

**Template for comments and secretariat observations
on CC:2022 Release 1 Part 2**

Date: 2023-03-17	Document: CC:2022 Release 1 Part 2	Project:
------------------	---	----------

MB/ NC ¹	Line number (e.g., 17)	Clause/ Subclause (e.g., 3.1)	Paragraph/ Figure/ Table/ (e.g. Table 1)	Type of comment ²	Comments	Proposed change	Observations of the secretariat
CCUF 01		11.9.5	FDP_ITC.1 Dependencies	ed	The dependencies list for SFR FDP_ITC.1 lists 'FMT_MSA.3 Static attribute initialization'. However, that SFR's name was changed in CC:2022 Release 1 Part 2 to 'Static attribute'	Change the entry in the dependencies list for SFR FDP_ITC.1 in Subclause 11.9.5 to 'FMT_MSA.3 Static attribute'	
CCUF 02		11.13.6	FDP_SDC.2 Dependencies	ed	The only dependencies listed for SFR FDP_SDC.2 is 'FCS_COP.1' without the full name of the SFR. This is inconsistent with SFRs listed as dependencies in all other SFRs which do give the full SFR name.	Change the SFR dependency listed for SFR FDP_SDC.2 to 'FCS_COP.1 Cryptographic operation'	
CCUF 03		15.3.4	Audit of FPT_FLS.1	ed	There is a typographical error at the end of the first sentence of this paragraph – it ends with "...in the PP, PP-Module, functional package or /ST". The '/' should not be there.	It should read "...in the PP, PP-Module, functional package or ST"	
CCUF 04		3	Terms and definitions	Te	Looking through the list of terms and definitions in Clause 3 and also in CC2022 Release 1 Part 1, the following important terms that are frequently used in CC2022 Release 1 Part 2 are not defined in Clause 3: <ul style="list-style-type: none"> • availability' • confidentiality • integrity • service 	Include the definitions of the four terms listed in the Comment in Clause 3 on CC2022 Release 1 Part 2	
CCUF 05		9.2.2	Components leveling and description (for Non-repudiation of origin (FCO_NRO))	Te	The summary of FCO_NRO.1 in Subclause 9.2.2 states: FCO_NRO.1 Selective proof of origin, requires the TSF to provide subjects with the capability to request evidence of the origin of information". Note that the summary of FCO_NRO.2 in Subclause 0.2.2 states: FCO_NRO.2 Enforced proof of origin, requires that the TSF always generate evidence of origin for transmitted information. The requirements in FCO_NRO.1.1 are: FCO_NRO.1.1 The TSF shall be able to generate evidence of origin for transmitted [assignment: list of information types] at the request of the [selection: originator, recipient, assignment: list of third parties]]. This means that FCO_NRO.1.1 deals with transmitted information also. The summary of FCO_NRO.1 in Subclause 9.2.2 should therefore also refer to transmitted information just as the summary for FCO_NRO.2 does.	Change the summary for FCO_NRO.1 in Subclause 9.2.2 to read: FCO_NRO.1 Selective proof of origin, requires the TSF to provide subjects with the capability to request evidence of the origin of transmitted information.	
CCUF 06		10.4.1	Family Behavior (for Random bit generation)	Te	The text in Subclause 10.4.1 states: Components in this family address the requirements for random	Change the text in Subclause 10.4.1 to read: Components in this family address the requirements for random	

1 **MB** = Member body / **NC** = National Committee (enter the ISO 3166 two-letter country code, e.g. CN for China; comments from the ISO/CS editing unit are identified by **)

2 **Type of comment:** **ge** = general **te** = technical **ed** = editorial

**Template for comments and secretariat observations
on CC:2022 Release 1 Part 2**

Date: 2023-03-17	Document: CC:2022 Release 1 Part 2	Project:
------------------	---	----------

MB/ NC ¹	Line number (e.g., 17)	Clause/ Subclause (e.g., 3.1)	Paragraph/ Figure/ Table/ (e.g. Table 1)	Type of comment ²	Comments	Proposed change	Observations of the secretariat
			(FCS_RBG))		bit/number generation. However, FCS_RBG only addresses random bit generation; there is a separate family FCS_RNG that addresses random number generation.	bit generation.	
CCUF 07		10.4.2	Components leveling and description (for Random bit generation (FCS_RBG))	Te	The summary for FCS_RBG.1 in Subclause 10.4.2 states: FCS_RBG.1 Random bit generation (RBG) requires random bit generation to be performed in accordance with selected standards. It also specifies whether the initial seeding is done via an internal or external noise source, as well as when and how an RBG's state is updated. However, the actual requirements in FCS_RBG.1 do not mention anything about whether the initial seeding is done via internal or external noise source; the requirements in FCS_RBG.1.2 just state: FCS_RBG.1.2 The TSF shall use a [selection: <i>TSF noise source</i> [assignment: <i>name of noise source</i>], <i>TSF interface for seeding</i>] for initialized seeding. Note that FCS_RBG.1.2 does not distinguish where the source comes from.	Change the second sentence in the summary for FCS_RBG.1 in Subclause 10.4.2 to read: It also specifies the noise sources, as well as when and how an RBG's state is updated.	
CCUF 08		11.8.2	Components leveling and description (for Information Retention Control (FDP_IRC))	Te	The summary for FDP_IRC.1 in Subclause 11.8.2 states FDP_IRC.1 Information retention control requires that the TSF ensure that any copy of a defined set of objects in the TOE is deleted when no longer strictly necessary for the operation of the TOE. However, the requirements FDP_IRC.1.1 and FDP_IRC.1.2 are: FDP_IRC.1.1 The TSF shall enforce the [assignment: <i>information erasure policy</i>] on a [assignment: <i>list of objects</i>] required for [assignment: <i>list of operations</i>] so that the selected objects are deleted irreversibly and untraceably from the TOE promptly upon termination of the selected operations. FDP_IRC.1.2 The TSF shall ensure that [assignment: <i>list of objects</i>] cannot be accessed after their release and prior to their irreversible and untraceable deletion. There is no mention of deleting copies of the defined objects in either FDP_IRC.1.1 or FDP_IRC.1.2.	Revise the summary for FDP_IRC.1 in Subclause 11.8.2 to read: FDP_IRC.1 Information retention control requires that the TSF ensure that a defined set of objects in the TOE is deleted when no longer strictly necessary for the operation of the TOE, and to identify and define the operations for which the object is required.	
CCUF 09		11.9.2	Components leveling and description (for	Te	The summary for FDP_ITC.1 in Subclause 11.9.2 states FDP_ITC.1 Import of user data without security attributes,	Revise the summary for FDP_ITC1 in Subclause 11.9.2 to read: FDP_ITC.1 Import of user data without security attributes,	

1 **MB** = Member body / **NC** = National Committee (enter the ISO 3166 two-letter country code, e.g. CN for China; comments from the ISO/CS editing unit are identified by **)

2 **Type of comment:** **ge** = general **te** = technical **ed** = editorial

**Template for comments and secretariat observations
on CC:2022 Release 1 Part 2**

Date: 2023-03-17	Document: CC:2022 Release 1 Part 2	Project:
------------------	---	----------

MB/ NC ¹	Line number (e.g., 17)	Clause/ Subclause (e.g., 3.1)	Paragraph/ Figure/ Table/ (e.g. Table 1)	Type of comment ²	Comments	Proposed change	Observations of the secretariat
			Import from outside of the TOE (FDP_ITC))		<p>requires that the security attributes correctly represent the user data and are supplied separately from the object.</p> <p>However, the requirements in FDP_ITC.1 are:</p> <p>FDP_ITC.1.1 The TSF shall enforce the [assignment: <i>access control SFP(s)</i> and/or <i>information flow control SFP(s)</i>] when importing user data, controlled under the SFP, from outside of the TOE.</p> <p>FDP_ITC.1.2 The TSF shall ignore any security attributes associated with the user data when imported from outside the TOE.</p> <p>FDP_ITC.1.3 The TSF shall enforce the following rules when importing user data controlled under the SFP from outside the TOE: [assignment: <i>additional importation control rules</i>].</p> <p>There is no indication in FDP_ITC.1.2 that the security attributes are supplied separately from the object; only that any association between security attributes and user data are ignored – there is no mention of any 'objects'; in either FDP_ITC.1.1, FDP_ITC.1.2 or FDP_ITC.1.3.</p>	requires that the security attributes correctly represent the user data and are supplied separately from the user data.	
CCUF 10		11.15.2	Components leveling and description (for Inter-TSF user data confidentiality transfer protection (FDP_UCT))	Te	<p>The summary for FDP_UCT.1 in Subclause 11.15.2 states:</p> <p>In FDP_UCT.1 Basic data exchange confidentiality, the goal is to provide protection from disclosure of user data while in transit.</p> <p>However, the requirement in FDP_UCT.1.1 state:</p> <p>FDP_UCT.1.1 The TSF shall enforce the [assignment: <i>access control SFP(s)</i> and/or <i>information flow control SFP(s)</i>] to [selection: <i>transmit, receive</i>] user data in a manner protected from unauthorized disclosure.</p> <p>The 'unauthorized disclosure' aspect is important and should be indicated in the summary for FDP_UCT.1 in Subclause 11.15.2.</p>	<p>Revise the summary for FDP_UCT.1 in Subclause 11.15.2 to read:</p> <p>In FDP_UCT.1 Basic data exchange confidentiality, the goal is to provide protection from unauthorized disclosure of user data while in transit.</p>	
CCUF 11		12.2.2	Components leveling and description (for Authentication failures (FIA_AFL))	Te	<p>The summary for FIA_AFL.1 in Subsection 12.2.2 states:</p> <p>FIA_AFL.1 Authentication failure handling, requires that the TSF be able to terminate the session establishment process after a specified number of unsuccessful user authentication attempts. It also requires that, after termination of the session establishment process, the TSF be able to disable the user account or the point of entry from which the attempts were made until an administrator-defined condition occurs.</p> <p>The actual requirements for FIA_AFL.1 are:</p>	Delete the second sentence from the summary of FIA_AFL.1 in Subclause 12.2.2.	

¹ **MB** = Member body / **NC** = National Committee (enter the ISO 3166 two-letter country code, e.g. CN for China; comments from the ISO/CS editing unit are identified by **)

² **Type of comment:** **ge** = general **te** = technical **ed** = editorial

**Template for comments and secretariat observations
on CC:2022 Release 1 Part 2**

Date: 2023-03-17	Document: CC:2022 Release 1 Part 2	Project:
------------------	---	----------

MB/ NC ¹	Line number (e.g., 17)	Clause/ Subclause (e.g., 3.1)	Paragraph/ Figure/ Table/ (e.g. Table 1)	Type of comment ²	Comments	Proposed change	Observations of the secretariat
					<p>FIA_AFL.1.1 The TSF shall detect when [selection: [assignment: <i>positive integer number</i>], an administrator configurable positive integer within [assignment: <i>range of acceptable values</i>]] unsuccessful authentication attempts occur related to [assignment: <i>list of authentication events</i>].</p> <p>FIA_AFL.1.2 When the defined number of unsuccessful authentication attempts has been [selection: <i>met, surpassed</i>], the TSF shall [assignment: <i>list of actions</i>].</p> <p>Note that the requirement to disable the user account or the point of entry from which attempts were made after termination of the session establishment process is not in either FIA_AFL.1.1 or FIA_AFL.1.2.;</p>		
CCUF 12		13.2.2	Components leveling and description (for Limited capabilities and availability (FMT_LIM))	Te	<p>The summary for FMT_LIM.1 in Subclause 13.2.2 states</p> <p>FMT_LIM.1 Limited capabilities requires that the TSF is built to provide only the capabilities (perform action, gather information) necessary for its genuine purpose.</p> <p>This does not totally agree with the actual requirements in FMT_LIM.1.1 which state:</p> <p>FMT_LIM.1.1 The TSF shall limit its capabilities so that in conjunction with “Limited availability (FMT_LIM.2)” the following policy is enforced [assignment: <i>Limited capability and availability policy</i>].”</p> <p>Specifically, the actual requirements in FMT_LIM.1.1 only state that the TSF shall limit its capabilities to meet the Limited capability and availability policy, but gives no specifics of what that policy should contain, whereas the summary in Subclause 13.2.2 specifies specific components ‘perform action’ and ‘gather information’ of this policy.</p>	Revise the summary of FMT_LIM.1 in Subclause 13.2.2 to read: FMT_LIM.1 Limited capabilities requires that the TSF is built to provide only limited capabilities identified in a Limited capability and availability policy.	
CCUF 13		13.2.2	Components leveling and description (for Limited capabilities and availability (FMT_LIM))	Te	<p>The summary for FMT_LIM.2 in Subclause 13.2.2 states:</p> <p>FMT_LIM.2 Limited availability requires that the TSF restrict the use of functions (refer to Limited capabilities (FMT_LIM.1)).</p> <p>The actual requirements in FMT_LIM.2.1 are</p> <p>FMT_LIM.2.1 The TSF shall be designed in a manner that limits its availability so that in conjunction with “Limited capabilities (FMT_LIM.1)” the following policy is enforced [assignment: <i>Limited capability and availability policy</i>].</p> <p>Limiting availability, which is what FMT_LIM.2.1 requires, in the content of FMT_LIM, is limiting capabilities which can be more than just limiting functions. To match what is actually in FMT_LIM.2.1, the summary of FMT_LIM.2 in Subclause 13.2.2</p>	Revise the summary of FMT_LIM.2 in Subclause 13.2.2 to read: FMT_LIM.2 Limited availability requires that the TSF limit availability by restricting its capabilities (refer to Limited capabilities (FMT_LIM.1)).	

¹ **MB** = Member body / **NC** = National Committee (enter the ISO 3166 two-letter country code, e.g. CN for China; comments from the ISO/CS editing unit are identified by **)

² **Type of comment:** **ge** = general **te** = technical **ed** = editorial

**Template for comments and secretariat observations
on CC:2022 Release 1 Part 2**

Date: 2023-03-17

Document: **CC:2022 Release 1
Part 2**

Project:

MB/ NC ¹	Line number (e.g., 17)	Clause/ Subclause (e.g., 3.1)	Paragraph/ Figure/ Table/ (e.g. Table 1)	Type of comment ²	Comments	Proposed change	Observations of the secretariat
					should be written around limiting availability by limiting capabilities per the Limited capability and availability policy.		
CCUF 14		13.3.2	Components leveling and description (for Management of functions in the TSF (FMT_MOF))	Te	<p>The summary for FMT_MOF.1 in Subclause 13.3.2 states:</p> <p>FMT_MOF.1 Management of security functions behaviour allows the authorized users (roles) to manage the behaviour of functions in the TSF that use rules or have specified conditions that may be manageable.</p> <p>The actual requirements in FMT_MOF.1.1 are:</p> <p>FMT_MOF.1.1 The TSF shall restrict the ability to [selection: <i>determine the behaviour of, disable, enable, modify the behaviour of</i>] the functions [assignment: <i>list of functions</i>] to [assignment: <i>the authorized identified roles</i>].</p> <p>The issue here is the last part of the summary of FMT_MOF.1 which reads</p> <p>“...that use rules or have specified conditions that may be manageable.”</p> <p>There are no requirements in FMT_MOF.1.1 that state anything about rules or specific conditions; the only requirements in FMT_MOF.1.1 are that the TSF will restrict the ability to manage the behaviour of the listed functions to the identified roles. The summary of FMT_MOF.1 in Subclause 13.3.2 should more accurately reflect the actual requirements in FMT_MOF.1.1.</p>	<p>Revise the summary of FMT_MOF.1 in Subclause 13.3.2 to read:</p> <p>FMT_MOF.1 Management of security functions behaviour allows the authorized users (roles) to manage the behaviour of functions in the TSF.</p>	
CCUF 15		13.4.2	Components leveling and description (for Management of security attributes (FMT_MSA))	Te	<p>The summary for FMT_MSA.2 in Subclause 13.4.2 states:</p> <p>FMT_MSA.2 Secure security attributes ensures that values assigned to security attributes are valid with respect to the secure state.</p> <p>The actual requirements in FMT_MSA.2.1 are:</p> <p>FMT_MSA.2.1 The TSF shall ensure that only secure values are accepted for [assignment: <i>list of security attributes</i>].</p> <p>The requirements in FMT_MSA.2.1 says nothing about a “secure state”; they only say that secure values shall be accepted for the listed security attributes. That may implicitly imply that this is part of the secure state, but it is not explicitly stated as a requirement. The summary for FMT_MSA.2 in Subclause 13.4.2 should reflect what is actually stated in the FMT_MSA.2.1 and not what may or may not be implied by the requirements in this SFR.</p>	<p>Revise the summary of FMT_MSA.2 in Subclause 13.4.2 to read:</p> <p>FMT_MSA.2 Secure security attributes ensures that secure values are assigned to security attributes.</p>	
CCUF		13.4.2	Components	Te	The summary for FMT_MSA.3 in Subclause 13.4.2 states:	Revise the summary of FMT_MSA.3 in Subclause 13.4.2 to	

1 **MB** = Member body / **NC** = National Committee (enter the ISO 3166 two-letter country code, e.g. CN for China; comments from the ISO/CS editing unit are identified by **)

2 **Type of comment:** **ge** = general **te** = technical **ed** = editorial

**Template for comments and secretariat observations
on CC:2022 Release 1 Part 2**

Date: 2023-03-17	Document: CC:2022 Release 1 Part 2	Project:
------------------	---	----------

MB/ NC ¹	Line number (e.g., 17)	Clause/ Subclause (e.g., 3.1)	Paragraph/ Figure/ Table/ (e.g. Table 1)	Type of comment ²	Comments	Proposed change	Observations of the secretariat
16			leveling and description (for Management of security attributes (FMT_MSA))		<p>FMT_MSA.3 Static attribute ensures that the default values of security attributes are appropriately either permissive or restrictive in nature.</p> <p>The actual requirements in FMT_MSA.3.1 state:</p> <p>FMT_MSA.3.1 The TSF shall enforce the [assignment: access control SFP, information flow control SFP] to provide [selection, choose one of: restrictive, permissive, [assignment: other property]] default values for security attributes that are used to enforce the SFP.</p> <p>These requirements means that the default values could be other that either restrictive or permissive if the '[assignment: other property]' selection option is chosen. Thus, the summary description for FMT_MSA.3 in Subclause 13.4.2 does not completely reflect what is in FMT_MSA.3.1.</p>	<p>read:</p> <p>FMT_MSA.3 Static attribute ensures that the default values of security attributes are appropriately permissive, restrictive or some other property in nature.</p>	
CCUF 17		13.4.2	Components leveling and description (for Management of security attributes (FMT_MSA))	Te	<p>The summary for FMT_MSA.4 in Subclause 13.4.2 states</p> <p>FMT_MSA.4 Security attribute value inheritance allows the rules/policies to be specified that will dictate the value to be inherited by a security attribute.</p> <p>However, the actual requirements in FMT_MSA.4.1 state:</p> <p>FMT_MSA.4.1 The TSF shall use the following rules to set the value of security attributes: [assignment: rules for setting the values of security attributes].</p> <p>The requirements in FMT_MSA.4.1 only discuss rules to be specified that will dictate the value inherited by a security attribute; there is no mention of policies in FMT_MSA.4.1</p>	<p>Revise the summary for FMS_MSA.4 in Subclause 13.4.2 to read:</p> <p>"FMT_MSA.4 Security attribute value inheritance allows the rules to be specified that will dictate the value to be inherited by a security attribute.</p>	
CCUF 18		14.3.2	Components leveling and description (for Pseudonymity (FPR_PSE))	Te	<p>The summary for FPR_PSE.1 in Subclause 14.3.2 states:</p> <p>FPR_PSE.1 Pseudonymity requires that a set of users and/or subjects are unable to determine the identity of a user bound to a subject or operation, but that this user is still accountable for its actions.</p> <p>The actual requirements for FPR_PDE.1 are:</p> <p>FPR_PSE.1.1 The TSF shall ensure that [assignment: set of users and/or subjects] are unable to determine the real user name bound to [assignment: list of subjects and/or operations and/or objects].</p> <p>FPR_PSE.1.2 The TSF shall be able to provide [assignment: number of aliases] aliases of the real user name to [assignment: list of subjects].</p>	<p>Revise the summary for FPR_PSE.1 in Subclause 14.3.2 to read:</p> <p>FPR_PSE.1 Pseudonymity requires that a set of users and/or subjects are unable to determine the identity of a user bound to a subject or operation.</p>	

¹ **MB** = Member body / **NC** = National Committee (enter the ISO 3166 two-letter country code, e.g. CN for China; comments from the ISO/CS editing unit are identified by **)

² **Type of comment:** **ge** = general **te** = technical **ed** = editorial

**Template for comments and secretariat observations
on CC:2022 Release 1 Part 2**

Date: 2023-03-17	Document: CC:2022 Release 1 Part 2	Project:
------------------	---	----------

MB/ NC ¹	Line number (e.g., 17)	Clause/ Subclause (e.g., 3.1)	Paragraph/ Figure/ Table/ (e.g. Table 1)	Type of comment ²	Comments	Proposed change	Observations of the secretariat
					<p>FPR_PSE.1.3 The TSF shall [selection, choose one of: <i>determine an alias for a user, accept the alias from the user</i>] and verify that it conforms to the [assignment: <i>alias metric</i>].</p> <p>Note that there is no requirement in either FPR_PSE.1.1, FPR_PSE.1.2 or FPS_PSE.1.3 that even remotely addresses requiring a user to be accountable for its actions.</p>		
CCUF 19		15.2.1	Family Behaviour (for TOE emanation (FPT_EMS))	Te	<p>In the discussion of the family behaviour for FPT_EMS, the follow sentence is included:</p> <p>The family FPT_EMS (TOE Emanation) of the class FPT (Protection of the TSF) describes the IT SFRs of the TOE related to leakage of information based on emanation.</p> <p>It is not clear what is meant by 'IT SFRs' in the context of this family, since the requirements in SFR FPT_EMS.1 make no mention if 'IT SFRs', nor is the term 'IT SFRs' used elsewhere in the discussion of FPT_EMS.</p>	Either clarify what the term 'IT SFRs' means or eliminate the term 'IT SFRs' in the discussion of the Family Behaviour of FPT_EMS in Subclause 15.2.1.	
CCUF 20		15.2.2	Components leveling and description (for TOE emanation (FPT_EMS))	Te	<p>The summary for FPT_EMS.1 in Subclause 15.2.2 states:</p> <p>This family consists of one component, FPT_EMS.1 Emanation of TSF and User data, which defines requirements for the TOE to mitigate intelligible emanations.</p> <p>However, the actual requirements in SFR FPT_EMS.1.1 state:</p> <p>FPT_EMS.1.1 The TSF shall ensure that the TOE does not emit emissions over its attack surface in such amount that these emissions enable access to TSF data and user data as specified in Table 1.</p> <p>These requirements make no mention at all about 'intelligible emanations'.</p>	<p>Revise the summary of FPT_EMS.1 in Subclause 15.2.2 to read:</p> <p>This family consists of one component, FPT_EMS.1 Emanation of TSF and User data, which defines requirements for the TOE to mitigate emissions that could reveal User and TSF data.</p>	
CCUF 21		15.4.2	Components leveling and description (for TSF initialization (FPT_INI))	Te	<p>The summary for FPT_INI.1 in Subclause 15.4.2 states:</p> <p>This family consists of only one component, Component FPT_INI.1. This component requires the TOE to provide a TSF initialization function that brings the TSF into a secure operational state at power-on.</p> <p>The actual requirements in SFR FPT_INI.1.2 state:</p> <p>FPT_INI.1.2 The TOE initialization function shall ensure that certain properties hold on certain elements immediately before establishing the TSF in a secure initial state, as specified in Table 2:</p> <p>The issue here is that the summary for FPT_INI.1 speaks of bringing the TSF into a "secure operational state" while the actual requirements in FPT_INI.1.2 refer to "establishing the</p>	<p>Since there is no definition for what a secure initial state is, the easiest remedy is to revise the summary of FPT_INI.1.1 in Subclause 15.5.2 to agree with FPT_INI.1.2 and read:</p> <p>This family consists of only one component, Component FPT_INI.1. This component requires the TOE to provide a TSF initialization function that brings the TSF into a secure initial state.</p>	

¹ **MB** = Member body / **NC** = National Committee (enter the ISO 3166 two-letter country code, e.g. CN for China; comments from the ISO/CS editing unit are identified by **)

² **Type of comment:** **ge** = general **te** = technical **ed** = editorial

**Template for comments and secretariat observations
on CC:2022 Release 1 Part 2**

Date: 2023-03-17	Document: CC:2022 Release 1 Part 2	Project:
------------------	---	----------

MB/ NC ¹	Line number (e.g., 17)	Clause/ Subclause (e.g., 3.1)	Paragraph/ Figure/ Table/ (e.g. Table 1)	Type of comment ²	Comments	Proposed change	Observations of the secretariat
					TSF in a secure initial state". First of all, it is not clear what constitutes a "secure initial state" or what that means, and more importantly it is not clear that a 'secure initial state' is the same thing as a 'secure operational state at power-on'.		
CCUF 22		15.5.2	Components leveling and description (for Availability of exported TSF data (FPT_ITA))	Te	<p>The summary for FPT_ITA.1 in Subclause 15.5.2 states:</p> <p>This family consists of only one component, FPT_ITA.1 Inter-TSF availability within a defined availability metric. This component requires that the TSF ensure, to an identified degree of probability, the availability of TSF data provided to another trusted IT product.</p> <p>The actual requirements in FPT_ITA.1.1 are:</p> <p>FPT_ITA.1.1 The TSF shall ensure the availability of [assignment: <i>list of types of TSF data</i>] provided to another trusted IT product within [assignment: <i>a defined availability metric</i>] given the following conditions [assignment: <i>conditions to ensure availability</i>].</p> <p>There is no mention of any degree of probability in FPT_ITA.1.1, so it is misleading to indicate that the SFR is providing such a calculation. All the SFR requires is to provide availability of specified TSF data provided to another trusted IT product within some defined availability metric under certain specified conditions.</p> <p>The summary of this SFR in Subclause 15.5.2 should reflect this but currently does not.</p>	<p>Revise the summary of FPT_ITA.1 in Subclause 15.5.2 to read:</p> <p>This family consists of only one component, FPT_ITA.1 Inter-TSF availability within a defined availability metric. This component requires that the TSF ensure, to an identified metric, the availability of TSF data provided to another trusted IT product.</p>	
CCUF 23		15.6.2	Components leveling and description (for Confidentiality of exported TSF data (FPT_ITC))	Te	<p>The summary for FPT_ITC.1 in Subclause 15.6.2 states:</p> <p>This family consists of only one component, FPT_ITC.1 Inter-TSF confidentiality during transmission, which requires that the TSF ensure that data transmitted between the TSF and another trusted IT product is protected from disclosure while in transit.</p> <p>The actual requirements in FPT_ITC.1.1 are:</p> <p>FPT_ITC.1.1 The TSF shall protect all TSF data transmitted from the TSF to another trusted IT product from unauthorized disclosure during transmission.</p> <p>Note that in FPT_ITC.1.1 the requirement is to protect all TSF data transmitted from the TSF to another trusted IT product from unauthorized disclosure. The summary of FPT_ITC.1 in Subclause 15.6.2 doesn't indicate that all TSF data is to be protected and also doesn't indicate that the TSF data is to be protected from 'unauthorized' disclosure.</p>	<p>Revise the summary of FPT_ITA.1 in Subclause 15.6.2 to read:</p> <p>This family consists of only one component, FPT_ITC.1 Inter-TSF confidentiality during transmission, which requires that the TSF ensure that all TSF data transmitted between the TSF and another trusted IT product is protected from unauthorized disclosure while in transit.</p>	

1 **MB** = Member body / **NC** = National Committee (enter the ISO 3166 two-letter country code, e.g. CN for China; comments from the ISO/CS editing unit are identified by **)

2 **Type of comment:** **ge** = general **te** = technical **ed** = editorial

**Template for comments and secretariat observations
on CC:2022 Release 1 Part 2**

Date: 2023-03-17	Document: CC:2022 Release 1 Part 2	Project:
------------------	---	----------

MB/ NC ¹	Line number (e.g., 17)	Clause/ Subclause (e.g., 3.1)	Paragraph/ Figure/ Table/ (e.g. Table 1)	Type of comment ²	Comments	Proposed change	Observations of the secretariat
CCUF 24		15.7.2	Components leveling and description (for Integrity of exported TSF data (FPT_ITI))	Te	<p>The summary for FPT_ITI.2 in Subclause 15.7.2 states:</p> <p>FPT_ITI.2 Inter-TSF detection and correction of modification, provides the ability for another trusted IT product not only to detect modification, but to correct modified TSF data under the assumption that another trusted IT product is cognizant of the mechanism used.</p> <p>The actual requirements in FPT_ITI.2.3 are:</p> <p>FPT_ITI.2.3 The TSF shall provide the capability to correct [assignment: <i>type of modification</i>] of all TSF data transmitted between the TSF and another trusted IT product.</p> <p>The issue here is that FPT_ITI.2.3 requires that the TSF have the capability to correct certain modifications for all TSF data transmitted between the TSF and another trusted IT product. The summary of FPT_ITI.2 in Subclause 15.7.2 doesn't indicate that this applies to all TSF data.</p>	Revise the summary of FPT_ITI.2 in Subclause 15.7.2 to read: FPT_ITI.2 Inter-TSF detection and correction of modification, provides the ability for another trusted IT product not only to detect modification, but to correct all TSF data under the assumption that another trusted IT product is cognizant of the mechanism used.	
CCUF 25		15.9.2	Components leveling and description (for TSF physical protection (FPT_PHP))	Te	<p>The summary for FPT_PHP.3 in Subclause 15.9.2 states:</p> <p>FPT_PHP.3 Resistance to physical attack, provides for features that prevent or resist physical tampering with TSF devices and TSF elements.</p> <p>The actual requirements in FPT_PHP.3.1 are:</p> <p>FPT_PHP.3.1 The TSF shall resist [assignment: <i>physical tampering scenarios</i>] to the [assignment: <i>list of TSF devices/elements</i>] by responding automatically such that the SFRs are always enforced.</p> <p>The requirements in FPT_PHP.3.1 state that the TSF shall automatically resist a set of physical tampering scenarios to a defined list of TSF devices or elements so that the SFRs are always enforced. These requirements do not provide any "features" to prevent such physical tampering as the summary in Subclause 15.2 indicates, but rather just states what physical tampering scenarios are to be resisted and what TSF devices/elements this applies to.</p> <p>The summary in Subclause 15.9.2 should be modified to more accurately reflect the actual requirements in FPT_PHP.3.1.</p>	Revise the summary of FPT_PHP.3 in Subclause 15.9.2 to read: FPT_PHP.3 Resistance to physical attack, provides for the automatic resistance to physical tampering with TSF devices and TSF elements.	
CCUF 26		15.10.2	Components leveling and description (for Trusted recovery (FPT_RCV))	Te	<p>The summary for FPT_RCV.1 in Subclause 15.10.2 states:</p> <p>FPT_RCV.1 Manual recovery, allows a TOE to only provide mechanisms that involve human intervention to return to a secure state.</p> <p>The actual requirements in FPT_RCV.1.1 are:</p>	Revise the summary of FPT_RCV.1 in Subclause 15.10.2 to read: FPT_RCV.1 Manual recovery, allows a TOE to only provide mechanisms to return to a secure state upon detection of specific failures/service discontinuities.	

¹ **MB** = Member body / **NC** = National Committee (enter the ISO 3166 two-letter country code, e.g. CN for China; comments from the ISO/CS editing unit are identified by **)

² **Type of comment:** **ge** = general **te** = technical **ed** = editorial

**Template for comments and secretariat observations
on CC:2022 Release 1 Part 2**

Date: 2023-03-17	Document: CC:2022 Release 1 Part 2	Project:
------------------	---	----------

MB/ NC ¹	Line number (e.g., 17)	Clause/ Subclause (e.g., 3.1)	Paragraph/ Figure/ Table/ (e.g. Table 1)	Type of comment ²	Comments	Proposed change	Observations of the secretariat
					<p>FPT_RCV.1.1After [assignment: <i>list of failures/service discontinuities</i>] the TSF shall enter a maintenance mode where the ability to return to a secure state is provided.</p> <p>The actual requirements in FPT_RCV.1.1 do not say anything about providing mechanisms involving human intervention to return to a secure state; these requirements simply state that for a specified list of failures or service discontinuities the TSF shall enter a maintenance mode that will provide the ability to return to a secure state.</p> <p>The “human intervention” may be implied here, but it is not explicitly stated in the requirements in FPT_RCV.1.1.</p>		
CCUF 27		15.10.8	FPT_RCV.1 Manual recovery	Te	<p>The requirements in FPT_RCV.1.1 in Subclause 15.10.8 are:</p> <p>FPT_RCV.1.1 After [assignment: <i>list of failures/service discontinuities</i>] the TSF shall enter a maintenance mode where the ability to return to a secure state is provided.</p> <p>The issue here is the term “maintenance mode” in this SFR. Although within the vendor community it is understood what “maintenance mode” is, in the context of this requirement “maintenance mode” may have a different meaning because of the requirement to return the device to a secure state. Often the term “maintenance mode” is more of a diagnostic mode and often times will not result in a return of the TSF to a secure state.</p> <p>Given the nature of “maintenance mode” in practice, Part 2 needs to define what is meant by “maintenance mode” in the context of this and other SFRs where the term is used.</p>	Define the term “maintenance mode” in Part 2.	
CCUF 28		15.13.2	Components leveling and description (for Time stamps (FPT_STM))	Te	<p>The summary for FPT_STM.2 in Subclause 15.13.2 states:</p> <p>FPT_STM.2 Time source, requires the description of the time source used in timestamps.</p> <p>The actual requirements in FPT_STM.2.1 are:</p> <p>FPT_STM.2.1 The TSF shall allow the [assignment: <i>user authorized by security policy</i>] to [assignment: <i>set the time, configure another time source</i>].</p> <p>The actual requirements in FPT_STM.2.1 are to allow the authorized user to either set the time or configure another time source; they do not say anything about providing a description of the time source used in timestamps.</p>	<p>Revise the summary of FPT_STM.2 in Subclause 15.13.2 to read:</p> <p>FPT_STM.2 Time source, allows an authorized user to set either the time or another time source.</p>	
CCUF 29		15.14.2	Components leveling and description (for Inter-TSF TSF data	Te	<p>The summary for FPT_TDC.1 in Subclause 15.14.2 states:</p> <p>FPT_TDC.1 Inter-TSF basic TSF data consistency, requires that the TSF provide the capability to ensure consistency of attributes between TSFs.</p>	<p>Revise the summary of FPT_TDC.1 in Subclause 15.14.2 to read:</p> <p>FPT_TDC.1 Inter-TSF basic TSF data consistency, requires that the TSF provide the capability to ensure consistency of data</p>	

1 **MB** = Member body / **NC** = National Committee (enter the ISO 3166 two-letter country code, e.g. CN for China; comments from the ISO/CS editing unit are identified by **)

2 **Type of comment:** **ge** = general **te** = technical **ed** = editorial

**Template for comments and secretariat observations
on CC:2022 Release 1 Part 2**

Date: 2023-03-17	Document: CC:2022 Release 1 Part 2	Project:
------------------	---	----------

MB/ NC ¹	Line number (e.g., 17)	Clause/ Subclause (e.g., 3.1)	Paragraph/ Figure/ Table/ (e.g. Table 1)	Type of comment ²	Comments	Proposed change	Observations of the secretariat
			consistency (FPT_TDC))		<p>The actual requirements in FPT_TDC.1.1 are:</p> <p>FPT_TDC.1.1 The TSF shall provide the capability to consistently interpret [assignment: <i>list of TSF data types</i>] when shared between the TSF and another trusted IT product.</p> <p>The actual requirements in FPT_TDC.1 require that the TSF provide the capability to ensure consistency of TSF data types, not attributes, between TSFs. The summary for FPT_TDC.1 in Subclause 15.14.2 should properly reflect what is actually in FPT_TDC.1.1</p>	types between TSFs.	
CCUF 30		17.3.2	Components leveling and description (for Limitations on multiple concurrent sessions (FTA_MCS))	Te	<p>The summary for FTA_MCS.2 in Subclause 17.3.2 states:</p> <p>FTA_MCS.2 Per user attribute limitation on multiple concurrent sessions extends FTA_MCS.1 Basic limitation on multiple concurrent sessions by requiring the ability to specify limitations on the number of concurrent sessions based on the related security attributes.</p> <p>The actual requirements in FTA_MCS.2.1 are:</p> <p>FTA_MCS.2.1 The TSF shall restrict the maximum number of concurrent sessions that belong to the same user according to the rules [assignment: <i>rules for the number of maximum concurrent sessions</i>].</p> <p>The actual requirements in FTS_MCS.2.1 require that the limitations on the number of concurrent sessions is based on rules for the maximum number of sessions. These rules may or may not be based on security attributes. Therefore, the summary for FTS_MCS.2.1 in Subclause 17.3.2 does not completely reflect what is actually in FTS_MCS.2.1</p>	Revise the summary of FTS_MCS.2 in Subclause 17.3.2 to read: FTA_MCS.2 Per user attribute limitation on multiple concurrent sessions extends FTA_MCS.1 Basic limitation on multiple concurrent sessions by requiring the ability to specify limitations on the number of concurrent sessions based on a set of rules.	
CCUF 31		18.4.2	Components leveling and description (for Trusted path (FTP_TRP))	Te	<p>The summary for FTP_TRP.1 in Subclause 18.4.2 states:</p> <p>FTP_TRP.1 Trusted path, requires that a trusted path between the TSF and a user be provided for a set of events defined by a PP, PP-Module, functional package or ST author. The user and/or the TSF can have the ability to initiate the trusted path.</p> <p>The actual requirements in FTP_TRP.1.1 are:</p> <p>FTP_TRP.1.1 The TSF shall provide a communication path between itself and [selection: <i>remote, local</i>] 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: <i>modification, disclosure, [assignment: other types of integrity or confidentiality violation]</i>].</p> <p>The requirements in FTP_TRP.1.1 do not explicitly indicate that the communications path is provided for a set of events,</p>	Revise the summary of FTP_TRP.1 in Subclause 18.4.2 to read: FTP_TRP.1 Trusted path, requires that a trusted path between the TSF and a user be provided. The user and/or the TSF can have the ability to initiate the trusted path.	

¹ **MB** = Member body / **NC** = National Committee (enter the ISO 3166 two-letter country code, e.g. CN for China; comments from the ISO/CS editing unit are identified by **)

² **Type of comment:** **ge** = general **te** = technical **ed** = editorial

**Template for comments and secretariat observations
on CC:2022 Release 1 Part 2**

Date: 2023-03-17	Document: CC:2022 Release 1 Part 2	Project:
------------------	---	----------

MB/ NC ¹	Line number (e.g., 17)	Clause/ Subclause (e.g., 3.1)	Paragraph/ Figure/ Table/ (e.g. Table 1)	Type of comment ²	Comments	Proposed change	Observations of the secretariat
					<p>regardless of where that set of events may come from. In fact, FTP_TRP.1.1 does not mention any type of events at all; it just states several requirements on the communications path itself.</p> <p>Therefore, the summary for FTP_TRP,1 in Subclause 18.4.2 does not accurately reflect what is actually in FTP_TRP.1.1</p>		
CCUF 32		B.1	Table B.10 – Dependency table for Class FTA: TOE Access	Te	In Table B.10, it is indicated that FTA_SSL.2 is dependent on FIA_UAU.1. Per Subclause 17.4.11, FTA_SSL.2 is actually dependent on FIA_UID.1.	Correct Table B.10 to show that FTA_SSL.2 is dependent on FIA_UID.1 instead of FIA_UAU.1.	

Name: Alan Sukert
Affiliation: CCUF
Email address: ansukert49@outlook.com

¹ **MB** = Member body / **NC** = National Committee (enter the ISO 3166 two-letter country code, e.g. CN for China; comments from the ISO/CS editing unit are identified by **)

² **Type of comment:** **ge** = general **te** = technical **ed** = editorial