NIST Checklist

ID	TECHNICAL PROCESSES	Device	PCH
		Traceability ID	Traceability ID
BA	**Business or Mission Analysis**		
BA-1	**PREPARE FOR THE SECURITY ASPECTS OF BUSINESS OR MISSION ANALYSIS**		
BA-1.1	Identify stakeholders who will contribute to the identification and assessment of any mission, business, or operational problems or opportunities.	O3	O3
BA-1.2	Review organizational problems and opportunities with respect to desired security objectives.	All	All
BA-1.3	Define the security aspects of the business or mission analysis strategy.	O7,O4	O7,O4
BA-1.4	Identify, plan for, and obtain access to enabling systems or services to support the security aspects of the business or mission analysis process.	O13	All, O13
BA-2	**DEFINE THE SECURITY ASPECTS OF THE PROBLEM OR OPPORTUNITY SPACE**		
BA-2.1	Analyze the problems or opportunities in the context of the security objectives and measures of success to be achieved.	Spec	Spec
BA-2.2	Define the security aspects and considerations of the mission, business, or operational problem or opportunity.	Spec	Spec
BA-3	**CHARACTERIZE THE SECURITY ASPECTS OF THE SOLUTION SPACE**		
BA-3.1	Define the security aspects of the preliminary operational concepts and other concepts in life cycle stages.	O5	O5
BA-3.2	Identify alternative solution classes that can achieve the security objectives within limitations, constraints, and other considerations.	NA	NA
BA-4	**EVALUATE AND SELECT SOLUTION CLASSES**		
BA-4.1	Assess each alternative solution class taking into account the security objectives, limitations, constraints, and other relevant security considerations.	NA	NA
BA-4.2	Select the preferred alternative solution class (or classes) based on the identified security objectives, trade space factors, and other criteria defined by the organization.	NA	NA
BA-5	**MANAGE THE SECURITY ASPECTS OF BUSINESS OR MISSION ANALYSIS**		
BA-5.1	Maintain traceability of the security aspects of business or mission analysis.	All	All, O13
BA-5.2	Provide security-relevant information items required for business or mission analysis to baselines.	All	All, O13
SN	**Stakeholder Needs and Requirements Definition**		
SN-1	**PREPARE FOR STAKEHOLDER PROTECTION NEEDS AND SECURITY REQUIREMENTS DEFINITION**		

NIST Checklist

SN-1.1	Identify the stakeholders who have a security interest in the system throughout its life cycle.	O3	O3
SN-1.2	Define the stakeholder protection needs and security requirements definition strategy.	O6	O6
SN-1.3	Identify, plan for, and obtain access to enabling systems or services to support the security aspects of the stakeholder needs and requirements definition process.		
SN-2	**DEFINE STAKEHOLDER PROTECTION NEEDS**		
SN-2.1	Define the security context of use across all preliminary life cycle concepts.	O5	O5
SN-2.2	Identify stakeholder assets and asset classes.	O6	O6
SN-2.3	Prioritize assets based on the adverse consequence of asset loss.	O7	O7
SN-2.4	Determine asset susceptibility to adversity and uncertainty.	O7	O7
SN-2.5	Identify stakeholder protection needs.	O7	O7
SN-2.6	Prioritize and down-select the stakeholder protection needs.	O7	O7
SN-2.7	Define the stakeholder protection needs and rationale.	O7	O7
SN-3	**DEVELOP THE SECURITY ASPECTS OF OPERATIONAL AND OTHER LIFE CYCLE CONCEPTS**		
SN-3.1	Define a representative set of scenarios to identify all required protection capabilities and security measures that correspond to anticipated operational and other life cycle concepts.	O7	O7
SN-3.2	Identify the security-relevant interaction between users and the system.	O7	O7
SN-4	**TRANSFORM STAKEHOLDER PROTECTION NEEDS INTO SECURITY REQUIREMENTS**		
SN-4.1	Identify the security-oriented constraints on a system solution.	Spec	Spec
SN-4.2	Identify the stakeholder security requirements and security functions.	Spec	Spec
SN-4.3	Define stakeholder security requirements, consistent with life cycle concepts, scenarios, interactions, constraints, and critical quality characteristics.	O6	O6
SN-4.4	Apply security metadata tagging to identify stakeholder security requirements and security-driven constraints.	O6	O6
SN-5	**ANALYZE STAKEHOLDER SECURITY REQUIREMENTS**		
SN-5.1	Analyze the complete set of stakeholder security requirements.	O7	O7
SN-5.2	Define critical security-relevant performance and assurance measures that enable the assessment of technical achievement.	O7	O7
SN-5.3	Validate that stakeholder protection needs and expectations have been adequately captured and expressed by the analyzed security requirements.	O7	O7
SN-5.4	Resolve stakeholder security requirements issues.	O7	O7

SN-6	**MANAGE STAKEHOLDER PROTECTION NEEDS AND SECURITY REQUIREMENTS DEFINITION**		
SN-6.1	Obtain explicit agreement on the stakeholder security requirements.	Spec	Spec
SN-6.2	Record asset protection data.	O16, DC10	O16,PC13
SN-6.3	Maintain traceability between stakeholder protection needs and stakeholder security requirements.	All	All, O13
SN-6.4	Provide security-relevant information items required for stakeholder needs and requirements definition to baselines.	O4	O4
SR	**System Requirements Definition**		
SR-1	**PREPARE FOR SYSTEM SECURITY REQUIREMENTS DEFINITION**		
SR-1.1	Define the security aspects of the functional boundary of the system in terms of the security behavior and security properties to be provided.	O6	O6
SR-1.2	Define the security domains of the system and their correlation to the functional boundaries of the system.	O6	O6
SR-1.3	Define the security aspects of the system requirements definition strategy.	O6	O6
SR-1.4	Identify, plan for, and obtain access to enabling systems or services to support the security aspects of the system requirements definition process.		
SR-2	**DEFINE SYSTEM SECURITY REQUIREMENTS**		
SR-2.1	Define each security function that the system is required to perform.	O6	O6
SR-2.2	Define system security requirements, security constraints on system requirements, and rationale.	O6	O6
SR-2.3	Incorporate system security requirements and associated constraints into system requirements and define rationale.	O6,O7	O6,O7
SR-2.4	Apply security metadata tagging to identify system security requirements and security-driven constraints.	O6,O7	O6,O7
SR-3	**ANALYZE SYSTEM SECURITY IN SYSTEM REQUIREMENTS**		
SR-3.1	Analyze the complete set of system requirements in consideration of security concerns.	O7	O7
SR-3.2	Define security-driven performance and assurance measures that enable the assessment of technical achievement.	O7	O7
SR-3.3	Provide the analyzed system security requirements and security-driven constraints to applicable stakeholders for review.	O7	O7
SR-3.4	Resolve system security requirements and security-driven constraints issues.	O7	O7
SR-4	**MANAGE SYSTEM SECURITY REQUIREMENTS**		

SR-4.1	Obtain explicit agreement on the system security requirements and security-driven constraints.	O7	O7
SR-4.2	Maintain traceability of system security requirements and security-driven constraints.	All	All, O13
SR-4.3	Provide security-relevant information items required for systems requirements definition to baselines.	All	All, O13
AR	**Architecture Definition**		
AR-1	**PREPARE FOR ARCHITECTURE DEFINITION FROM THE SECURITY VIEWPOINT**		
AR-1.1	Identify the key drivers that impact the security aspects of the system architecture.	O8	O8
AR-1.2	Identify stakeholder security concerns.	All	All, O13
AR-1.3	Define the security aspects of the architecture definition roadmap, approach, and strategy.	O8	O8
AR-1.4	Define evaluation criteria based on stakeholder security concerns and security-relevant requirements.	O14	O14
AR-1.5	Identify, plan for, and obtain access to enabling systems or services to support the security aspects of the architecture definition process.		
AR-2	**DEVELOP SECURITY VIEWPOINTS OF THE ARCHITECTURE**		
AR-2.1	Define the concept of secure function for the system at the architecture level.	O7	O7
AR-2.2	Select, adapt, or develop the security viewpoints and model kinds based on stakeholder security concerns.	All	All, O13
AR-2.3	Identify the security architecture frameworks to be used in developing the security models and security views of the system architecture.	All	All, O13
AR-2.4	Record the rationale for the selection of architecture frameworks that address security concerns, security viewpoints, and security model types.	O8	O8, O9
AR-2.5	Select or develop supporting security modeling techniques and tools.	O7	O7
AR-3	**DEVELOP SECURITY MODELS AND SECURITY VIEWS OF CANDIDATE ARCHITECTURES**		
AR-3.1	Define the security context and boundaries of the system in terms of interfaces, interconnections, and interactions with external entities.	NA	NA
AR-3.2	Identify architectural entities and relationships between entities that address key stakeholder security concerns and system security requirements.	NA	NA
AR-3.3	Allocate security concepts, properties, characteristics, behavior, functions, or constraints to architectural entities.	NA	NA
AR-3.4	Select, adapt, or develop security models of the candidate architectures.	NA	NA

NIST Checklist

AR-3.5	Compose views in accordance with security viewpoints to express how the architecture addresses stakeholder security concerns and meets stakeholder and system security requirements.	NA	NA
AR-3.6	Harmonize the security models and security views with each other and with the concept of secure function.	NA	NA
AR-4	**RELATE SECURITY VIEWS OF THE ARCHITECTURE TO DESIGN**		
AR-4.1	Identify the security-relevant system elements that relate to architectural entities and the nature of these relationships.	Spec	Spec
AR-4.3	Allocate system security requirements to architectural entities and system elements.	Spec	Spec
AR-4.2	Define the security interfaces, interconnections, and interactions between the system elements and with external entities.	Spec	Spec
AR-4.4	Map security-relevant system elements and architectural entities to security design characteristics.	Spec	Spec
AR-4.5	Define the security design principles for the system design and evolution that reflect the concept of secure function.	Spec	Spec
AR-5	**SELECT CANDIDATE ARCHITECTURE**		
AR-5.1	Assess each candidate architecture against the security requirements and security-related constraints.	NA	NA
AR-5.2	Assess each candidate architecture against stakeholder security concerns using evaluation criteria.	NA	NA
AR-5.3	Select the preferred architecture(s) and capture key security decisions and rationale for those decisions.	NA	NA
AR-5.4	Establish the security aspects of the architecture baseline of the selected architecture.	NA	NA
AR-6	**MANAGE THE SECURITY VIEW OF THE SELECTED ARCHITECTURE**		
AR-6.1	Formalize the security aspects of the architecture governance approach and specify security governance-related roles and responsibilities, accountabilities, and authorities.	O2, O3	O2, O3
AR-6.2	Obtain explicit acceptance of the security aspects of the architecture by stakeholders.	O9	O8, O9
AR-6.3	Maintain concordance and completeness of the security architectural entities and their security-related architectural characteristics.	Spec	Spec
AR-6.4	Organize, assess, and control the evolution of the security models and security views of the architecture.	O7	O7
AR-6.5	Maintain the security aspects of the architecture definition and evaluation strategy.	O7	O7, O8

AR-6.6	Maintain traceability of the security aspects of the architecture.	O8	O8
AR-6.7	Provide security-relevant information items required for architecture definition to baselines.	Spec	Spec
DE	**Design Definition**		
DE-1	**PREPARE FOR SECURITY DESIGN DEFINITION**		
DE-1.1	Apply the concept of secure function for the system at the design level.	O9	O8, O9
DE-1.2	Determine the security technologies required for each system element composing the system.	O9	O8, O9, O10
DE-1.3	Determine the types of security design characteristics.	O9	O8, O9
DE-1.4	Define the principles for secure evolution of the system design.	O9	O8, O9
DE-1.5	Define the security aspects of the design definition strategy.	O7,O9,O10	O7,O9
DE-1.6	Identify, plan for, and obtain access to enabling systems or services to support the security aspects of the design definition process.		
DE-2	**ESTABLISH SECURITY DESIGN CHARACTERISTICS AND ENABLERS FOR EACH SYSTEM ELEMENT**		
DE-2.1	Allocate system security requirements to system elements.	O6, O9	O6, O9
DE-2.2	Transform security architectural characteristics into security design characteristics.	O6, O9	O6, O8, O9
DE-2.3	Define the necessary security design enablers.	O6, O9	O6, O9
DE-2.4	Examine security design alternatives.	O6, O9	O6, O9
DE-2.5	Refine or define the security interfaces between the system elements and with external entities.	O6, O9	O6, O9
DE-2.6	Develop the security design artifacts.	O9	O9
DE-3	**ASSESS THE ALTERNATIVES FOR OBTAINING SECURITY-RELEVANT SYSTEM ELEMENTS**		
DE-3.1	Identify security-relevant nondevelopmental items (NDI) that may be considered for use.	NA	NA
DE-3.2	Assess each candidate NDI and new design alternative against the criteria developed from expected security design characteristics or system element security requirements to determine suitability for the intended application.	NA	NA
DE-3.3	Determine the preferred alternative among candidate NDI solutions and new design alternatives for a system element.	NA	NA
DE-4	**MANAGE THE SECURITY DESIGN**		
DE-4.1	Map the security design characteristics to the system elements.	O6, O9	O6, O9
DE-4.3	Maintain traceability of the security aspects of the system design.	O6, O9	O6, O9
DE-4.2	Capture the security design and rationale.	O7, O9	O7, O9

DE-4.4	Provide security-relevant information items required for the system design definition to baselines.	Spec	Spec
SA	**System Analysis**		
SA-1	**PREPARE FOR THE SECURITY ASPECTS OF SYSTEM ANALYSIS**		
SA-1.1	Identify the security aspects of the problem or question that requires system analysis.	Spec	Spec
SA-1.2	Identify the stakeholders of the security aspects of system analysis.	Spec	Spec
SA-1.3	Define the objectives, scope, level of fidelity, and level of assurance of the security aspects of system analysis.	Spec	Spec
SA-1.4	Select the methods associated with the security aspects of system analysis.	Spec	Spec
SA-1.5	Define the security aspects of the system analysis strategy.	Spec	Spec
SA-1.6	Identify, plan for, and obtain access to enabling systems or services to support the security aspects of the system analysis process.	Spec	Spec
SA-1.7	Collect the data and inputs needed for the security aspects of system analysis.	Spec	Spec
SA-2	**PERFORM THE SECURITY ASPECTS OF SYSTEM ANALYSIS**		
SA-2.1	Identify and validate the assumptions associated with the security aspects of system analysis.	Spec	Spec
SA-2.2	Apply the selected security analysis methods to perform the security aspects of required system analysis.	Spec	Spec
SA-2.3	Review the security aspects of the system analysis results for quality and validity.	Spec	Spec
SA-2.4	Establish conclusions, recommendations, and rational based on the results of the security aspects of system analysis.	Spec	Spec
SA-2.5	Record the results of the security aspects of system analysis.	Spec	Spec
SA-3	**MANAGE THE SECURITY ASPECTS OF SYSTEM ANALYSIS**		
SA-3.1	Maintain traceability of the security aspects of the system analysis results.	All	All, O13
SA-3.2	Provide security-relevant system analysis information items that have been selected for baselines.	All	All, O13
IP	**Implementation**		
IP-1	**PREPARE FOR THE SECURITY ASPECTS OF IMPLEMENTATION**		
IP-1.1	Develop the security aspects of the implementation strategy.	All	All, O13
IP-1.2	Identify constraints from the security aspects of the implementation strategy and technology on the system requirements, architecture, design, or implementation techniques.	All	All, O13

IP-1.3	Identify, plan for, and obtain access to enabling systems or services to support the security aspects of implementation.		
IP-2	**PERFORM THE SECURITY ASPECTS OF IMPLEMENTATION**		
IP-2.1	Realize or adapt system elements in accordance with the security aspects of the implementation strategy, defined implementation procedures, and security-driven constraints.	All	All
IP-2.2	Securely package and store system elements.	O14. O16	O14. O16
IP-2.3	Record evidence that system elements meet the system security requirements.	O14, O15	O14, O15
IP-3	**MANAGE RESULTS OF THE SECURITY ASPECTS OF IMPLEMENTATION**		
IP-3.1	Record the security aspects of implementation results and any security-related anomalies encountered.	O14, O15	O14, O15
IP-3.3	Provide security-relevant information items required for implementation to baselines.	Spec	Spec
IP-3.2	Maintain traceability of the security aspects of implemented system elements.	O15	O15
IN	**Integration**		
IN-1	**PREPARE FOR THE SECURITY ASPECTS OF INTEGRATION**		
IN-1.1	Identify and define checkpoints for the trustworthy secure operation of the assembled interfaces and selected system functions.	O9 & O10	O9 & O10
IN-1.2	Develop the security aspects of the integration strategy.	Entire DC subsection'	Spec
IN-1.3	Identify, plan for, and obtain access to enabling systems or services to support the security aspects of integration.		
IN-1.4	Identify the constraints resulting from the security aspects of integration to be incorporated into the system requirements, architecture, or design.	O7	O7
IN-2	**PERFORM THE SECURITY ASPECTS OF INTEGRATION**		
IN-2.1	Obtain implemented system elements in accordance with security criteria and requirements established in agreements and schedules.	NA	Spec
IN-2.2	Assemble the implemented system elements to achieve secure configurations.	Entire DC subsection'	Entire PC subsection
IN-2.3	Perform checks of the security characteristics of interfaces, functional behavior, and behavior across interconnections.	O14,O15	O14,O15
IN-3	**MANAGE RESULTS OF THE SECURITY ASPECTS OF INTEGRATION**		
IN-3.1	Record the security aspects of integration results and any security anomalies encountered.	O14,O15	O14,O15
IN-3.2	Maintain traceability of the security aspects of integrated system elements.	O14,O15	O14,O15
IN-3.3	Provide security-relevant information items required for integration to baselines.	Spec	Spec

NIST Checklist

VE	**Verification**		
VE-1	**PREPARE FOR THE SECURITY ASPECTS OF VERIFICATION**		
VE-1.1	Identify the security aspects within the verification scope and corresponding security-focused	O14	O14
VE-1.2	Identify the constraints that can potentially limit the feasibility of the security-focused verification actions.	O14,O15	O14,O15
VE-1.3	Select the appropriate methods or techniques for the security aspects of verification and the associated security criteria for each security-focused verification action.	O14,O15	O14,O15
VE-1.4	Define the security aspects of the verification strategy.	O14	O14
VE-1.5	Identify the system constraints resulting from the security aspects of the verification strategy to be incorporated into the system requirements, architecture, or design.	O14	O14
VE-1.6	Identify, plan for, and obtain access to enabling systems or services to support the security aspects of verification.		
VE-2	**PERFORM SECURITY-FOCUSED VERIFICATION**		
VE-2.1	Define the security aspects of the verification procedures, each supporting one or a set of security-focused verification actions.	O14,O15	O14,O15
VE-2.2	Perform security verification procedures.	O14,O15	O14,O15
VE-3	**MANAGE RESULTS OF SECURITY-FOCUSED VERIFICATION**		
VE-2.3	Analyze security-focused verification results against any established expectations and success criteria.	O14,O15	O14,O15
VE-3.1	Record the security aspects of verification results and any security anomalies encountered.	O14,O15	O14,O15
VE-3.2	Record the security characteristics of operational incidents and problems and track their resolution.	O14,O15	O14,O15
VE-3.3	Obtain stakeholder agreement that the system or system element meets the specified system security requirements and characteristics.	O14,O15	O14,O15
VE-3.4	Maintain traceability of the security aspects of verified system elements.	O14,O15,O7	O14,O15,O7
VE-3.5	Provide security-relevant information items required for verification to baselines.	Spec	Spec
TR	**Transition**		
TR-1	**PREPARE FOR THE SECURITY ASPECTS OF TRANSITION**		
TR-1.1	Develop the security aspects of the transition strategy.	O18	O18
TR-1.2	Identify the facility or site changes needed for security purposes.	O17 & O18	O17 & O18
TR-1.3	Identify the constraints resulting from the security aspects of transition to be incorporated into the system requirements, architecture, and design.	O17, O18, O19	O17, O18, O19, PC26

TR-1.4	Identify and arrange the training necessary for secure system utilization, sustainment, and support.	O17, O18, O19	O17, O18, O19, PC26
TR-1.5	Identify, plan for, and obtain access to enabling systems or services to support the security aspects of transition.		
TR-2	**PERFORM THE SECURITY ASPECTS OF TRANSITION**		
TR-2.1	Prepare the facility or site in accordance with the secure installation requirements.	O17, O18, O19	O17, O18, O19, PC26
TR-2.2	Securely deliver the system for installation.	O17, O18, O19	O17, O18, O19, PC26
TR-2.3	Install the system at its specified location and establish secure interconnections to its environment.	O17, O18, O19	O17, O18, O19, PC26
TR-2.4	Demonstrate proper achievement of the security aspects of system installation.	O17, O18, O19	O17, O18, O19, PC26, PC24
TR-2.5	Provide security training for stakeholders that interact with the system.		
TR-2.6	Perform activation and checkout of the security aspects of the system.	O17, O18, O19	O17, O18, O19, PC26, PC24
TR-2.7	Demonstrate that the installed system is capable of delivering the required protection capability.	O17, O18, O19	O17, O18, O19, PC26, PC24
TR-2.8	Demonstrate that the security functions provided by the system are sustainable by the enabling systems.	O17, O18, O19	O17, O18, O19, PC26, PC24
TR-2.9	Review the security aspects of the system for operational readiness.	O17, O18, O19	O17, O18, O19, PC26, PC24
TR-2.10	Commission the system for secure operation.	O17, O18, O19	O17, O18, O19, PC26, PC24
TR-3	**MANAGE RESULTS OF THE SECURITY APECTS OF TRANSITION**		
TR-3.1	Record the security aspects of transition results and any security anomalies encountered.	O18	O18
TR-3.2	Record the security aspects of operational incidents and problems and track their resolution.	O21	O21
TR-3.4	Provide security-relevant information items required for transition to baselines.	Spec	Spec
TR-3.3	Maintain traceability of the security aspects of transitioned system elements.	All	All
VA	**Validation**		
VA-1	**PREPARE FOR THE SECURITY ASPECTS OF VALIDATION**		
VA-1.1	Identify the security aspects of the validation scope and corresponding security-focused validation actions.	O17, PC22, PC23, All of Demonstration section	O17, PC22, PC23, All of Demonstration section
VA-1.2	Identify the constraints that can potentially limit the feasibility of the security-focused validation actions.	Spec	Spec

VA-1.3	Select the appropriate methods or techniques for the security aspects of validation and the associated security criteria for each security-focused validation action.	O17, PC22, PC23, All of Demonstration section	O17, PC22, PC23, All of Demonstration section
VA-1.4	Develop the security aspects of the validation strategy.	O17, PC22, PC23, All of Demonstration section	O17, PC22, PC23, All of Demonstration section
VA-1.5	Identify system constraints resulting from the security aspects of validation to be incorporated into the stakeholder security requirements.	Spec	Spec
VA-1.6	Identify, plan for, and obtain access to enabling systems or services to support the security aspects of validation.		
VA-2	**PERFORM SECURITY-FOCUSED VALIDATION**		
VA-2.1	Define the security aspects of the validation procedures, each supporting one or a set of security- focused validation actions.	MS12, O14, O15	O14, O15
VA-2.2	Perform security validation procedures in the defined environment.	O14, O7	O14, O7
VA-2.3	Review security-focused validation results to confirm that the protection services of the system that are required by stakeholders are available.	O14, O7	O14, O7
VA-3	**MANAGE RESULTS OF SECURITY-FOCUSED VALIDATION**		
VA-3.1	Record the security aspects of validation results and any security anomalies encountered.	O14, O7	O14, O7
VA-3.2	Record the security characteristics of operational incidents and problems and track their resolution.	O21	O21
VA-3.3	Obtain stakeholder agreement that the system or system element meets the stakeholder protection needs.	O14, O7	O14, O7
VA-3.4	Maintain traceability of the security aspects of validated system elements.	O14, O7	O14, O7
VA-3.5	Provide security-relevant information items required for validation to baselines.	Spec	Spec
OP	**Operation**		
OP-1	**PREPARE FOR SECURE OPERATION**		
OP-1.1	Develop the security aspects of the operation strategy.	O19, O22, MS21	O19, O22, MS21
OP-1.2	Identify the constraints resulting from the security aspects of operation to be incorporated into the system requirements, architecture, and design.	All of the tamper section	All of the tamper section
OP-1.3	Identify, plan for, and obtain access to enabling systems or services to support the security aspects of operation.	All of MS sub section & All of DC	All of PC sub section
OP-1.4	Identify or define security training and qualification requirements; train, and assign personnel needed for system operation.		
OP-2	**PERFORM SECURE OPERATION**		

OP-2.1	Securely use the system in its intended operational environment.	MS11, MS12, MS13	MS11, MS12, MS13
OP-2.2	Apply materials and other resources, as required, to operate the system in a secure manner and sustain its security services.	All of MS sub section & All of DC	All of PC sub section
OP-2.3	Monitor the security aspects of system operation.	MS11, MS12, MS13	PC2, PC3, PC5, PC6, PC7, PC8, PC9
OP-2.4	Identify and record when system security performance is not within acceptable parameters.	O21	O21, PC25
OP-2.5	Perform system security contingency operations, if necessary.		
OP-3	**MANAGE RESULTS OF SECURE OPERATION**		
OP-3.1	Record results of secure operation and any security anomalies encountered.	O21	O21
OP-3.2	Record the security aspects of operational incidents and problems and track their resolution.	O21	O21
OP-3.3	Maintain traceability of the security aspects of the operations elements.	MS13	PC24
OP-3.4	Provide security-relevant information items required for operation to baselines.	Spec	Spec
OP-4	**SUPPORT SECURITY NEEDS OF CUSTOMERS**		
OP-4.1	Provide security assistance and consultation to customers as requested.		
OP-4.2	Record and monitor requests and subsequent actions for security support.		
OP-4.3	Determine the degree to which the delivered system security services satisfy the needs of the customers.		
MA	**Maintenance**		
MA-1	**PREPARE FOR THE SECURITY ASPECTS OF MAINTENANCE**		
MA-1.1	Define the security aspects of the maintenance strategy.	MS10, MS12, SQ14, DM9	Entire PC subsection
MA-1.2	Identify the system constraints resulting from the security aspects of maintenance and logistics to be incorporated into the system requirements, architecture, and design.	MS10, MS12, SQ14, DM9	Entire PC subsection
MA-1.3	Identify trades such that the security aspects of system maintenance and logistics result in a solution that is trustworthy, secure, affordable, operable, supportable, and sustainable.		
MA-1.4	Identify, plan for, and obtain enabling systems or services to support the security aspects of system maintenance and logistics.		
MA-2	**PERFORM THE SECURITY ASPECTS OF MAINTENANCE**		
MA-2.1	Review incident and problem reports to identify security relevance and associated maintenance needs.	O21	O21

NIST Checklist

MA-2.2	Record the security aspects of maintenance incidents and problems and track their resolution.	O21	O21
MA-2.3	Implement the procedures for the correction of random faults or scheduled replacement of system elements to ensure the ability to deliver system security functions and services.	O21	O21
MA-2.4	Implement action to restore the system to secure operational status when a random fault causes a system failure.	O21	O21
MA-2.5	Perform preventive maintenance by replacing or servicing system elements prior to failure with security-related impact.	O21, MS13, O17	O17, O21, PC24
MA-2.6	Perform failure identification actions when security noncompliance has occurred in the system.	O21, MS13, O17	O17, O21, PC24
MA-2.7	Identify when security-relevant adaptive or perfective maintenance is required.	MS12, DC5, DM2	DM2
MA-3	**PERFORM THE SECURITY ASPECTS OF LOGISTICS SUPPORT**		
MA-3.1	Perform the security aspects of acquisition logistics.		
MA-3.2	Perform the security aspects of operational logistics.		
MA-3.3	Implement any secure packaging, handling, storage, and transportation needed during the life cycle of the system.		
MA-3.4	Confirm that security aspects incorporated into logistics actions satisfy the required protection levels so that system elements are securely stored and able to meet repair rates and planned schedules.		
MA-3.5	Confirm that the security aspects of logistics actions include security supportability requirements that are planned, resourced, and implemented.		
MA-4	**MANAGE RESULTS OF THE SECURITY ASPECTS OF MAINTENANCE AND LOGISTICS**		
MA-4.1	Record the security aspects of maintenance and logistics results and any security anomalies encountered.	MS12, O21, O22	O21, O16, O22
MA-4.2	Record operational security incidents and security problems and track their resolution.	MS12	O16
MA-4.3	Identify and record the security-related trends of incidents, problems, and maintenance and logistics actions.	MS12, O21, O22	O21, O16, O22
MA-4.4	Maintain traceability of system elements and the security aspects of maintenance actions and logistics actions performed.		
MA-4.5	Provide security-relevant configuration items from system maintenance to baselines.	Spec	Spec
MA-4.6	Monitor customer satisfaction with the security aspects of system performance and maintenance support.		

NIST Checklist

DS	Disposal		
DS-1	**PREPARE FOR THE SECURITY ASPECTS OF DISPOSAL**		
DS-1.1	Develop the security aspects of the disposal strategy.	MS5, MS6	PC8, PC15, PC18, PC19
DS-1.2	Identify the system constraints resulting from the security aspects of disposal to be incorporated into the system requirements, architecture, and design.		
DS-1.3	Identify, plan for, and obtain the enabling systems or services to support the secure disposal of the system.	O19	O19
DS-1.4	Specify secure storage criteria for the system if it is to be stored.	PC10, O17, MS5, MS6	PC10, O17
DS-1.5	Identify and preclude terminated personnel or disposed system elements and materials from being returned to service.	O19 & O20	O19 & O20
DS-2	**PERFORM THE SECURITY ASPECTS OF DISPOSAL**		
DS-2.1	Deactivate the system or system element to prepare it for secure removal from operation.	MS13	
DS-2.2	Securely remove the system or system element from use for appropriate secure disposition and action.	O28, O26	O28, O26
DS-2.3	Securely withdraw impacted operating staff from the system and record relevant secure operation knowledge.	O28	O28
DS-3	**FINALIZE THE SECURITY ASPECTS OF DISPOSAL**		
DS-3.1	Confirm that no unresolved security factors exist following disposal of the system.	O19	O19, PC27
DS-3.2	Return the environment to its original state or to a secure state specified by agreement.	All	All
DS-3.3	Archive and protect information generated during the life cycle of the system.	O28	O28

ISMS Checklist

TECHNICAL PROCESSES		Device	PCH
		Traceability ID	Traceability ID
A5	**INFORMATION SECURITY POLICIES**		
A5.1	**MANAGEMENT DIRECTION FOR INFORMATION SECURITY**		
A5.2.1	Policies for information security	Spec	Spec
A5.2.2	Review of the policies for information security	NA	NA
A6	**ORGANIZATION OF INFORMATION SECURITY**		
A6.1	**INTERNAL ORGANIZATION**		
A6.1.1	Information security roles and responsibilities	O3	O3
A6.1.2	Segregation of duties	O3	O3
A6.1.3	Contact with authorities	O3	O3
A6.1.4	Contact with special interest groups	NA	NA
A6.1.5	Information security in project management	O5	O5
A6.2	**MOBILE DEVICE AND TELEWORKING**		
A6.2.1	Mobile device policy	NA	NA
A6.2.2	Teleworking	NA	NA
A7	**HUMAN RESOURCES SECURITY**		
A7.1	**PRIOR TO EMPLOYMENT**		
A7.1.1	Screening	NA	NA
A7.1.2	Terms and conditions of emplyment	NA	NA
A7.2	**DURING EMPLOYMENT**		
A7.2.1	Management responsibilities	Yes	Yes
A7.2.2	Information security awareness, education and training	O4,O5,O6,O7	O4,O5,O6,O7
A7.2.3	Disciplinary process	NA	NA
A7.3	**TERMINATION AND CHANGE OF EMPLOYMENT**		
A7.3.1	Termination or change of employment responsibilities	NA	NA
A8	**ASSET MANAGEMENT**		
A8.1	**RESPONSIBILITY FOR ASSETS**		
A.8.1.1	Inventory of assets	O26, MS7, MS13	O26
A.8.1.2	Ownership of assets	NA	NA
A.8.1.3	Acceptable use of assets	O26, MS15	O26, PC26
A 8.1.4	Return of assets	NA	NA
A8.2	**INFORMATION CLASSIFICATION**		

A.8.2.1	Classification of information	O6	O6
A.8.2.2	Labelling of information	O6	O6
A.8.2.3	Handling of assets	O6	O6
A8.3	**MEDIA HANDLING**		
A.8.3.1	Management of removable media	NA	NA
A.8.3.2	Disposal of media	NA	NA
A.8.3.3	Physical media transfer	NA	NA
A9	**ACCESS CONTROL**		
A9.1	**BUSINESS REQUIREMENTS FOR ACCESS CONTROL**		
A.9.1.1	Access control policy	MS3	PC13
A.9.1.2	Access to networks and network services	MS3	PC13
A9.2	**USER ACCESS MANAGEMENT**		
A.9.2.1	User registration and de-registration	NA	NA
A.9.2.2	User access provisioning	NA	NA
A.9.2.3	Management of privileged access rights	MS15	PC26
A.9.2.4	Management of secret authentication information of users	MS15	PC26
A.9.2.5	Review of user access rights	NA	NA
A.9.2.6	Removal or adjustment of access rights	NA	NA
A9.3	**USER RESPONSIBILITIES**		
A.9.3.1	Use of secret authentication information	MS15	PC26
A9.3	**SYSTEM AND APPLICATION ACCESS CONTROL**		
A.9.4.1	Information access restriction	NA	NA
A.9.4.2	Secure log-on procedures	NA	NA
A.9.4.3	Password management system	NA	NA
A.9.4.4	Use of privileged utility programs	MS15	PC26
A 9.4.5	Access control to program source code	NA	NA
A10	**CRYPTOGRAPHY**		
A.10.1	**CRYPTOGRAPHIC CONTROLS**		
A.10.1.1	Policy on the use of cryptographic controls	Spec	Spec
A.10.1.2	Key management	Spec	Spec
A11	**PHYSICAL AND ENVIRONMENTAL SECURITY**		
A.11.1	**SECURE AREAS**		
A 11.1.1	Physical security perimeter	MS14, DC8	O17
A.11.1.2	Physical entry controls	MS14, DC8	O17

ISMS Checklist

A.11.1.3	Securing offices, rooms and facilities	MS14, DC8	O17
A.11.1.4	Protecting against external and environmental threats	MS14, DC8	O17
A.11.1.5	Working in secure areas	MS14, DC8	O17
A.11.1.6	Delivery and loading areas	MS14, DC8	O17
A.11.2	**EQUIPMENT**		
A.11.2.1	Equipment siting and protection	MS14, DC8	O17
A.11.2.2	Supporting utilities	MS14, DC8	O17
A.11.2.3	Cabling security	MS14, DC8	O17
A.11.2.4	Equipment maintenance	MS14, DC8	O17
A.11.2.5	Removal of assets	MS14, DC8	O17
A.11.2.6	Security of equipment and assets off-premises	MS14, DC8	O17
A.11.2.7	Secure disposal or reuse of equipment	MS14, DC8	O17
A.11.2.8	Unattended user equipment	MS14, DC8	O17
A.11.2.9	Clear desk and clear screen policy	NA	NA
A12	**OPERATIONS SECURITY**		
A.12.1	**OPERATIONAL PROCEDURES AND RESPONSIBILITIES**		
A.12.1.1	Documented operating procedures	O5	NA
A.12.1.2	Change management	O5	NA
A.12.1.3	Capacity management	MS11	NA
A.12.1.4	Separation of development and operational environments	MS11	NA
A.12.2	**PROTECTION FROM MALWARE**		
A.12.2.1	Controls against malware	O5	O6
A.12.3	**BACKUP**		
A.12.3.1	Information backup	MS13	NA
A.12.4	**LOGGING AND MONITORING**		
A 12.4.1	Event Logging	MS13	NA
A 12.4.2	Protection of log information	MS13	NA
A 12.4.3	Administrator and operator logs	MS13	NA
A 12.4.4	Clock synchronization	MS13	NA
A.12.5	**CONTROL OF OPERATIONAL SOFTWARE**		
A.12.5.1	Instalation of software on operational systems	MS12, SQ14, SQ13, DM3	DC5, DM3
A.12.6	**TECHNICAL VULNERABILITY MANAGEMENT**		
A.12.6.1	Management of technical vulnerabilities	MS12, SQ14, SQ13, DM3	DC5, DM3

A.12.6.2	Restriction of software installation	MS12, SQ14, SQ13, DM3	DC5, DM3
A.12.7	**INFORMATION SYSTEMS AUDIT CONSIDERATIONS**		
A.12.7.1	Information systems audit controls	MS13	MS13
A13	**COMMUNICATIONS SECURITY**		
A.13.1	**NETWORK SECURITY MANAGEMENT**		
A.13.1.1	Network controls	Spec	Spec
A.13.1.2	Security of network services	Spec	Spec
A.13.1.3	Segregation in networks	Spec	Spec
A.13.2	**INFORMATION TRANSFER**		
A.13.2.1	Information transfer policies and procedures	NA	NA
A.13.2.2	Agreements on information transfer	NA	NA
A.13.2.3	Electronic messaging	NA	NA
A.13.2.4	Confidentiality or nondisclosure agreements	NA	NA
A.14	**SYSTEM ACQUISITION, DEVELOPMENT AND MAINTENANCE**		
A.14.1	**SECURITY REQUIREMENTS OF INFORMATION SYSTEMS**		
A.14.1.1	Information security requirements analysis and specification	O6	O6
A.14.1.2	Securing application services on public networks	MS3	NA
A.14.1.3	Protecting application services transactions	Spec	Spec
A.14.2	**SECURITY IN DEVELOPMENT AND SUPPORT PROCESSES**		
A.14.2.1	Secure development policy	Yes	Yes
A.14.2.2	System change control procedures	O5, DC9, MS15	O5, PC26
A.14.2.3	Technical review of applications after operating platform changes	O5	O5
A.14.2.4	Restrictions on changes to software packages	O5	O5
A.14.2.5	Secure system engineering principles	All	All
A.14.2.6	Secure development environment	O5	O5
A.14.2.7	Outsourced development	NA	NA
A.14.2.8	System security testing	All	All
A.14.2.9	System acceptance testing	All	All
A.14.3	**TEST DATA**		
A.14.3.1	Protection of test data	NA	NA
A.15	**SUPPLIER RELATIONSHIP**		
A.15.1	**INFORMATION SECURITY IN SUPPLIER RELATIONSHIP**		
A.15.1.1	Information security policy for supplier relationships	MS*, PC*	NA

ISMS Checklist

A.15.1.2	Addressing security within supplier agreements	NA	NA
A.15.1.3	Information and communication technology supply chain	NA	NA
A.15.2	**SUPPLIER SERVICE DELIVERY MANAGEMENT**		
A.15.2.1	Monitoring and review of supplier services	NA	NA
A.15.2.2	Managing changes to supplier services	NA	NA
A.16	**INFORMATION SECURITY INCIDENT MANAGEMENT**		
A.16.1	**MANAGEMENT OF INFORMATION SECURITY INCIDENTS AND IMPROVEMENTS**		
A.16.1.1	Responsibilities and procedures	O21	PC25
A.16.1.2	Reporting information security events	O21	PC25
A.16.1.3	Reporting information security weaknesses	O21	PC25
A.16.1.4	Assessment of and decision on information security events	O21	PC25
A.16.1.5	Response to information security incidents	O21	PC25
A.16.1.6	Learning from information security incidents	O21	PC25
A.16.1.7	Collection of evidence	O21	PC25
A.17	**INFORMATION SECURITY ASPECTS OF BUSINESS CONTINUITY MANAGEMENT**		
A.17.1	**INFORMATION SECURITY CONTINUITY**		
A.17.1.1	Planning information security continuity	O24	O24
A.17.1.2	Implementing information security continuity	NA	NA
A.17.1.3	Verify, review and evaluate information security continuity	NA	NA
A.17.2	**REDUNDANCIES**		
A.17.2.1	Availability of information processing facilities	MS6	No
A.18	**COMPLAINS**		
A.18.1	**COMPLAINS WITH LEGAL & CONTRACTUAL REQUIREMENTS**		
A.18.1.1	Identification of applicable legislation and contractual requirements	NA	NA
A.18.1.2	Intellectual property rights	NA	NA
A.18.1.3	Protection of records	MS13, O17	PC24, O17
A.18.1.4	Privacy and protection of personally identifiable information	O25	O25
A.18.1.5	Regulation of cryptographic controls	Spec	Spec
A.18.2	**INFORMATION SECURITY REVIEWS**		
A.18.2.1	Independent review of information security	O15,O17	O15, O17, PC2, PC3, PC5, PC6, PC7, PC8, PC22

ISMS Checklist

A.18.2.2	Compliance with security policies and standards	O15, O25, O17, MS11, MS12	O15, O17, O25, PC2, PC3, PC5, PC6, PC7, PC8, PC22
A.18.2.3	Technical compliance review	NA	NA

Traceability Matrix

S.No	Overall	PCH	Device Provider
O1	Document the entity applying for RD service certification & Models for certification is requested	Y	Y
O2	Document the single point of contact (SPC) profile and contact details. The SPC should be the product security manager. The SPC is responsible for both hardware and software security and set in place organizational processes to meet the security objectives of L1 RD service	Y	Y
O3	Document the stakeholder charts. Stakeholders include both third parties and internal resources involved in the L1 registered device process. Create a stakeholder chart documenting roles and responibilties of all entites involved in the L1 RD service solution. Please submit the agremments involving any 3rd partys defining their responsibilities.	Y	Y
O4	Document the security objectives for L1 registered device. This should include all security features as per the UIDAI L1 Registered device specification and any additional security features claimed by the PCH/Device providers	Y	Y
O5	Document the Secure Device Life Cycle process document including Secure Manufacturing process, Secure Provisioning process, SDLC process for software, Secure Maintanence/Patch management process followed for L1 device. The governance gates and approvals at each stage should be documented	Y	Y
O6	Document the requirements to meet the objectives of L1 registered device specification. Document should provide clear details on the security, data classification of senstive information classified as Secret, Internal, Public	Y	Y
O7	Document the threat model based on STRIDE and DREAD. Document the mitigations proposed and implemented.	Y	Y
O8	Document the overall architecture of the device defining the external interfaces. Both software and hardware interfaces should be documented	Y	Y
O9	Document the component & software design for L1 registered device. The design document should include the PCB design and all the key components and their connection details. It should also include a pictorial memory map view at rest and at operation	Y	Y
O10	Document the BOM for the device highlighting the security critical elments. Documentation should include all the parts and their vendor names.	Y	Y
O11	Document the sequence diagram of the key generation, key usage including the memory location where the keys are stored or processed.	**Y**	Y
O12	Provide a declaration from the PCH provider stating that the PCH provider has validated the design and the design has the correct usage of PCH.	Y	Y
O13	Document the tracebility matrix tracing the objective and how the architecture, design and implementation covers the security threats.	Y	Y

Traceability Matrix

O14	Document the security test strategy for all security claims. Methods used for test cases should be documented. All the test cases executed and their results should be documented	Y	Y
O15	Provide a formal security code review report. The report should cover review of the mitigation implemented for all software attacks mentioned in Section 3 of L1 registered device addendum.	Y	Y
O16	Document security controls/certification in place for provisioning,root of trust key storage, security for issuance of certifcate for the device.The root of trust, crypto library and Secure Boot Manager is the responsibility of the PCH provider. PCH provider is expected to ensure the proper identity key is inserted and tracked. The device provider has the responsibility to operate the device registration, key management, capture, process & protect biometrics.	Y	Y
O17	Provide security audit report of the provisioning partner.	Y	N
O18	Document the transition plan to move from one provisioning partner to another.	Y	N
O19	Document the SOP for disoposal of the L1 registered device. Document the device disposal process, include stolen device strategy, specifically clearing of sensitive information.	Y	Y
O20	Provide declaration that the device has a clear End Of life and end of support dates. End of life is defined as the date after which the device/PCH will not be manufactured. End of support is the date after which the software upgrades are not released and the device/PCH must be deregistered/removed from the UIDAI eco system	Y	Y
O21	Provide declaration stating "All new vulnerabililties, incidents related to L1 will be reported to UIDAI/STQC within the 24 hours of the occurance". In case of vulnerabilities or incidents its expected that the SPC provides the daily report of the progress made, workarounds, containment strategies until the final fix is delivered	Y	Y
O22	Document the monitoring mechanism and process for security related incidents.	Y	Y
O23	Document the process used for revocation of root of trust. In the event of a private key compromise of Device Provider/PCH document the process followed to inform UIDAI/STQC.	Y	Y
O24	Document the BCP plan Including all ecosystem partners: PCH, Management Server, Field Support, Certification management, Key Rotation etc.	Y	Y
O25	Provide a audit report of Compliance to Aadhaar act. At this time compliance to all elements of the traceability matrix will be sufficient for compliance to Aadhaar Act. However changes may occur in the future that could require an additional audit report.	N	Y

O26	Maintain the asset register in a spreadsheet with clear CIA (Confidentiality, Integrity, Availability) rating. Essential for Provisioning environment, Management server. Provide a declaration that asset database will be updated at regular interval (minimum of 1 week). Please refer to ISO 27001 process and asset register templates	Y	Y
O27	Document the details of the security awareness program details and schedule. Refer ISO 27001 for more details.	Y	Y
O28	Provide declaration that all sensitive backup keys and HSM backups are handled by the employees of device/PCH provider or its declared stakeholder and not individual contractors.	Y	Y
O29	Provide a declaration that periodic audit on physical security, keystorage, software signing, roles & responsibilities would be performed for all partners in the ecosystem. The reports should be submited to UIDAI upon request.	Y	Y
O30	Document the hardware block diagram with component list and PCH vendor details starting from image capture all the way to the encryption of the PID block	Y	Y
	PCH Certification		
PC1	Provide datasheet for chipset proposed to be used in the L1 registered design.	Y	N
PC2	Provide International certifications for secure crypto block in compliance to the objectives of the L1 RD specification	Y	N
PC3	Provide Certification for Cryptography algorithm (RSA, AES and SHA256) in compliance with objectives of the L1 RD specification	Y	N
PC4	Provide declaration and explain in detail for the protection mechanism built on PCH for side channel attacks	Y	N
PC5	Provide relevant international certifications for Trusted Execution Enviroment in case of shared hardware (Shared hardware means the PCH is used to run applications other than the RD Service).	Y	N
PC6	Provide declaration and reports to prove the cryptographic algorithms has resistance to side channel attacks	Y	N
PC7	Provide declaration that upon a tamper the chip would zero all the keys except the identity key.	Y	N
PC8	Provide declaration that the chip does not store the keys unencrypted in the non volatile storage	Y	N
PC9	Document the details of the proposed memory management profiles with clear demarcation of several zones and their respective rights.	Y	N
PC10	Document the secure boot sequence and root of trust certificate injection and storage for PCH and device vendor.	Y	N
PC11	Demonstrate the capability to perform secure boot, secure upgrade of OS.	Y	N
PC12	Demonstrate any security claims that are not covered under the listed certifications (international or self)	Y	N
PC13	Document the provisioning process including all third party vendors their roles and their security controls	Y	N

Traceability Matrix

PC14	Provide a letter of authorization from the provisioning vendor authorizing the UIDAI/STQC to intiaite audit of the facilities used for provisioning.	Y	N
PC15	Document and provide proof of the usage of FIPS 140-2 complaint Level 3 device to store the keys at the time of provisioning	Y	N
PC16	Document the approval process using a sequence diagram including the necessary checks and balances to release the latest trusted softwares by the provisioning facility.	Y	N
PC17	Document the process that would be followed for key rotation of root of trust.	Y	N
PC18	Provide declaration that all debug options are disabled as a part of provisioning process	Y	N
PC19	Provide declaration that all the private keys are stored, processed, used in secure memory from where extraction or cloning is not possible with the tools or techniques known at the time of submission for approval.	Y	N
PC20	Provide declaration that all encrypted/wrapped keys used for the encryption/wrapping should be AES 256 or RSA 2048	Y	N
PC21	Provide declaration that the encryption keys including generation of keys are never unwrapped or used in a non secure memory.		
PC22	Provide certification details for CC or FIPS or PCI precertification, PED compliance for the PCH.		
PC23	Provide declaration that the PCH configurations used for the international certifications as listed in PC23 is same as the one provided for the current need.	Y	N
PC24	Provide a declaration that audit records for all provisioning activities will be maintained for a period of 10 year	Y	N
PC25	Provide declaration that the keys stored on the PCH is not extractable with any of the current technologies. If PCH provider is aware of any such methods/technologies in the future that could extract sensitive keys then its the responsibility of the PCH provider to inform UIDAI/STQC.	Y	N
PC26	Document the change control procedure for software update, root of trust keys, vendor key management.	Y	N
PC27	Provide declaration that the PCH components can not be dismantled from the device after provisioning, If dismantled will not be in a usabled condition with all its secret keys deleted.	Y	N
PC28	Provide declaration that all debug options are disabled as a part of provisioning process and the debug feature cannot be subsequently enabled by the device provider or on the field.	Y	N
PC29	Provide declaration that the AES keys used to encrypt the PID are not logged or stored or sent out of the cryptographic library	Y	N
	Device Certification		
DC1	Provide declaration that biometric data is not logged or stored or sent out other than the UIDAI prescribed format.	N	Y
DC2	Provide a declaration that the memory used to process the biometric data can not be modified by any external means.	N	Y

Traceability Matrix

DC3	Design document for the timestamp sync feature.	N	Y
DC4	Design document for the software upgrade design as per the specification.	N	Y
DC5	Provide declaration that all cryptographic operations use the cryptographic library provided by the PCH.	N	Y
DC6	Document explaining the logic used to identify your device during registration.	N	Y
DC7	Document the location, roles and responsibilities of users and security of the keys used for signing the device provider softwares.	N	Y
DC8	Document the change control process followed for new software upgrades.	N	Y
DC9	Provide declaration that a biometric can not be injected into the L1 device. If injected the device will not sign the biometric	N	Y
DC10	Document the measures taken to prevent the seperation of the PCH and the sensor	N	Y
DC12	Provide User manual for the device (L1 registered device.).	N	Y
	'Management Server'		
MS1	Document management server architecture		Y
MS2	Document high availability for management Server		Y
MS3	Document secure connection from RD Service and management server		Y
MS4	Document the deployment and security architecture of the management server		Y
MS5	Document the HSM security in the Management Server. Provide evidence of the FIPS 140-2 level 3 at which the HSM is operating.		Y
MS6	Provide evidence regarding the DR HSM and the FIPS level.		Y
MS7	Document the methodology to pre-load device serial number in the management server		Y
MS8	Document the time sync for the management servers.		Y
MS10	Features for Key rotation upon manual trigger, Blacklist or delist a device, handling lost devices and other device management features should be part of the management server and same has to be demonstrated.		Y
MS11	Monitor the sever for bussiness continuity, security and operations.		Y
MS12	Provide declaration that every month the management servers a vulnerability assessment is performed on the public facing IP address (addresses) and every major release a penetration testing is performed. The reports should be presented upon need		Y
MS13	All devices managed by the server should have audit records about the device registration, key rotation, host combinations for a period of 6 months. The audit records should be backed up at end of day.		Y
MS14	Physical security of the HSM and management server should be ensured.		Y
MS15	Document the HSM change control procedures.		Y
	RD Service		
RD1	Document discovery of the RD Service		Y
RD2	Document handling of multiple RD Service on same host		Y

Traceability Matrix

RD3	Document multiple applications talking to same RD service		Y
	Sequence Diagram for "init" Function		
SQI1	Document sequence Diagram for device registration		Y
SQI2	Document sequence diagram for key rotation		Y
SQI3	Document sequence diagram for RD service update		Y
SQI4	Document sequence diagram for UIDAI Public Key update		Y
	Sequence Diagram for "capture" Function		
SQC1	Document sequence diagram for Preview if available		Y
SQC2	Document sequence diagram for Quality check if available		Y
SQC3	Document sequence diagram for capture, sign and encrypt		Y
	Demonstration		
DM1	Demonstrate that the secure boot will occur only if the hardware and software systems and subsystems are trusted.	Y	N
DM2	Demonstrate secure upgrade will occur only in case of the trusted software and hardware integrity needs to be reconfirmed.	Y	N
DM3	Demonstrate that the lower version of a valid patch cannot be pushed as an update.	Y	Y
DM4	Demonstrate device identitification process which should combine device id, Chip identity key, PCH root of trust	N	Y
DM5	Demonstrate all functional test cases with the RD service functional test suite	N	Y
DM6	Demonstrate commands and command security between the rd service and device	N	Y
DM7	Demonstrate debug enabled and disabled options. This should ensure that any change in the debug modes should clear all the sensitive keys.	Y	N
DM8	Demonstrate debug is disabled and can not be enabled.	Y	Y
DM9	Demonstrate time sync between the mangement server and the device	N	Y
	System Level Tamper Responsiveness (Optional for certification)		
T1	Document list of tamper responsive features available pre-certified hardware along with the necessary international certification	Y	N
T2	Document list of system level tamper responsive features against chemical attacks, probing attacks, memory remanance attack	N	Y
T3	Provide declaration from the PCH vendor validating the system level tamper responsiveness design and implementation to ensure all sensitive data would be cleared upon tamper attempt	Y	Y
T4	Document the design of the features listed in T2	N	Y
T5	Demonstrate all the features listed in T2	N	Y