equipment's physical security, environmental physical security, system's physical security and personnel security management, etc. These operating environment security policies prevent DBMS software and the database that it manages from security threats in the operating environment of DBMS.

This Standard may be adopted to evaluate DBMS security of multiple deployment structures, which include, but are not limited to the following architectures:

a) Centralized architecture: DBMS software and database application program are installed and operated on a host; user can only send out database access requests or administrative commands through the application terminal, which is transmitted to the host through communication lines; after database's instance response and processing on the host, the processing result is returned to the user terminal through the communication lines.

b) Client/server system structure: client-side database application and server-side database instance implement communication through network connections; client-side sends database access requests or administrative commands, demonstrates the returned data by database instance; server-side securely executes user's database access requests and administrative commands. Front-end application may be implemented on the basis of browser; through remote Web server or application server, implement connections with database server; the remote server takes charge of the interaction with the database server.

c) Distributed database architecture: database nodes are respectively stored on multiple site database servers, which are physically mutually independent. The database servers among these sites, which are connected through the network, collaboratively provide distributed database data access service. User may execute certain database access requests or administrative

operation data, which leads to failure of TSF security control mechanism.

5.2.3 Audit mechanism's failure (T.AUDIT_FAILURE)

Malicious user or process might modify security audit strategy, which would lead to disabled or invalidated database audit function, audit record loss or tampered audit record. Or, through the invalidated audit data storage, the storage of the subsequent audit record would be prevented, which would wipe out user's database operation.

5.2.4 Cryptographic attack (T.CRYPTO_COMPROMISE)

Malicious user or process might lead to improper browse, modification or deletion of executable codes of database storage and communication encryption function-related key, data or ciphertext service components, which would undermine the database encryption mechanism and leak the data protected by the encryption mechanism.

5.2.5 Data transmission eavesdropping (T.EAVESDROP)

Malicious user or process might observe or modify user data or TSF data transmitted among TOE physically isolated components (including user requests and responses between the client-side and the server, data transmission among different nodes of distributed database, etc.).

5.2.6 Flawed design (T.FLAWED_DESIGN)

Unintentional logic errors in TOE demand specifications or design might lead to design weaknesses or flaws. Malicious user might take advantage of these flaws to initiate security attack against TOE.

5.2.7 Flawed implementation (T.FLAWED_IMPLEMENTATION)

Unintentional errors during the development of TOE might lead to weaknesses or flaws in TOE implementation. Malicious user might take advantage of these unknown loopholes to attack TOE.

5.2.8 Label data out-of-control (T.LBAC)

Malicious user or process might illegally browse, modify or delete label strategy data, controlled subject classification label data and controlled object bond label data of TOE. Authorized administrator's illegal access to label management-based data assets of controlled subject.

5.2.9 Masqueraded authorized user (T.MASQUERADE)

Malicious user or process might masquerade as authorized administrator or authorized user to access database dictionary, system security configuration parameters or data assets protected by DBMS.

It is assumed that there will be one or multiple authorized administrators with appointed role permissions in TOE, and their roles are divided in accordance with security principles like minimum privileges, separation of duties and in-depth defense (ST author needs to explain the specific meaning of “security role” in accordance with the system permissions supported by DBMS and the solutions to specific application that DBMS targets at).

5.4.5 Multi-tier application accountability (A.MIDTIER)

In multi-tier application environment, in order to guarantee the security accountability of TOE, the TOE operating environment component service of any middle tier shall send the original authorized user identification to TSF (ST author shall explain the specific meaning of “multi-tier application accountability” in accordance with the solutions to specific application that DBMS targets at).

5.4.6 Administrator hypothesis (A.NO_HARM)

Authorized user and authorized administrator that use the database are equipped with fundamental database security protection knowledge and good habits of using the database. They are well-trained; they could comply with TOE administrator guidance and use the database through secure modes.

5.4.7 Exclusive for server (A.NO_GENERAL_PURPOSE)

On the host where DBMS is operated, other programs or services that obtain universal computation or storage capability (for example, compiler, editor or application program) are not installed.

5.4.8 Physical security (A.PHYSICAL)

DBMS operating environment shall provide physical security that is consistent with the data value under its management. For example, store and manage TOE-related data (such as: configuration parameters and archived logs, etc.) that is stored outside the database through a secure mode.

5.4.9 Communication security (A.SECURE_COMMS)

It is assumed that communication channels among different nodes in the distributed database between data server and application terminal are safe and reliable (for example, satisfied confidentiality and integrity). The implementation mode may be through shared key, public/private key pair, or, the generation of session key through other keys being stored.

management of DBMS products. TOE shall provide authorized user with user operation manual documents related with database object establishment and application (ST author shall base on TOE security mechanism to explain pre-configurated database administrator role, so as to implement authorized management of separated duties).

6.1.5 Administrator role separation (O.ADMIN_ROLE)

TOE shall provide authorized administrator role, which is consistent with different database management operations, so as to provide role management functions, such as: the separation of duties and role constraints, etc. In addition, these management functions may implement security management through local or remote mode (ST author shall base on TOE security mechanism to explain pre-configurated database administrator role, so as to implement authorized management of separated duties).

6.1.6 Audit data generation (O.AUDIT_GENERATION)

TOE shall provide the capability of detecting and establishing user-related security events, such as: database audit policy definition, audit function start-stop management, database management operations and user database object operations, etc. (ST author shall base on the composition and storage mechanism of TOE audit record to explain the mode of audit data storage (inside and outside database), and audit data security management mechanism).

6.1.7 Audit data protection (O.AUDIT_PROTECTION)

TOE shall have the capability of securely storing audit data and protecting audit events being stored.

6.1.8 Available database service (O.AVAIL)

TOE shall provide data recovery mechanism for affairs, database instance and storage medium failures; provide the capability of self-maintenance of database storage structure in DBMS updates; guarantee the restorability of TOE management data assets.

TOE shall provide primary and secondary server TSF control transfer and database instance failover mechanism, so as to support distributed component deployment of distributed database service for the management demand of availability.

6.1.9 Configuration identification (O.CONFIG)

TOE shall identify product component configuration and evaluation configuration items of its documents, so as to provide methods of correcting and tracing them when DBMS is re-distributed and correction errors are corrected.

NOTE: generally speaking, configuration identification refers to issuance baseline that is

TOE operating environment shall be equipped with database administrator group or role; provide necessary functions and facilities for the management and configuration of DBMS operation security; prevent these functions and facilities from unauthorized usage.

6.2.5 Directory access control protection (OE.DIR_CONTROL)

DBMS operating environment that supports directory service (for example, LDAP server) shall provide mechanisms like user identification, identity authentication and access control, so as to prevent illegal user from accessing TSF data stored under the directory service. The access control mechanism of directory service shall provide security protection measures of TSF control data import/export.

6.2.6 IT domain separation (OE.DOMAIN_SEPARATION)

TOE operating environment under distributed deployment shall provide TOE operation nodes with one separable security execution domain. Communication among different DBMS nodes shall be conducted through a secure mode.

6.2.7 Administrator Integrity (OE.NO_HARM)

Organization that adopts TOE shall guarantee that authorized administrator is trustworthy, well-trained, and can comply with organization security policy and relevant database administrator guidance.

6.2.8 Exclusive for database server (OE.NO_GENERAL_PURPOSE)

Apart from providing necessary service components for TOE operation, management and support, database server shall not have computation or storage functional components (for example, compiler, editor or application program) that are irrelevant with database instance operation.

6.2.9 Consistency of physical security (OE.PHYSICAL)

TOE operating environment shall provide physical security that is consistent with DBMS and the value of its management data assets.

6.2.10 Communication security environment (OE.SECURE_COMMS)

TOE operating environment shall provide secure communication lines between remote user/program and database server.

6.2.11 IT environment self-protection (OE.SELF_PROTECTION)

TOE operating environment shall maintain one execution domain which prevents DBMS and its operating environment from external interference, damage or unauthorized leakage.

FMT_MSA_EXT.1.2 TSF shall implement [option: ***label access control-based security policy***, [***assignment: information flow control policy with appointed mechanism by ST author***]]; merely through [option: ***LBAC authorized user***, ***[assignment: authorized administrator appointed by ST author***]], implement [[assignment: ***security attribute***] to [assignment: ***security label***]].

NOTE: this requirement is applicable to EAL-3 evaluation assurance level.

7.1.3.2 Security attribute management [FMT_MSA_EXT.1(2)]

FMT_MSA_EXT.1.1 TSF shall implement [option: ***user control policy-based, role control policy-based and user group control policy-based, [assignment: compulsory access control defined by ST author***]]; merely through [option: ***authorized administrator, authorized user***] to conduct [option: ***alteration of default value, query, modification, deletion***, [***assignment: other operations***]] on security attribute [option: ***database object access permission, security role***].

FMT_MSA_EXT.1.2 TSF shall implement [option: ***label access control-based security policy***, [***assignment: information flow control policy with appointed mechanism by ST author***]]; merely through [option: ***LBAC authorized user***, [***assignment: authorized administrator appointed by ST author***]], implement [[assignment: ***security attribute***] to [assignment: ***security label***]].

NOTE: this requirement is applicable to EAL-4 evaluation assurance level.

7.1.3.3 Static attribute initialization [FMT_MSA_EXT.3]

FMT_MSA_EXT.3.1 TSF shall implement [option: ***user control policy-based, role control policy-based and user group control policy-based***, [***assignment: self-access control defined by ST author***]], so as to provide default value to the execution of SFP security attribute [option: select one of them: ***restricted, permitted***, [***assignment: other properties***]].

7.2 Requirements of Security Function

7.2.1 Overview

Table 7 lists TOE security functional components of evaluation assurance level (EAL) of DBMS: EAL2, EAL3 and EAL4. In the description of security functional component elements, in square brackets [], bold font signifies already completed operations; bold italics signifies assignment and options that still need to be determined by ST author in the security objectives.

7.2.2.3 Security audit review (FAU_SAR.1)

FAU_SAR.1.1 TSF shall provide [assignment: ***authorized administrator***] with the authority to read the audit record and acquire the audit information listed below:

a) User, user group or role identification;

b) Type of audit events;

c) Database object identification;

d) [option: ***subject identification, host identification, null***];

e) [option: ***successful auditable security event, failed auditable security event,*** and [option: [***assignment: list of selective audit events based on other selection conditions***], ***without any additional condition***]];

f) Database permission [option: ***system permission, instance permission, database permission, mode object permission, fine-grained data permission***].

FAU_SAR.1.2 TSF shall provide audit record in a mode that can be understood by authorized user.

7.2.2.4 Restriction of audit review (FAU_SAR.2)

FAU_SAR.2.1 authorizes specific permission of reading and accessing audit data to authorized administrator. Apart from this, TSF shall prohibit all the authorized users from reading or accessing audit record.

7.2.2.5 Optional audit review (FAU_SAR.3)

FAU_SAR.3.1 TSF shall provide the capability of [**searching and sequencing**] reviewed audit data in accordance with [**searching and classification conditions of the value in audit data field**].

7.2.2.6 Selective audit (FAU_SEL.1)

FAU_SEL.1.1 TSF shall be able to select auditable events from a set of auditable events in accordance with the following attributes:

a) User identity [option: ***object identity, user identity, group identity, subject identity, host identity***];

b) Operation type [option: ***definition statement, query statement, update statement, control statement***];

c) Permission level [option: ***system permission, instance permission, database permission, mode object level audit, fine-grained data***

organization in accordance with the specific condition of cryptographic algorithm.

7.2.3.2 Key destruction (FCS_CKM.4)

FCS_CKM.4.1 TSF shall destruct keys in accordance with a specific key destruction method [assignment: ***key destruction method***] that complies with the following standard [assignment: ***cryptographic management-related standards or specifications requested by the state or the industry***].

7.2.3.3 Cryptographic operation (FCS_COP.1)

FCS_COP.1.1 TSF shall execute [assignment: ***cryptographic operation list***] in accordance with a specific cryptographic algorithm [assignment: ***cryptographic algorithm***] that complies with the following standard [assignment: ***cryptographic management-related standards or specifications requested by the state or the industry***]and key length [assignment: ***key length***].

7.2.4 User data protection (Type-FDP)

7.2.4.1 Subset access control (FDP_ACC.1)

FDP_ACC.1.1 TSF shall execute the following access control policy [option: ***user control policy-based, role control policy-based, user group control policy-based,*** [***assignment: self-access control policy defined by ST author***]] defined by subject (system and user) on authorized database object operation list.

7.2.4.2 Security attribute-based access control (FDP_ACF.1)

FDP_ACF.1.1 TSF shall execute access control on the operation of database object in accordance with [option: ***user control policy-based, role control policy-based, user group control policy-based,*** [***assignment: self-access control defined by ST author***]], which shall include the following:

a) Subject-related authorized user identity and/or role and/or group member relationship;

b) Executable access operation and/or role/group permission of controlled database object;

c) Controlled database object identification;

d) Execute [option: ***user control policy-based, role control policy-based, user group control policy-based,*** [***assignment: self-access control policy defined by ST author***]] on database object.

FDP_ACF.1.2 TSF shall execute [assignment: ***between controlled subject and controlled database object, manage access rules by adopting controlled operation on controlled database object***], so as to determine whether an operation

a) There is an ordered function which can determine whether two valid security attributes being provided are equivalent, whether one security attribute is larger than the other, or, whether they are incomparable;

b) A “minimum upper bound” exists in the security attribute set. In terms of two valid security attributes being provided, there is a valid security attribute that is larger than, or, equals to the two security attributes;

c) A “maximum lower bound” exists in the security attribute set. In terms of two valid security attributes being provided, there is a valid security attribute that is not larger than the two attributes.

7.2.4.5 User data output with security attribute (FDP_ETC.2)

Under SFP control, when FDP_ETC.2.1 outputs user data to beyond TOE, TSF shall execute [assignment: ***access control SFP and/or information flow control SFP***].

FDP_ETC.2.2 TSF shall output user data and user data-associated security attribute.

FDP_ETC.2.3 TSF shall ensure that when security attribute is output to beyond TOE, it is exactly associated with the output user data.

FDP_ETC.2.4 when user data is output from TOE, TSF shall execute the following rule [assignment: ***additional output control rule***].

7.2.4.6 User data input without security attribute (FDP_ITC.1)

Under SFP control, when FDP_ITC.1.1 inputs user data from beyond TOE, TSF shall execute [assignment: ***access control SFP and/or information flow control SFP***].

When FDP_ITC.1.2 inputs user data from beyond TOE, TSF shall neglect any security attribute associated with user data.

Under SPF control, when FDP_ITC.1.3 inputs user data from beyond TOE, TSF shall execute the following rule: [assignment: ***additional input control rule***].

7.2.4.7 Basic internal transmission protection (FDP_ITT.1)

When FDP_ITT.1.1 transmits user data among physically divided parts on TOE, TSF shall execute [assignment: ***access control SFP and/or information flow control SFP***] to prevent [option: ***leakage, tampering, loss of availability***] of user data.

7.2.4.8 Subset residual information protection (FDP_RIP.1)

FDP_RIP.1.1 TSF shall ensure that any prior information content of server resources (such as: database server shared cache and storage space) is no longer available after the release of the resources, or, after the resources are re-allocated to other model objects.

d) Server resource restriction;

e) Database object access permission;

f) Database management permission;

g) [assignment: ***any additional security attribute of authorized administrator***].

7.2.5.3 Verification of secrets (FIA_SOS.1)

FIA_SOS.1.1 TSF shall provide a mechanism to verify that secrets can satisfy [assignment: an established quality measurement]. For example, the verification of user commands shall satisfy:

a) Be restricted between the minimum and the maximum number of character length;

b) Contain a combination of uppercase and lowercase characters;

c) At least contain a numeric character;

d) At least contain a special character;

e) Cannot be user identification or username;

f) Be restricted within a period of validity;

g) Previously used command can no longer be used again within XX days.

7.2.5.4 Timing of authentication (FIA_UAU.1)

Before database user identity is authenticated, FIA_UAU.1.1 TSF shall allow the execution of [assignment: ***action list facilitated by TSF***], which represents the user. For example:

a) Obtain information of the current DBMS version;

b) Establish database connection;

c) If it is unsuccessful, return error message.

Before allowing the execution of database user's database requested actions, FIA_UAU.1.2 TSF shall request this user to be already successfully authenticated.

NOTE: this component directs at TOE locally authenticated users, which do not include management and control data package transmitted between the client-side and DBMS prior to the authentication.

configuration parameter];

b) Restricted enable/disable security functions for authorized administrator [assignment: ***relevant event audit specifications***];

c) Configuration [assignment: ***execution behavior***] management in security warning events;

d) Management [assignment: ***take action***] in authentication failure events;

e) Management [assignment: ***take action***] before user is successfully authenticated;

f) If authorized administrator can modify the list of actions adopted by user before being identified, conduct management [assignment: ***action***] of authorized administrator;

g) Conditional management in data and operation integrity self-check [option: ***initialization start, periodic interval, other specific conditions***] of DBMS management;

h) Additional [assignment: ***security function list***] management in ST.

7.2.6.2 TSF data management (FMT_MTD.1)

FMT_MTD_EXT.1.1 TSF shall be merely restricted to authorized administrator with [option: ***system administrator, security administrator,*** [***assignment: authorized security administrator***]] role to [assignment: ***alter default value, query, modify, delete,*** [***or add***]] [option: ***user identification, user group member, security role***].

FMT_MTD_EXT.1.2 TSF shall be merely restricted to authorized administrator with [option: ***system administrator, security administrator,*** [assignment: ***authorized security administrator***]] role to [assignment: ***alter default value, modify, delete,*** [***or add***]] [**authentication data**] of authorized user.

FMT_MTD_EXT.1.3 TSF shall be merely restricted to authorized administrator with [option: ***system administrator, security administrator,*** [***assignment: authorized security administrator***]] role to [assignment: ***include or eliminate auditable policy***].

FMT_MTD_EXT.1.4 TSF shall be merely restricted to authorized administrator with [option: ***system administrator, security administrator,*** [***assignment: authorized security administrator***]] role to [**delete** and [**check**]] [***auditable event set in audit trail***].

FMT_MTD_EXT.1.5 TSF shall base on [assignment: ***security metadata list defined by ST author***], be merely restricted to [option: ***system administrator, security administrator***, [***assignment: authorized security administrator***]] to execute operation [option: ***alter default value, query, modify, delete, eliminate***, [***assignment:***

n) Establish and delete label-based access control (LBAC) policy and label;

o) Authorize and revoke the binding of LBAC security label, and controlled subject and controlled object;

p) Establish, delete, authorize and revoke database role;

q) Authorize and revoke database administrator's access attribute;

r) Manage database user's password policy;

s) Manage database user's maximum limit of system resource utilization.

7.2.6.5 Security role (FMT_SMR.1)

FMT_SMR.1.1 TSF shall maintain role [assignment: ***already identified authorized role or group***]. For example, the following database security management roles or groups:

a) Security administrator;

b) Audit administrator;

c) Database administrator;

d) System administrator;

e) Security role or group defined by authorized security administrator.

FMT_SMR.2.2 TSF shall be able to associate user with role or group.

7.2.6.6 Security role restriction (FMT_SMR.2)

FMT_SMR.2.1 TSF shall maintain role [assignment: ***already identified authorized role or group***]. For example, the following database security management roles or groups:

a) Security administrator;

b) Audit administrator;

c) Database administrator;

d) System administrator;

e) Security role or group defined by authorized security administrator.

FMT_SMR.2.2 TSF shall be able to associate user with role or group.

FMT_SMR.2.3 TSF shall ensure the conditions [assignment: ***conditions of different***

7.2.8.1 Downgraded fault tolerance (FRU_FLT.1)

FRU_FLT.1.1 TSF shall ensure when the following failure [assignment: ***list of failure types***] occurs, [assignment: ***list of TOE capabilities***] can normally operate.

7.2.8.2 Minimum and maximum quota (FRU_RSA.2)

FRU_RSA.2.1 TSF shall allocate the maximum quota to the following resources of database server: [option: ***physical I/O, logical I/O, persistent storage space, temporary storage space, continuous usage time or unused time of a specific transaction,*** [***assignment: resource list defined and appointed by ST***]], so that [option: ***single user, pre-defined user, subject***] can be used [option: ***within an appointed time interval***].

FRU_RSA.2.2 TSF shall ensure the minimum supply of the following resources of database server: [option: ***physical I/O, logical I/O, persistent storage space, temporary storage space, continuous usage time or unused time of a specific transaction,*** [***assignment: resource list defined and appointed by ST***]], so that [option: ***single user, pre-defined user group, subject***] can be used [option: ***simultaneously, within an appointed time interval***].

7.2.9 TOE access (Type-FTA)

7.2.9.1 Restriction of optional attribute range (FTA_LSA.1)

FTA_LSA.1.1 TSF shall base on [assignment: ***attribute***] to restrict the range of the security attribute of the following sessions: [assignment: ***session security attribute***].

7.2.9.2 Basic restriction of multiple concurrent sessions (FTA_MCS.1)

FTA_MCS.1.1 TSF shall restrict the maximum number of concurrent sessions that belong to the same user.

FTA_MCS.1.2 TSF shall restrict [assignment: ***default number***] of sessions of each user by default.

7.2.9.3 Termination of TSF original session (FTA_SSL.3)

FTA_SSL.3.1 TSF shall terminate an interactive session after reaching [assignment: ***user inactivity interval***].

7.2.9.4 TOE access history (FTA_TAH.1)

Based on successful establishment of session, FTA_TAH.1.1 TSF shall display [assignment: ***date, time, access application program, IP address and access method***] of the previous successfully established session to user.

Based on successful establishment of session, FTA_TAH.1.2 TSF shall display

the content and form requirement of evidence.

7.3.2.2 Specification of security execution function (ADV_FSP.2)

Developer's behavioral element:

ADV_FSP.2.1D Developer shall provide a specification of function.

ADV_FSP.2.2D Developer shall provide traceability of function specification to security functional requirement.

Content and form element:

ADV_FSP.2.1C Function specification shall completely describe TSF.

ADV_FSP.2.2C Function specification shall describe all the objectives and application methods of TSFI.

ADV_FSP.2.3C Function specification shall identify and describe all the relevant parameters of TSFI.

ADV_FSP.2.4C In terms of each SFR-execution TSFI, function specification shall describe TSFI-related SFR-execution behavior.

ADV_FSP.2.5C In terms of SFR-execution TSFI, function specification shall describe direct error information caused by relevant processing of SFR-execution behavior.

ADV_FSP.2.6C Function specification shall demonstrate traceability of security functional requirement to TSFI.

Evaluator's behavioral element:

ADV_FSP.2.1E Evaluator shall confirm that the provided information satisfies all the content and form requirements of the evidence.

ADV_FSP.2.2E Evaluator shall confirm that function specification is an accurate and complete instantiation of security functional requirement.

7.3.2.3 Function specification with complete abstract (ADV_FSP.3)

Developer's behavioral element:

ADV_FSP.3.1D Developer shall provide a specification of function.

ADV_FSP.3.2D Developer shall provide traceability of function specification to security functional requirement.

Content and form element:

describe all the TSFI-related behaviors.

ADV_FSP.4.5C Function specification shall describe all the direct error information that might be caused by the invocation of each TSFI.

ADV_FSP.4.6C Function specification shall verify traceability of security functional requirement to TSFI.

Evaluator's behavioral element:

ADV_FSP.4.1E Evaluator shall confirm that the provided information satisfies all the content and form requirements of the evidence.

ADV_FSP.4.2E Evaluator shall confirm that function specification is an accurate and complete instantiation of security functional requirement.

7.3.2.5 TSF implementation representation (ADV_IMP.1)

ADV_IMP.1.1D Developer shall provide implementation representation to all the TSFs.

ADV_IMP.1.2 Developer shall provide mapping between TOE design description and implementation representation instance.

Content and form element:

ADV_IMP.1.1C Implementation representation shall define TSF in accordance with the level of detail; the degree of detail shall be able to generate TSF without any further design.

ADV_IMP.1.2C Implementation representation shall be provided in the form adopted by developer.

ADV_IMP.1.3C The mapping between TOE design description and implementation representation instance shall be able to prove their consistency.

Evaluator's behavioral element:

ADV_IMP.1.1E In terms of selected implementation representation instance, evaluator shall confirm that the provided information satisfies all the content and form requirements of the evidence.

7.3.2.6 Fundamental design (ADV_TDS.1)

Developer's behavioral element:

ADV_TDS.1.1D Developer shall provide TOE design.

ADV_TDS.1.2D Developer shall provide the mapping from TSFI of function specification to the lowest level of decomposition obtained from TOE design.

ADV_TDS.2.5C Design shall summarize SFR-supported and SFR-irrelevant behaviors of SFR-execution subsystem.

ADV_TDS.2.6C Design shall summarize the behaviors of SFR-supported subsystem.

ADV_TDS.2.7C Design shall describe the interaction among all the subsystems of TSF.

ADV_TDS.2.8C The mapping relation shall verify that all the behaviors described in TOE design can be mapped to TSFI that invokes it.

Evaluator's behavioral element:

ADV_TDS.2.1E Evaluator shall confirm that the provided information satisfies all the content and form requirements of the evidence.

ADV_TDS.2.2E Evaluator shall confirm that design is an accurate and complete instantiation of all the security functional requirements.

7.3.2.8 Fundamental module design (ADV_TDS.3)

Developer's behavioral element:

ADV_TDS.3.1D Developer shall provide TOE design.

ADV_TDS.3.2D Developer shall provide the mapping from TSFI of function specification to the lowest level of decomposition obtained from TOE design.

Content and form element:

ADV_TDS.3.1C Design shall describe TOE structure in accordance with subsystem.

ADV_TDS.3.2C Design shall describe TSF in accordance with module.

ADV_TDS.3.3C Design shall identify all the subsystems of TSF.

ADV_TDS.3.4C Design shall describe each subsystem of TSF.

ADV_TDS.3.5C Design shall describe the interaction among all the subsystems of TSF.

ADV_TDS.3.6C Design shall provide the mapping relation between TSF subsystem and TSF module.

ADV_TDS.3.7C Design shall describe each SFR-execution module, including its objective and the interaction with other modules.

ADV_TDS.3.8C Design shall describe each SFR-execution module, including its security functional requirement-related interface, returned value of other interfaces, the interaction with other modules, and the invoked interface.

AGD_OPE.1.7C User operation guidance shall be explicit and reasonable.

Evaluator's behavioral element:

AGD_OPE.1.1E Evaluator shall confirm that the provided information satisfies all the content and form requirements of the evidence.

7.3.3.2 Preparation procedure (AGD_PRE.1)

Developer's behavioral element:

AGD_PRE.1.1D Developer shall provide TOE, including its preparation procedure.

Content and form element:

AGD_PRE.1.1C Preparation procedure shall describe all the steps that are indispensable to the secure acceptance and delivery of TOE and are consistent with developer's delivery procedure.

AGD_PRE.1.2C Preparation procedure shall describe all the steps of secured installation and preparation of TOE, and operating environment that is consistent with the security objectives described in ST.

Evaluator's behavioral element:

AGD_PRE.1.1E Evaluator shall confirm that the provided information satisfies all the content and form requirements of the evidence.

AGD_PRE.1.2E Evaluator shall adopt the preparation procedure to confirm that TOE operation can be securely prepared.

7.3.4 Life cycle support (Type-ALC)

7.3.4.1 Application of CM system (ALC_CMC.2)

Developer's behavioral element:

ALC_CMC.2.1D Developer shall provide TOE and its reference No.

ALC_CMC.2.2D Developer shall provide CM document.

ALC_CMC.2.3D Developer shall adopt CM system.

Content and form element:

ALC_CMC.2.1C shall identify TOE with a unique reference No.

ALC_CMC.2.2C CM document shall describe the method for unique identification configuration item.

This is an excerpt of the PDF (Some pages are marked off intentionally)

------ The End ------