

CC 2.3								
Assurance class	Assurance Family	Assurance Components by Evaluation Assurance Level						
		EAL1	EAL2	EAL3	EAL4	EAL5	EAL6	EAL7
Configuration Management	ACM_AUT				1	1	2	2
	ACM_CAP	1	2	3	4	4	5	5
	ACM_SCP			1	2	3	3	3
Delivery and operation	ADO_DEL		1	1	2	2	2	3
	ADO_IGS	1	1	1	1	1	1	1
Development	ADV_FSP	1	1	1	2	3	3	4
	ADV_HLD		1	2	2	3	4	5
	ADV_IMP				1	2	3	3
	ADV_INT					1	2	3
	ADV_LLD				1	1	2	2
	ADV_RCR	1	1	1	1	2	2	3
	ADV_SPM				1	3	3	3
	AGD_ADM	1	1	1	1	1	1	1
Guidance documents	AGD_USR	1	1	1	1	1	2	2
	ALC_DVS			1	1	1	2	2
Life cycle support	ALC_FLR	<i>(ALC_FLR subactivities optional at all EALs)</i>						
	ALC_LCD				1	2	3	3
	ALC_TAT				1	2	3	3
Tests	ATE_COV		1	2	2	2	3	3
	ATE_DPT			1	1	2	2	3
	ATE_FUN		1	1	1	1	2	2
	ATE_IND	1	2	2	2	2	2	3
Vulnerability assessment	AVA_CCA					1	2	2
	AVA_MSU			1	2	2	3	3
	AVA_SOF		1	1	1	1	1	1
	AVA_VLA		1	1	2	3	4	4

CC 3.1								
Assurance class	Assurance Family	Assurance Components by Evaluation Assurance Level						
		EAL1	EAL2	EAL3	EAL4	EAL5	EAL6	EAL7
Development	ADV_ARC		1	1	1	1	1	1
	ADV_FSP	1	2	3	4	5	5	6
	ADV_IMP				1	1	2	2
	ADV_INT					2	3	3
	ADV_SPM						1	1
	ADV_TDS		1	2	3	4	5	6
Guidance documents	AGD_OPE	1	1	1	1	1	1	1
	AGD_PRE	1	1	1	1	1	1	1
Life-cycle support	ALC_CMC	1	2	3	4	4	5	5
	ALC_CMS	1	2	3	4	5	5	5
	ALC_DEL		1	1	1	1	1	1
	ALC_DVS			1	1	1	2	2
	ALC_FLR	<i>(ALC_FLR subactivities optional at all EALs)</i>						
	ALC_LCD			1	1	1	1	2
Security Target evaluation	ALC_TAT				1	2	3	3
	ASE_CCL	1	1	1	1	1	1	1
	ASE_ECD	1	1	1	1	1	1	1
	ASE_INT	1	1	1	1	1	1	1
	ASE_OBJ	1	2	2	2	2	2	2
	ASE_REQ	1	2	2	2	2	2	2
	ASE_SPD		1	1	1	1	1	1
	ASE_TSS	1	1	1	1	1	1	1
Tests	ATE_COV		1	2	2	2	3	3
	ATE_DPT			1	2	3	3	4
	ATE_FUN		1	1	1	1	2	2
	ATE_IND	1	2	2	2	2	2	3
Vulnerability assessment	AVA_VAN	1	2	2	3	4	5	5

√	CC 3.1 Evidence (CI's)	1	2	3	4	5
	Security Target	√	√	√	√	√
	CM Plan		√	√	√	√
	CM Authorization			√	√	√
	Automated CM system				√	√
	Acceptance Plan				√	√
	CI Lists			√	√	√
	Unique identification of CI		√	√	√	√
	CM Scope	√	√	√	√	√
	Labeled TOE	√	√	√	√	√
	Source Code			√	√	√
	Component Binaries		√	√	√	√
	Final Form TOE	√	√	√	√	√
	TOE components		√	√	√	√
	LC model description			√	√	√
	Dev tools description				√	√
	CM tools description				√	√
	Compiler description				√	√
	Linker description				√	√
	Debugger description				√	√
	Test tools description				√	√
	Other tools description				√	√
	Coding & other standards					√
	Delivery Process		√	√	√	√
	Delivery chain security		√	√	√	√
	Proof of authenticity (prod)		√	√	√	√
	Proof of integrity (prod)		√	√	√	√
	Build ID (prod)		√	√	√	√

√	CC 3.1 Evidence (CI's)	1	2	3	4	5
	Proof of authenticity (docs)		√	√	√	√
	Proof of integrity (docs)		√	√	√	√
	Build ID (docs)		√	√	√	√
	Dev. process security			√	√	√
	Physical access			√	√	√
	Procedural			√	√	√
	Personnel			√	√	√
	Flaw Remediation Procedures				√	√
	Security Flaw Reports				√	√
	Build Plan		√	√	√	√
	Preparative procedures		√	√	√	√
	Operational User Guide		√	√	√	√
	Architectural Design			√	√	√
	Functional Specification		√	√	√	√
	FSP > SFR map		√	√	√	√
	Error msgs from SFR TSFI			√	√	√
	Error msgs from all TSFI				√	√
	Error message rationale					√
	Imp rep for TSF				√	√
	Internals desc & justifi					√
	TOE design (HLD/TDS)		√	√	√	√
	TOE ds map > LL Decomp		√	√	√	√
	TOE ds map > IMP sample				√	√
	SFR Non interfering desc				√	√
	Subsystem interaction desc				√	√
	Subsystem description				√	√
	Module description				√	√

√	CC 3.1 Evidence (CI's)	1	2	3	4	5
	Subsystem > module map				√	√
	SFR module designation					√
	Test plan		√	√	√	√
	Test scenarios		√	√	√	√
	Test dependencies		√	√	√	√
	Expected test results		√	√	√	√
	Test procedures		√	√	√	√
	Test cases		√	√	√	√
	Test Mapping to FSP		√	√	√	√
	All TSFI in FSP tested				√	√
	Depth of testing analysis		√	√	√	√
	Test > Subsystem map				√	√
	SFR enforcing mod tested				√	√
	All TOE modules tested					√
	Penetration test plan		√	√	√	√
	Pen Testing results		√	√	√	√
	Test results		√	√	√	√
	Vul. search: design docs		√	√	√	√
	Vulnerability search: PD		√	√	√	√
	Independent VA		√	√	√	√
	Dev info base component					
	HL desc base component					
	Comp. correspondence					
	Interface map > base subs					
	Reliance information					
	Composed testing					
	Composed vul. analysis					

FAU: Security audit		FMT: Security management	
FAU_ARP	Security audit automatic response	FMT_MOF	Management of functions in TSF
FAU_GEN	Security audit data generation	FMT_MSA	Management of security attributes
FAU_SAA	Security audit analysis	FMT_MTD	Management of TSF data
FAU_SAR	Security audit review	FMT_REV	Revocation
FAU_SEL	Security audit event selection	FMT_SAE	Security attribute expiration
FAU_STG	Security audit event storage	FMT_SMF	Specification of Management Functions
		FMT_SMR	Security management roles
FCO: Communication		FPR: Privacy	
FCO_NRO	Non-repudiation of origin	FPR_ANO	Anonymity
FCO_NRR	Non-repudiation of receipt	FPR_PSE	Pseudonymity
		FPR_UNL	Unlinkability
		FPR_UNO	Unobservability
FCS: Cryptographic support		FPT: Protection of the TSF	
FCS_CKM	Cryptographic key management	FPT_TEE	Testing of external entities
FCS_COP	Cryptographic operation	FPT_FLS	Fail secure
		FPT_ITA	Availability of exported TSF data
		FPT_ITC	Confidentiality of exported TSF data
		FPT_ITI	Integrity of exported TSF data
		FPT_ITT	Internal TOE TSF data transfer
		FPT_PHP	TSF physical protection
		FPT_RCV	Trusted recovery
		FPT_RPL	Replay detection
		FPT_SSP	State synchrony protocol
		FPT_STM	Time stamps
		FPT_TDC	Inter-TSF TSF data consistency
		FPT_TRC	Internal TOE TSF data replication consistency
		FPT_TST	TSF self test
FDP: User data protection		FTA: TOE access	
FDP_ACC	Access control policy	FTA_LSA	Limitation on scope of selectable attributes
FDP_ACF	Access control functions	FTA_MCS	Limitation on multiple concurrent sessions
FDP_DAU	Data authentication	FTA_SSL	Session locking and termination
FDP_ETC	Export from the TOE	FTA_TAB	TOE access banners
FDP_IFC	Information flow control policy	FTA_TAH	TOE access history
FDP_IFT	Information flow control functions	FTA_TSE	TOE session establishment
FDP_ITC	Import from outside of the TOE		
FDP_ITT	Internal TOE transfer	FTP: Trusted path/channels	
FDP_RIP	Residual information protection	FTP_ITC	Inter-TSF trusted channel
FDP_ROL	Rollback	FTP_TRP	Trusted path
FDP_SDI	Stored data integrity		
FDP_UCT	Inter-TSF user data confidentiality transfer protection		
FDP_UIT	Inter-TSF user data integrity transfer protection		
FDP_ACC	Access control policy		
FDP_ACF	Access control functions		
FDP_DAU	Data authentication		
FDP_ETC	Export from the TOE		
FDP_IFC	Information flow control policy		
FDP_IFT	Information flow control functions		
FDP_ITC	Import from outside of the TOE		
FDP_ITT	Internal TOE transfer		
FDP_RIP	Residual information protection		
FDP_ROL	Rollback		
FDP_SDI	Stored data integrity		
FDP_UCT	Inter-TSF user data confidentiality transfer protection		
FDP_UIT	Inter-TSF user data integrity transfer protection		
FIA: Identification and authentication			
FIA_AFL	Authentication failures		
FIA_ATD	User attribute definition		
FIA_SOS	Specification of secrets		
FIA_UAU	User authentication		
FIA_UID	User identification		
FIA_USB	User-subject binding		