Security Requirement Templates based on CC

We provide 36 Security Functionalities(SF), which can correspond to the Functional Family in the second part of the CC (Common Criteria) standard. Each SF has a brief introduction and one or a group of security requirements templates (based on Functional Elements of CC), which can support one or more security objectives respectively. The mapping relationship among SF, Functional Family and Security Objectives can be seen in Appendix I. Each security requirement template has its matching conditions and placeholders to be filled in.

Content

SF.1 Security audit data generation

SF Introduction:

This SF defines requirements for recording the occurrence of security relevant events.

Security Control Scope 1:

Security objects:

Accountability

Matching conditions:

<actions>

Security requirement:

The SF shall be able to generate an audit record of the following events: [assignment: <events>], within each audit record at least the following information: Date and time of the event, type of event, subject identity (identified users, if applicable), and the outcome (success or failure) of the event.

SF.2 Non-repudiation of origin

SF Introduction:

Non-repudiation of origin ensures that the originator of information cannot successfully deny having sent the information. This SF requires that the SF provide a method to ensure that a subject that receives information during a data exchange is provided with evidence of the origin of the information. This evidence can then be verified by either this subject or other subjects.

Security Control Scope 1:

Security objects:

Accountability

Matching conditions:

<actions>=send,receive,transmit

Security requirement:

The SF shall be able to generate evidence of origin for transmitted [assignment: <information>] at the request of the [selection: <originator>, <recipient>, <third parties>].

SF.3 Non-repudiation of receipt

SF Introduction:

Non-repudiation of receipt ensures that the recipient of information cannot successfully

deny receiving the information. This SF requires that the SF provide a method to ensure that a subject that transmits information during a data exchange is provided with evidence of receipt of the information. This evidence can then be verified by either this subject or other subjects.

Security Control Scope 1:

Security objects:

Accountability

Matching conditions:

<actions>=send,receive,transmit

Security requirement:

The SF shall be able to generate evidence of receipt for received [assignment: <information>] at the request of the [selection: <originator>, <recipient>, <third parties>].

SF.4 Cryptographic operation

SF Introduction:

In order for a cryptographic operation to function correctly, the operation must be performed in accordance with a specified algorithm and with a cryptographic key of a specified size. Typical cryptographic operations include data encryption and/or decryption, digital signature generation and/or verification, cryptographic checksum generation for integrity and/or verification of checksum, secure hash (message digest), cryptographic key encryption and/or decryption, and cryptographic key agreement.

Security Control Scope 1:

Security objects:

Confidentiality

Matching conditions:

<information>

Security requirement:

The SF shall perform [assignment: <cryptographic operations>] on [assignment: <information>] in accordance with a specified cryptographic algorithm: [assignment: <cryptographic algorithm>] and cryptographic key sizes: [assignment: <cryptographic key sizes>] that meet the following: [assignment: <standards>].

Cryptographic keys must be managed throughout their life cycle：

The SF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm: [assignment: <cryptographic key generation algorithm>] and specified cryptographic key sizes: [assignment: <cryptographic key sizes>] that meet the [assignment: <standards>].

The SF shall distribute cryptographic keys in accordance with a specified cryptographic key distribution method: [assignment: <cryptographic key distribution method>] that

meets the [assignment: <standards>].
The SF shall perform [assignment: <type of cryptographic key access>] in accordance with a specified cryptographic key access method: [assignment: <cryptographic key access method>] that meets the [assignment: <standards>].
The SF shall destroy cryptographic keys in accordance with a specified cryptographic key destruction method: [assignment: <cryptographic key destruction method>] that meets the [assignment: <standards>].

SF.5 Access control policy

SF Introduction:

This SF identifies the access control SFPs (by name) and defines the scope of control of the policies that form the identified access control portion of the SFRs related to the SFP. This scope of control is characterised by three sets: the subjects under control of the policy, the objects under control of the policy, and the operations among controlled subjects and controlled objects that are covered by the policy. The criteria allows multiple policies to exist, each having a unique name.

Security Control Scope 1:

Security objects:

Confidentiality

Matching conditions:

<subjects> and <actions> and <objects>

Security requirement:

The SF shall enforce the [assignment: <access control SFP>] on [assignment: <events>].

SF.6 Data authentication

SF Introduction:

Data authentication permits an entity to accept responsibility for the authenticity of information (e.g., by digitally signing it). This SF provides a method of providing a guarantee of the validity of a specific unit of data that can be subsequently used to verify that the information content has not been forged or fraudulently modified.

Security Control Scope 1:

Security objects:

Integrity

Matching conditions:

<objects> or <information>

Security requirement:

The SF shall provide a capability to generate evidence that can be used as a guarantee of the validity of [assignment: <objects>, <information>].

Security Control Scope 2:

Security objects:

Identification & Authentication, Accountability

Matching conditions:

<subjects> and <information>

Security requirement:

The SF shall provide [assignment: <subjects>] with the ability to verify evidence of the validity of the indicated [assignment: <information>] and the identity of the user that generated the evidence.

SF.7 Export from the TOE

SF Introduction:

This SF defines functions for SF-mediated exporting of user data from the TOE.

Security Control Scope 1:

Security objects:

Confidentiality

Matching conditions:

<actions>=export

Security requirement:

The SF shall enforce the [assignment: <access control SFP>, <information flow control SFP>] when exporting user data outside of the TOE.

SF.8 Information flow control policy

SF Introduction:

This SF identifies the information flow control SFPs (by name) and defines the scope of control for each named information flow control SFP. This scope of control is characterised by three sets: the subjects under control of the policy, the information under control of the policy, and operations which cause controlled information to flow to and from controlled subjects covered by the policy. The criteria allows multiple policies to exist, each having a unique name.

Security Control Scope 1:

Security objects:

Confidentiality

Matching conditions:

<subjects> and <actions> and <information>

Security requirement:

The SF shall enforce the [assignment: <information flow control SFP>] on [assignment: <events>].

SF.9 Import from outside of the TOE

SF Introduction:

This SF defines the mechanisms for SF-mediated importing of user data into the TOE such that it has appropriate security attributes and is appropriately protected. It is concerned with limitations on importation, determination of desired security attributes, and interpretation of security attributes associated with the user data.

Security Control Scope 1:

Security objects:

Confidentiality

Matching conditions:

<actions>=import

Security requirement:

The SF shall enforce the [assignment: <access control SFP>, <information flow control SFP>] when importing user data, controlled under the SFP, from outside of the TOE.

SF.10 Internal TOE transfer

SF Introduction:

This SF provides requirements that address protection of user data when it is transferred between separated parts of a TOE across an internal channel.

Security Control Scope 1:

Security objects:

Confidentiality, Integrity

Matching conditions:

<actions>=transmit

Security requirement:

The SF shall enforce the [assignment: <access control SFP>, <information flow control SFP>] to prevent the [selection: <disclosure>, <modification>] of user data when it is transmitted between physically-separated parts of the TOE.

SF.11 Residual information protection

SF Introduction:

This SF addresses the need to ensure that any data contained in a resource is not available when the resource is de-allocated from one object and reallocated to a different object.

Security Control Scope 1:

Security objects:

Availability

Matching conditions:

<actions>=allocate

Security requirement:

The SF shall ensure that any previous information content of a resource is made unavailable upon the [selection: <allocation of the resource to>, <deallocation of the resource from>] the following objects: [assignment: <objects>].

SF.12 Rollback

SF Introduction:

The rollback operation involves undoing the last operation or a series of operations, bounded by some limit, such as a period of time, and return to a previous known state. Rollback provides the ability to undo the effects of an operation or series of operations to preserve the integrity of the user data.

Security Control Scope 1:

Security objects:

Integrity

Matching conditions:

<actions>=rollback,revoke

Security requirement:

The SF shall enforce [assignment: <access control SFP>, <information flow control SFP>] to permit the rollback of the [assignment: <actions>] on the [assignment: <information>, <objects>].

SF.13 Stored data integrity

SF Introduction:

This SF provides requirements that address protection of user data while it is stored

within containers controlled by the SF. Integrity errors may affect user data stored in memory, or in a storage device.

Security Control Scope 1:

Security objects:

Integrity

Matching conditions:

<actions>=store

Security requirement:

The SF shall monitor user data stored in containers controlled by the SF for integrity errors on all objects, based on the following attributes: [assignment: <user data attributes>].

SF.14 Inter-SF user data confidentiality transfer protection

SF Introduction:

This SF defines the requirements for ensuring the confidentiality of user data when it is transferred using an external channel between the TOE and another trusted IT product.

Security Control Scope 1:

Security objects:

Confidentiality

Matching conditions:

<actions>=transmit,receive

Security requirement:

The SF shall enforce the [assignment: <access control SFP>, <information flow control SFP>] to [selection: <transmit>, <receive>] user data in a manner protected from unauthorised disclosure.

SF.15 Inter-SF user data integrity transfer protection

SF Introduction:

This SF defines the requirements for providing integrity for user data in transit between the TOE and another trusted IT product and recovering from detectable errors. At a minimum, this SF monitors the integrity of user data for modifications.

Security Control Scope 1:

Security objects:

Confidentiality, Integrity

Matching conditions:

<actions>=transmit,receive

Security requirement:

The SF shall enforce the [assignment: <access control SFP>, <information flow control SFP>] to [selection: <transmit>, <receive>] user data in a manner protected from [selection: <modification>, <deletion>, <insertion>, <replay>] errors.

SF.16 Authentication failures

SF Introduction:

This SF contains requirements for defining values for some number of unsuccessful authentication attempts and SF actions in cases of authentication attempt failures.

Security Control Scope 1:

Security objects:

Identification & Authentication

Matching conditions:

<key words>=authentication

Security requirement:

The SF shall define maximum number of unsuccessful authentication attempts, When the number has been [selection: <met>, <surpassed>], the SF shall [assignment: <actions>].

SF.17 User attribute definition

SF Introduction:

All authorised users may have a set of security attributes, other than the user's identity, that is used to enforce the SFRs. This SF defines the requirements for associating user security attributes with users as needed to support the SF in making security decisions.

Security Control Scope 1:

Security objects:

Identification & Authentication

Matching conditions:

<users>

Security requirement:

The SF shall maintain the following security attributes belonging to individual users:

[assignment: <security attributes>].

SF.18 Specification of secrets

SF Introduction:

This SF defines requirements for mechanisms that enforce defined quality metrics on provided secrets and generate secrets to satisfy the defined metric.

Security Control Scope 1:

Security objects:

Identification & Authentication

Matching conditions:

<key words>=secret,password

Security requirement:

The SF shall provide a mechanism to generate secrets that meet [assignment: <a defined quality metric>].

SF.19 User authentication

SF Introduction:

This SF defines the types of user authentication mechanisms supported by the SF. This SF also defines the required attributes on which the user authentication mechanisms must be based.

Security Control Scope 1:

Security objects:

Identification & Authentication

Matching conditions:

<actions>

Security requirement:

The SF shall require each user to be successfully authenticated before [assignment: <actions>].

SF.20 User identification

SF Introduction:

This SF defines the conditions under which users shall be required to identify themselves before performing any other actions that are to be mediated by the SF and which require

user identification.

Security Control Scope 1:

Security objects:

Identification & Authentication

Matching conditions:

<actions>

Security requirement:

The SF shall require each user to be successfully identified before [assignment: <actions>].

SF.21 User-subject binding

SF Introduction:

An authenticated user, in order to use the TOE, typically activates a subject. The user's security attributes are associated (totally or partially) with this subject. This SF defines requirements to create and maintain the association of the user's security attributes to a subject acting on the user's behalf.

Security Control Scope 1:

Security objects:

Identification & Authentication

Matching conditions:

<subjects>

Security requirement:

The SF shall associate the following user security attributes with subjects acting on the behalf of that user: [assignment: <user security attributes>].

SF.22 Anonymity

SF Introduction:

This SF ensures that a user may use a resource or service without disclosing the user's identity. The requirements for Anonymity provide protection of the user identity. Anonymity is not intended to protect the subject identity.

Security Control Scope 1:

Security objects:

Privacy

Matching conditions:

<subjects>

Security requirement:

The SF shall ensure that [assignment: <users>, <subjects>] are unable to determine the real user name bound to [assignment: <subjects>, <events>, <objects>].

SF.23 Pseudonymity

SF Introduction:

This SF ensures that a user may use a resource or service without disclosing its user identity, but can still be accountable for that use.

Security Control Scope 1:

Security objects:

Privacy

Matching conditions:

<subjects>

Security requirement:

The SF shall be able to provide [assignment: <aliases>] of the real user name to [assignment: <subjects>].

SF.24 Unlinkability

SF Introduction:

This SF ensures that a user may make multiple uses of resources or services without others being able to link these uses together.

Security Control Scope 1:

Security objects:

Privacy

Matching conditions:

<subjects>

Security requirement:

The SF shall ensure that [assignment: <users>, <subjects>] are unable to determine whether [assignment: <actions>] were caused by the same user.

SF.25 Unobservability

SF Introduction:

This SF ensures that a user may use a resource or service without others, especially third

parties, being able to observe that the resource or service is being used.

Security Control Scope 1:

Security objects:

Privacy

Matching conditions:

<subjects>

Security requirement:

The SF shall ensure that [assignment: <users>, <subjects>] are unable to observe the operation [assignment: <actions>] on [assignment: <objects>] by [assignment: <users>, <subjects>].

SF.26 Fault tolerance

SF Introduction:

The requirements of this SF ensure that the TOE will maintain correct operation even in the event of failures.

Security Control Scope 1:

Security objects:

Availability

Matching conditions:

<actions>

Security requirement:

The SF shall ensure [assignment: <actions>, <resources>] when the following failures occur: [assignment: <failures>].

SF.27 Priority of service

SF Introduction:

The requirements of this SF allow the SF to control the use of resources under the control of the SF by users and subjects such that high priority activities under the control of the SF will always be accomplished without undue interference or delay caused by low priority activities.

Security Control Scope 1:

Security objects:

Availability

Matching conditions:

<subjects> or <users>

Security requirement:

The SF shall ensure that each access to [assignment: <resources>] shall be mediated on the basis of the subjects assigned priority.

SF.28 Resource allocation

SF Introduction:

The requirements of this SF allow the SF to control the use of resources by users and subjects such that denial of service will not occur because of unauthorised monopolisation of resources.

Security Control Scope 1:

Security objects:

Availability

Matching conditions:

<subjects> or <users>

<resources>=resource,service

Security requirement:

The SF shall ensure the provision of minimum and maximum quantity of each [assignment: <resource>] that is available for [selection: <an individual user>, <defined group of users>, <subjects>] to use [selection: <simultaneously>, <over a specified period of time>].

SF.29 Limitation on scope of selectable attributes

SF Introduction:

This SF defines requirements to limit the scope of session security attributes that a user may select for a session.

Security Control Scope 1:

Security objects:

Identification & Authentication

Matching conditions:

<key words>=session

Security requirement:

The SF shall restrict the scope of the session security attributes [assignment: <session security attributes>], based on [assignment: <attributes>].

SF.30 Limitation on multiple concurrent sessions

SF Introduction:

This SF defines requirements to place limits on the number of concurrent sessions that belong to the same user.

Security Control Scope 1:

Security objects:

Identification & Authentication, Availability

Matching conditions:

<key words>=session

<users>

Security requirement:

The SF shall restrict the maximum number of concurrent sessions that belong to the same user.

SF.31 Session locking and termination

SF Introduction:

This SF defines requirements for the SF to provide the capability for SF-initiated and user-initiated locking, unlocking, and termination of interactive sessions.

Security Control Scope 1:

Security objects:

Identification & Authentication, Availability, Confidentiality

Matching conditions:

<key words>=session

<actions>

Security requirement:

The SF shall lock an interactive session after [assignment: <time interval of user inactivity>] by:clearing or overwriting display devices, making the current contents unreadable;disabling any activity of the user's data access/display devices other than unlocking the session.

Security Control Scope 2:

Security objects:

Identification & Authentication, Availability, Confidentiality

Matching conditions:

<key words>=session

<users>

Security requirement:

The SF shall allow user-initiated locking of the user's own interactive session, by:clearing or overwriting display devices, making the current contents unreadable;disabling any activity of the user's data access/display devices other than unlocking the session.

Security Control Scope 3:

Security objects:

Identification & Authentication

Matching conditions:

<key words>=session

<users>

Security requirement:

The SF shall terminate an interactive session after a [assignment: <time interval of user inactivity>].

Security Control Scope 4:

Security objects:

Identification & Authentication

Matching conditions:

<key words>=session

<users>

Security requirement:

The SF shall allow user-initiated termination of the user's own interactive session.

SF.32 TOE access banners

SF Introduction:

This SF defines requirements to display a configurable advisory warning message to users regarding the appropriate use of the TOE.

Security Control Scope 1:

Security objects:

Confidentiality

Matching conditions:

<key words>=session,system

<users>

Security requirement:

Before establishing a user session, the SF shall display an advisory warning message regarding unauthorised use of the TOE.

SF.33 TOE access history

SF Introduction:

This SF defines requirements for the SF to display to a user, upon successful session establishment, a history of successful and unsuccessful attempts to access the user's account.

Security Control Scope 1:

Security objects:

Confidentiality, Accountability

Matching conditions:

<key words>=session

<users>

Security requirement:

Upon successful session establishment, the SF shall display the [selection: <date>, <time>, <method>, <location>] of the last session establishment to the user.

SF.34 TOE session establishment

SF Introduction:

This SF defines requirements to deny a user permission to establish a session with the TOE.

Security Control Scope 1:

Security objects:

Identification & Authentication, Availability

Matching conditions:

<key words>=session,establishment

<users>

Security requirement:

The SF shall be able to deny session establishment based on [assignment: <attributes>].

SF.35 Inter-SF trusted channel

SF Introduction:

This SF defines requirements for the creation of a trusted channel between the SF and other trusted IT products for the performance of security critical operations. This SF should be included whenever there are requirements for the secure communication of user or SF data between the TOE and other trusted IT products.

Security Control Scope 1:

Security objects:

Confidentiality, Integrity

Matching conditions:

<key words>=channel,communication

<actions>

<system>=system,other systems,IT product,application

Security requirement:

The SF shall provide a communication channel between itself and another 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.

SF.36 Trusted path

SF Introduction:

This SF defines the requirements to establish and maintain trusted communication to or from users and the SF. A trusted path may be required for any security-relevant interaction. Trusted path exchanges may be initiated by a user during an interaction with the SF, or the SF may establish communication with the user via a trusted path.

Security Control Scope 1:

Security objects:

Confidentiality, Integrity

Matching conditions:

<key words>=path,communication

<users>

Security requirement:

The SF shall provide a communication path between itself and [selection: <remote>, <local>] users that is logically distinct from other communication paths and provides assured identification of its end points and protection of the communicated data from [selection: <modification>, <disclosure>, <confidentiality violation>]].

Appendix I

The mapping relationship among SF, Functional Family and Security Objectives.

Functional Family	SF	Identification & Authentication	Integrity	Availability	Privacy	Accountability	Confidentiality
FAU_GEN	SF.1					D	
FCO_NRO	SF.2					D	
FCO_NRR	SF.3					D	
FCS_COP	SF.4						D
FDP_ACC	SF.5						D
FDP_DAU	SF.6	D	D			D	
FDP_ETC	SF.7					D	D
FDP_IFC	SF.8						D
FDP_ITC	SF.9					D	D
FDP_ITT	SF.10		D			D	D
FDP_RIP	SF.11			D			
FDP_ROL	SF.12		D				
FDP_SDI	SF.13		D				
FDP_UCT	SF.14					D	D
FDP_UIT	SF.15		D			D	D
FIA_AFL	SF.16	D					
FIA_ATD	SF.17	D					
FIA_SOS	SF.18	D					
FIA_UAU	SF.19	D					
FIA_UID	SF.20	D					
FIA_USB	SF.21	D					
FPR_ANO	SF.22				D		
FPR_PSE	SF.23				D		
FPR_UNL	SF.24				D		
FPR_UNO	SF.25				D		
FRU_FLT	SF.26			D			
FRU_PRS	SF.27			D			
FRU_RSA	SF.28			D			
FTA_LSA	SF.29	D					
FTA_MCS	SF.30	D		D			
FTA_SSL	SF.31	D		D			D
FTA_TAB	SF.32						D
FTA_TAH	SF.33					D	D
FTA_TSE	SF.34	D		D			
FTP_ITC	SF.35		D				D
FTP_TRP	SF.36		D				D