Digital Certificate Management Standard

Version No	5.1
Document Type	Standard
Parent Document	Group Information and Cyber Security Policy
Parent Framework	Information & Cyber Security RTF
Document Approver Name	Jamie Cowan
Document Approver Job Title	Head, ICS Risk Framework & Governance
Document Owner Name	Ibrahim Gathungu
Document Owner Job Title	Director, ICS Standards
Document Contact Name	Katarzyna Wencka
Document Contact Job Title	Director, ICS Standards
Business Scope	All Businesses
Function Role	All Functions
Geography Scope	Global
Effective Date	17 February 2025
Approval Date	4 December 2024
Next Review Date	13 September 2027

Standard Chartered Bank

www.sc.com

Table of Contents

Version Control Table

Name	Changes made	Materiality	Approved by	Version number	Approval Date	Effective Date
Anna Kowal-Hughes **[ICS Standards]**	Editorial changes: 1. Document template updated in line with Template for Group Standards, V 7.0 2. Document references updated 3. Roles references updated in line with the new org structure	Non-material	Jamie Cowan Head, ICS Risk Framework & Governance	5.1	04-Dec-24	17-Feb-25

1 INTRODUCTION AND SCOPE

The purpose of a Public-Key Infrastructure [PKI] is to exchange trust between parties which do not know each other. PKI is based on the concept of having trust in entities because they are trusted by an entity which is trustworthy. In a hierarchically organised PKI the Certificate Authority [CA] is the topmost instance and is known and trusted by all other members of the PKI.

The most important tool within the PKI concept is the Digital Certificate. It is the certification of trust in the Digital Certificate holder by the CA. The Digital Certificate contains the unique name of the certificate holder, the electronic verifiable signature of the CA and the public key of the certificate holder, as well as some Information on the use of the Digital Certificate.

Examples of Digital Certificates:

- Server certificates (such as Transport Layer Security [TLS] certificates): used to establish trust in application server's identity and to establish secure connectivity.

- Client certificates (such as Virtual Private Network [VPN] and Network Access Control [NAC] certificates): used to establish trust in the clients' identity.

- Code Signing certificates: used for signing specific code/app/APIs

- Digital Signing certificates (such as Secure Multipurpose Internet Mail Extensions [S/MIME]): used for signing the emails, documents etc. so that Third Parties can verify the sender's identity and ensure that data is not altered during transmission.

This Security Standard defines the control requirements for PKI and Digital Certificates as the overall approach to establishing trust, proving identity of users, devices and services as well as for secure connectivity, authentication, code signing and digital signing in the Group.

1.1 Risks[1]

The Digital Certificate Management Standard mandates that adequate controls are implemented for non-repudiation, authentication, confidentiality and integrity protection of Group Information and Technology Assets.

Failure to adopt and implement this Standard may expose the Group to risks which may result into:

- Financial Loss by External Attacker and/or Trusted Insider,
- Disclosure of Sensitive Information by External Attacker and/or Trusted Insider,
- Disruption of Business Operations by External Attacker and/or Trusted Insider.

1.2 Scope

This Standard must be read, and controls deployed in conjunction with all other ICS Standards.

The Standard is mandatory and applies to the Group businesses, functions, and countries/regions except where explicitly prohibited by local Law or Regulation [assessed as per section 4.2 Reporting Non-Compliance].

[1] As defined by the ICS risk sub-types in the ERMF

***Note:** In case of any Country specific LRM requirement, the approach defined in ERMF (Chapter Eleven, Part B, section 4.2 "Country-level Host Regulatory Obligations") must be followed.*

The Standard covers all Digital Certificates which are used by the Group, in the Group's Technology Assets and by 3rd parties (when processing Group's Information or hosting Group's Technology Assets). Wherever the term 'Systems' or 'Information System' is used in a control statement it refers to Information System, Application(s) and Technology Infrastructure.

Where a Control Statement is aligned to an Information Asset [IA] or S-BIA ratings, they are applicable only to those rated Systems. All other Control Statements apply to all Systems regardless of ratings and hosted environments [Production or Non-Production unless stated otherwise].

The Systems owned and or managed by the Third Parties [including Cloud Systems, Vendor Systems, Regulatory Systems, Self Service Terminal [SST] and similar], must additionally refer to the ICS Standards for Security in Interactions with Third Parties, Secure Asset Management and Secure Configuration Management.

1.3 Out of scope

This Standard does not define the requirements for cryptographic aspects of the Digital Certificates as well as the requirements for securing confidential cryptographic elements/attributes of Digital Certificates, such as private keys. Those aspects are defined and regulated by the ICS Cryptography Standard.

The Digital Certificates as in the 3rd party Technology Assets, which are not owned by the Group are considered out of scope.

2 ROLES & RESPONSIBILITIES

Information Asset/System Owner [includes Owner of underlying Application(s)/Product and Technology Infrastructure]

The Information Asset/System Owner is accountable for the protection of their Information Assets and Information Systems and with complying to the Control Statements applicable to them.
They are also responsible for ensuring that the Application and Technology Infrastructure Owners correctly apply the controls as set out in this standard.
As first line role holders they must have in place a model for validation of control existence and effectiveness.

Process Owner [of the DCM Process]

As defined in Enterprise Risk Management Framework [ERMF] and appointed by Group CISO, in line with applicable requirements of ICS Standards.

All Staff

All Staff are responsible for the safety of Group Technology Assets under their care, the security of Group Information allowed for accessing via the Technology Assets and for compliance with the applicable Control Statements defined in this Standard.

People Leader

People Leaders must comply with the requirements and ensure that their Staff are made aware of their responsibilities in complying to this standard.

CISO ICS Standards & Controls

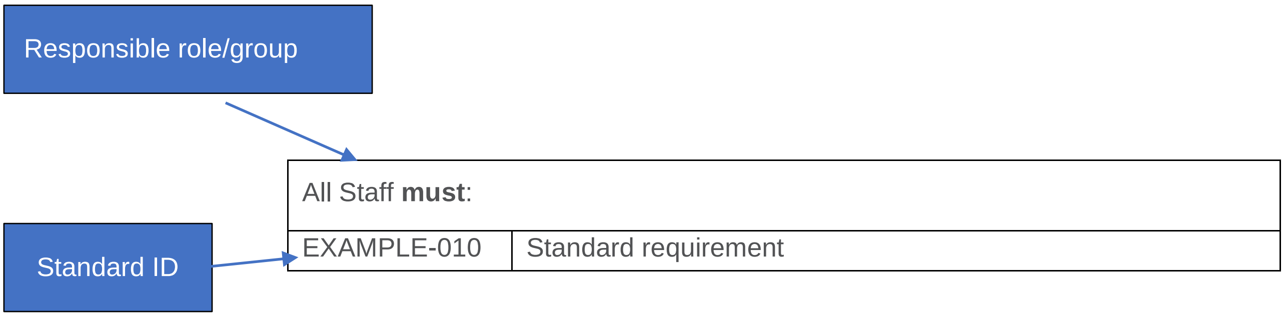
The CISO is the owner of this Security Standard and will ensure the document is updated to an agreed schedule.

***Note**: The Responsible role who **‘must’** execute against this standard can do so either directly or by delegation. Where this is the case and a delegate exercises the control, the named role remains accountable.*

All roles & responsibilities including their corelations within ICS risk management activities are defined in Chapter Eleven, Part B, section 2 “Three LoD Responsibility and Governance Committee Oversight” of the Enterprise Risk Management Framework.

3 STANDARD REQUIREMENTS

This section outlines minimum mandatory requirements that apply to this Standard. The requirements are set out in the following format:



3.1 Control Area: Usage of Digital Certificates

3.1.1 General Provisions

All Staff **must**:	
DCM-020	Always obtain authorization from the DCM Process Owner/Internal Certificate Authority (“ICA”) team for any use of the Digital Certificates for the Group purposes, especially for: 1) the use of Internal Digital Certificates outside the Group, 2) the use of Public and Self-signed Digital Certificates within the Group’s internal systems, 3) the procurement and use of any 3rd party issued Digital Certificates. *[Example: Internal digital Certificates may be used/shared outside the Group for 3rd party integration purposes, code development by 3rd party, etc.].* *[Objective: Digital Certificates used in the Group are under robust governance and use strong and effective cryptography to ensure required level of trust in terms of data protection and proving the identity of users, devices and services.]*
DCM-060	Ensure that the Digital Certificate is: 1) always requested or procured in line with DCM Process requirements, 2) used only for the purpose, scope and context it is issued for and in line with applicable guidance provided by the DCM Process Owner/ICA team, 3) checked for validity of applicable parameters/attributes as per the approved procedure (as defined by the DCM PO), 4) not used after expiration, except decryption of information/data with the use of associated private key. *[Example: Digital Certificates issued for encryption purposes must not be used for authentication.* *[Reference: Digital Certificate fields “Key Usage” and “Extended Key Usage”]* *[Objective: Digital Certificates used in the Group are under robust governance and use strong and effective cryptography to ensure required level of trust in terms of data protection and proving the identity of users, devices and services.]*
DCM-070	*[consolidated under DCM-060].*

All Staff **must**:	
DCM-080	Ensure that in case of suspicion of disclosure, compromise, theft or loss of any confidential cryptographic element corresponding with Digital Certificate (such as private keys or data media containing those), this fact is reported to ICA without undue delay. *[Objective: Digital Certificates which are orphaned' (i.e. the need for their use is no longer present) or can no longer be trusted (for example: due to private key compromise, owner compromise, flaws in the used cryptography or Digital Certificate itself) are revoked so they cannot be used or misused and the risk of identity spoofing or data compromise is mitigated.]*
DCM-090	*[consolidated under DCM-060]*
DCM-100	Ensure that issued Digital Certificate is: 1) requested for renewal only if still required and in advance as defined by the DCM Process, 2) requested for revocation if no longer required. *[Objective:* *1) Digital Certificates must be renewed periodically to ensure the need for their issuing is still valid and only strong and secure technologies and cryptography is used.* *2) Digital Certificates which are 'orphaned' (i.e. the need for their use is no longer present) or can no longer be trusted (for example: due to private key compromise, owner compromise, flaws in the used cryptography or Digital Certificate itself) are revoked so they cannot be used or misused and the risk of identity spoofing or data compromise is mitigated.]*

People Leader **must**:	
DCM-110	Ensure that all Digital Certificates (and corresponding cryptographic material) used in the Group are replaced or revoked when Staff with access to them leave the Group or move to a different department within the Group. *[Objective: Digital Certificates that are orphaned' (i.e. the need for their use is no longer present) or can no longer be trusted (for example: due to private key compromise, owner compromise, flaws in the used cryptography or Digital Certificate itself) are revoked so they cannot be used or misused and the risk of identity spoofing or data compromise is mitigated.]*
DCM-111	Ensure that private keys of Staff's revoked Digital Certificates are retained in a secured environment in line with the guidance from the DCM Process. *[Objective: The Group data/information encrypted with private keys corresponding with expired Digital Certificates must be available to authorised stakeholders as per the retention period.]*

3.1.2 Digital Certificates use in Group's Technology Assets

Information System/Technology Infrastructure/Application Owner **must**:	
DCM-120	Ensure that Digital Certificate is: 1) requested in line with their use and purpose (as per the applicable template and usage pattern), 2) used only for the purpose, scope and context it is issued for and in line with applicable guidance provided by the DCM Process Owner/ICA team. *[Reference: Digital Certificate fields "Key Usage" and "Extended Key Usage"]* *[Objective:* *1) Digital Certificates used in the Group are under robust governance and use strong and effective cryptography to ensure required level of trust in terms of data protection and proving the identity of users, devices and services.* *2) Digital Certificate's attributes and specification corresponds with the ICS risk exposure and nature of their use, so the anticipated risk can be effectively mitigated.]*
DCM-125	Ensure that effective automatic checks of the Digital Certificate validity are implemented and enabled, at its every usage, in Information System and Technology Infrastructure. *[Note: Validity of Digital Certificate should include:* • *Verification of the validity period (start date and expiration date),* • *Verification of the validity of signature of the Digital Certificate,* • *Verification of the certificate's revocation status* • *Verification that the Certificate Authority which issued the Digital Certificate is trusted.]* *[Objective: Only valid, trusted and compliant Digital Certificates can be considered as effective in protecting data and proving the identity of users, devices and services.]*
DCM-130	*[consolidated under DCM-120]*
DCM-140	Ensure that all Information Systems and all Technology Infrastructure (where required) have only valid and compliant Digital Certificate installed. *[Note: For self-signed Digital Certificate please follow DCM-145 and DCM-145a.]* *[Objective: Only valid, trusted and compliant Digital Certificates can be considered as effective in protecting data and proving the identity of users, devices and services.]*
DCM-145	*[moved to section for Requesting & Issuing Digital Certificates (from ICA)]*

Information System/Technology Infrastructure/Application Owner **must**:	
DCM-150	Ensure that all Digital Certificates used by the Group (except self-signed certificates, as defined by DCM-145) are issued/procured, managed, and tracked by the ICA team. AND Never use/implement Digital Certificates which are not issued, procured or accepted by the DCM PO/ICA team (except self-signed certificates, as per the DCM-145). *[Note:* *1) If any non-compliant DC (DC issued by non-trusted Third Party's CA or any DC using unapproved algorithms), must be used then SIA must be conducted.* *2) If it contradicts with local LRM requirements then ICA team must be notified about procured Digital Certificates (except self-signed certificates, as per the DCM-145)]* *[Objective:* *1) Digital Certificates used in the Group are under robust governance and use strong and effective cryptography to ensure required level of trust in terms of data protection and proving the identity of users, devices and services.* *2) Digital Certificates used in the Group are identified and inventoried so:* *a. any anomalies can be detected and handled;* *b. ICS incidents and risk events (involving to the Digital Certificates use) can be effectively manged.* *3) Only valid, trusted and compliant Digital Certificates can be considered as effective in protecting data and proving the identity of users, devices and services.]*
DCM-160	*[consolidated under DCM-150]*
DCM-170	Request the revocation of Digital Certificates when no longer required. AND Request the revocation and replacement of Digital Certificates when their purpose, scope or context changes. *[Example: when decommissioning of Technology Assets]* *[Objective:* *1) Digital Certificates must be renewed periodically to ensure the need for their issuing is still valid and only strong and secure technologies and cryptography is used.* *2) Digital Certificates which are 'orphaned' (i.e. the need for their use is no longer present) or can no longer be trusted (for example: due to private key compromise, owner compromise, flaws in the used cryptography or Digital Certificate itself) are revoked so they cannot be used or misused and the risk of identity spoofing or data compromise is mitigated.]*
DCM-190	*[covered by DCM-080]*
DCM-195	*[covered under DCM-125]*

Information System/Technology Infrastructure/Application Owner **must**:	
DCM-720 *[new]*	Ensure that for owned Technology Asset(s) there is a proper documentation and validated mechanisms/procedures for Digital Certificates management. AND Digital Certificates used are compliant with applicable requirements of the Standard and DCM Process. *[Objective:* *1) Only valid, trusted and compliant Digital Certificates can be considered as effective in protecting data and proving the identity of users, devices and services.* *2) The specification and use of Digital Certificates in Technology Assets is identified, documented and manageable to allow for effective response to ICS incidents as well as compliance with the DCM PO requirements.]*

Technology Product/Application Owner **must**:	
DCM-730 *[new]*	Ensure that Application/Technology Product has available, validated and documented mechanisms/procedures for Digital Certificates management to ensure that Group compliant certificates (as per the DCM-370) can be deployed. *[Objective:* *1) Only valid, trusted and compliant Digital Certificates can be considered as effective in protecting data and proving the identity of users, devices and services.* *2) The specification and use of Digital Certificates in Technology Assets is identified, documented and manageable to allow for effective response to ICS incidents as well as compliance with the DCM PO requirements.]*

3.2 Control Area: PKI Architecture and Governance

3.2.1 Group PKI

Process Owner [of the DCM Process] **must**:	
DCM-197 *[new]*	Define, maintain and deploy the Group Public Key Infrastructure ("PKI") in line with applicable requirements of this Standard and industry best practices. *[Objective:* *1) Digital Certificates used in the Group are under robust governance and use strong and effective cryptography to ensure required level of trust in terms of data protection and proving the identity of users, devices and services.* *2) Only valid, trusted and compliant Digital Certificates can be considered as effective in protecting data and proving the identity of users, devices and services.]*

Process Owner [of the DCM Process] **must**:	
DCM-230	Document the requirements for the end-to-end Digital Certificate Management (as defined by this Standard) as well practises employed by Internal (private) Certificate Authority (“ICA”) in the Group PKI in: 1) Certificate Policy (“CP”) and Certificate Practice Statement (“CPS”), 2) applicable operational instructions and procedures for the DCM Process end-users. AND Ensure the documentation is kept up to date and available to applicable stakeholders. *[Objective:* *1) Digital Certificates used in the Group are under robust governance and use strong and effective cryptography to ensure required level of trust in terms of data protection and proving the identity of users, devices and services.* *2) Only valid, trusted and compliant Digital Certificates can be considered as effective in protecting data and proving the identity of users, devices and services.]*
DCM-200	Define, maintain and deploy the model and architecture for the Group PKI that: 1) establishes the Trust Anchor(s) (i.e. authoritative entity(-ies) for trust) 2) enforces a hierarchical trust model(s) with established Trust Anchor(s) 3) delivers required interoperability with relevant PKIs at root level, 4) is trusted by the Group’s users and Technology Assets. *[Objective:* *1) Digital Certificates used in the Group are under robust governance and use strong and effective cryptography to ensure required level of trust in terms of data protection and proving the identity of users, devices and services.* *2) Only valid, trusted and compliant Digital Certificates can be considered as effective in protecting data and proving the identity of users, devices and services.]*
DCM-201	*[Moved to DCM-200]*
DCM-210	*[Moved to DCM-200]*
DCM-220	Ensure that only strong and secure cryptographic standards and solutions are used for the Group PKI and Digital Certificates (used in the Group) by: 1) identifying, documenting and deploying applicable industry standards (for components of the Group PKI) 2) ensuring compliance with applicable requirements of the ICS Cryptography Standard, 3) defining trusted and approved tools, products and hardware in use to support PKI related activities (such as key generation and distribution, secure key storage, etc.) with relevant level of compliance. *[Objective:* *1) Digital Certificates used in the Group are under robust governance and use strong and effective cryptography to ensure required level of trust in terms of data protection and proving the identity of users, devices and services.* *2) Only valid, trusted and compliant Digital Certificates can be considered as effective in protecting data and proving the identity of users, devices and services.]*
DCM-221	Ensure effective delivery of the trust model (for the Group PKI) as well as the automation of the Certificate Lifecycle Management (“CLM”) practises via integration (of the Group's PKI) with the relevant Group's technology and security services and solutions, such as: directory/repository/configuration systems like: Active Directory/LDAP, SCCM, DNS, etc. *[Objective: Digital Certificates lifecycle is, where possible, automated to minimise human interaction to ensure data accuracy and integrity, prevent errors, issues and risk events such as key comprise or fraudulent requests.]*

Process Owner [of the DCM Process] **must**:	
DCM-250	Define, deploy and maintain effective and secure architecture of the Group's PKI considering: 1) Subordinate/Issuing CA(s) to mitigate the impact of potential root CA breaches, 2) Registration Authorities ("RAs") for vetting requests for Digital Certificates, in line with documented and reviewed procedure and applicable requirements of this Standard. *[Objective:* *1) Digital Certificates lifecycle is, where possible, automated to reduce the likelihood of errors and flaws due to human interaction.* *2) CA architecture ensure not only effective digital certificate related services delivery, but also limits likelihood and impact of potential CA breaches or risk events.* *3) Requests for Digital Certificates are diligently verified to ensure they are issued to authorised and trusted parties and use in line with their issuing purpose.]*
DCM-222	*[Moved to DCM-200]*
DCM-240	*[Moved to DCM-230]*

3.2.2 Federated Services for Digital Certificate Management

Information System Owner [of the PKIs in the Group] **must**:	
DCM-740 *[new]*	1) Identify, document, deploy and follow applicable DCM Process requirements (as defined by the DCM PO) when delivering any PKI solutions in the Group. 2) Consult and obtain approval for any new or materially changed PKI service(s) from the DCM PO. *[Objective: PKI services in the Group are delivered in a consistent manner to ensure their compliance and effective delivery of Digital Certificate use objectives.]* *[Note: Decentralised PKI is any internal Group PKI, other that the one owned and managed by the DCM PO. Such PKIs can be established on an exceptional basis due to tangible technology or regulatory limitations.]*

3.3 Control Area: Identification and Authentication [I&A]

Process Owner [of the DCM Process] **must**:	
DCM-250	*[moved to section for Group PKI]*
DCM-260	*[moved under section for Requesting and Issuing Digital Certificates]*
DCM-270	*[consolidated under DCM-260]*
DCM-280	*[removed as covered by general requirements defined in ICS Standards]*
DCM-290	*[moved to section for general provisions for digital certificates]*
DCM-300	*[moved under section for Monitoring & Auditing Digital Certificates]*
DCM-310	*[moved to principle level under DCM-260]*

3.4 Control Area: Certificate Lifecycle Management (“CLM”)

3.4.1 General Provisions for Digital Certificates

Process Owner [of the DCM Process] **must**:	
DCM-370	Define and document types and categories of Digital Certificates for use in the Group together with the attributes to drive compliance with applicable PKI and regulatory requirements. *[Objective: Digital Certificates’ types and their attributes correspond with the purpose of their use, anticipated ICS risk of that use as well as industry best practices and regulatory requirements.]*
DCM-370a	Enforce overall compliance of the Digital Certificates by defining, deploying and maintaining templates and usage patterns for requesting, procuring and issuing Digital certificates, that mandate presence of applicable attributes, including: 1) their purpose/use and applicable use constraints, 2) issuing CA and CA signature (except root CA and self-signed DCs), 3) subject, 4) utilised encryption and signing algorithms, 5) relevant key(s), 6) serial number, 7) thumbprint, 8) key timestamps such as issue and expiration date and renewal period, 9) timelines and conditions for renewal. *[Objective:* *1) Digital Certificates types and their attributes correspond with the purpose of their use, anticipated ICS risk of that use as well as industry best practices and regulatory requirements.* *2) Only valid, trusted and compliant Digital Certificates can be considered as effective in protecting data and proving the identity of users, devices and services.]*
DCM-370b	Ensure that the attributes and corresponding values mandated via Digital Certificate templates and usage patterns commensurate with the: 1) intended use and purpose of the Digital Certificate, 2) applicable regulatory requirements, industry standards/best practices, 3) applicable requirements of the ICS Cryptography Standard, and 4) ICS risk exposure. *[Objective:* *1) Digital Certificates types and their attributes corresponds with the purpose of their use, anticipated ICS risk of that use as well as industry best practices and regulatory requirements.* *2) Only valid, trusted and compliant Digital Certificates can be considered as effective in protecting data and proving the identity of users, devices and services.]*

Process Owner [of the DCM Process] **must**:	
DCM-370c	Enforce effective use of the Digital Certificate templates and usage patterns by: 1) creating and issuing Digital Certificates compliant with applicable templates and usage patterns, 2) reviewing external Digital Certificates for compliance with applicable template(s) and usage patterns, 3) revoking and (if applicable) replacing any Digital Certificates considered non-compliant. *[Objective:* *1) Digital Certificate's types and their attributes corresponds with the purpose of their use, anticipated ICS risk of that use as well as industry best practices and regulatory requirements.* *2) Only valid, trusted and compliant Digital Certificates can be considered as effective in protecting data and proving the identity of users, devices and services.]*
DCM-550	Define, deploy and maintain the repository for Digital Certificates (used by the Group) with relevant level of details so PKI activities can be effectively supported. AND Support the accuracy of the repository with predefined discovery activities. *[Objective:* *1) Digital Certificates used in the Group are identified and inventoried so:* *a. any anomalies can be detected and handled,* *b. ICS incidents and risk events (involving to the Digital Certificates use) can be effectively manged.* *2) Only valid, trusted and compliant Digital Certificates can be considered as effective in protecting data and proving the identity of users, devices and services.]*
DCM-320	Define, deploy, maintain and manage key activities for Certificate Lifecycle Management ("CLM") (for both internal and externa Digital Certificates used by the Group) considering: 1) activities for registering/revoking key PKI entities, such as Issuing or Registration Cas, 2) requesting, creating, issuing, suspending/revoking, renewing, distributing, and destroying Digital Certificates. *[Objective: Digital Certificates used in the Group are under robust governance and use strong and effective cryptography to ensure required level of trust in terms of data protection and proving the identity of users, devices and services.]*
DCM-290	Where possible and effective, automate CLM related activities. *[Objective: Digital Certificates lifecycle is, where possible, automated to minimise human interaction to ensure data accuracy and integrity, prevent errors, issues and risk events such as key comprise or fraudulent requests.]*

3.4.2 Monitoring & Auditing of Certificates

Process Owner [of the DCM Process] **must**:	
DCM-300	Store and retain Digital Certificate registration data. AND Keep an audit trail of the key activities related to Digital Certificates management and lifecycle. *[Objective: Key metadata corresponding with Digital Certificate lifecycle are available for audit and verification.]*
DCM-750 *[new]*	Ensure that verification and reporting approach is in place to track and verify the compliance status (i.e. alignment with the DCM Process requirements) of the Digital Certificates (as per the inventory). *[Reference: DCM-370, DCM-550]* *[Objective:* *1) Digital Certificates used in the Group are under robust governance and use strong and effective cryptography to ensure required level of trust in terms of data protection and proving the identity of users, devices and services.* *2) Only valid, trusted and compliant Digital Certificates can be considered as effective in protecting data and proving the identity of users, devices and services.]*

3.4.3 Requesting & Issuing Digital Certificates (from ICA)

Process Owner [of the DCM Process] **must**:	
DCM-260	Deploy procedures for both automated and manual requests for Digital Certificates ensuring that only valid requests result in Digital Certificate issuance and registration, i.e. requests: 1) from validated and authorised users or entities, 2) using/following pre-defined templates and usage patterns, 3) meeting all other applicable requirements as defined in CP/CPS. *[Objective:* *1) Digital Certificates used in the Group are under robust governance and use strong and effective cryptography to ensure required level of trust in terms of data protection and proving the identity of users, devices and services.* *2) Only valid, trusted and compliant Digital Certificates can be considered as effective in protecting data and proving the identity of users, devices and services.* *3) Requests for Digital Certificates are diligently verified to ensure they are issued to authorised and trusted parties and use in line with their issuing purpose.]*
DCM-145	Define and formalise the criteria, requirements and use limitations for the use of self-signed Digital Certificates. *[Objective: Use of self-signed Digital Certificates is limited to cases where:* *1) the risk anticipated from their use is within the Group ICS risk appetite, AND* *2) there are specific limitations of the technology.]*

Process Owner [of the DCM Process] **must**:	
DCM-315	Where required, provide Digital Certificate Usage guidance (to relevant stakeholders, including Staff, People Leaders and Technology Asset & Product Owners) regarding: 1) requesting and using Digital Certificates as well as limitations for the Digital Certificates use (such as use of self-signed certificates or Group certificates externally, use of the certificates in line with the purpose of their issuing), 2) 'how-to' for checking the Digital certificates validity, 3) mandatory activities in the case of loss or disclosure of a certificate private key, 4) use and use limitations for revoked or suspended certificates, 5) any retention requirements for the certificates used by the Group, 6) applicable destruction requirements and guidance. *[Objective:* 1) *Digital Certificates' types and their attributes correspond with the purpose of their use, anticipated ICS risk of that use as well as industry best practices and regulatory requirements.* *2) Digital Certificates used in the Group are under robust governance and use strong and effective cryptography to ensure required level of trust in terms of data protection and proving the identity of users, devices and services.* *3) Relying parties are fully aware of the risks and implications of improper use of Digital Certificates as well as the importance of proper Digital Certificates handling.]*

All Staff/Information System/Technology Infrastructure/Application/Product Owners **must**:	
DCM-260a *[new]*	1) Adhere to formal DCM Process requirements when requesting Digital Certificates 2) Use only formal requests that correspond with requested Digital Certificate type and purpose. *[Objective:* 1) *Digital Certificates types and their attributes correspond with the purpose of their use, anticipated ICS risk of that use as well as industry best practices and regulatory requirements.* *2) Digital Certificates used in the Group are under robust governance and use strong and effective cryptography to ensure required level of trust in terms of data protection and proving the identity of users, devices and services.* *3) Relying parties are fully aware of the risks and implications of improper use of Digital Certificates as well as the importance of proper Digital Certificates handling.]*
DCM-145a *[new]*	Follow DCM Process requirements in the case of self-signed certificate creation and use, considering special provisions and use limitations. *[Objective:* *1) Use of self-signed Digital Certificates is limited to cases where the risk anticipated from their use is low and can be accepted.* *2) Relying parties are fully aware of the risks and implications of improper use of Digital Certificates as well as the importance of proper Digital Certificates handling.]*

3.4.4 Digital Certificates Suspension, Revocation and Renewals (from ICA)

Process Owner [of the DCM Process] **must**:	
DCM-385	Establish a process of informing all Digital Certificates Owners about upcoming Digital Certificate expiration in line with the timeframes defined (as per applicable Digital Certificates templates for validity period and renewal period). *[Reference: DCM-370]* *[Objective:* *1) Expiration alerts must be sent early enough to allow (where applicable) Digital Certificate renewal prior its expiration date to minimise operational impact.* *2) Only valid, trusted and compliant Digital Certificates can be considered as effective in protecting data and proving the identity of users, devices and services.* *3) Digital certificates are renewed periodically to ensure the use of technology and cryptography that can effectively deliver the objectives of Digital Certificates use (i.e. proving identity and protecting data).]*
DCM-410	Define and enforce procedure(s) for Digital Certificates renewal, ensuring that: 1) every renewal request is checked for validity and integrity and verified against predefined criteria before being accepted, 2) Digital Certificate renewal results in generation of a new key pair. *[Objective:* *1) Digital Certificates must be renewed periodically to ensure the need for their issuing is still valid and only strong and secure technologies and cryptography is used.* *2) Digital Certificates which are 'orphaned' (i.e. the need for their use is no longer present) or can no longer be trusted (for example: due to private key compromise, owner compromise, flaws in the used cryptography or Digital Certificate itself) are revoked so they cannot be used or misused and the risk of identity spoofing or data compromise is mitigated.* *3) Requests for Digital Certificates are diligently verified to ensure they are issued to authorised and trusted parties and use in line with their issuing purpose.* *4) Digital Certificates lifecycle is, where possible, automated to minimise human interaction to ensure data accuracy and integrity, prevent errors, issues and risk events such as key comprise or fraudulent requests.]*
DCM-470	Define and enforce procedure(s) for Digital Certificates suspensions and revocations ensuring that: 1) certificate revocation or suspension is available via Online Certificate Status Protocol ("OCSP") without undue delay and in Certification Revocation List ("CRL") as per the DCM Process defined timelines, 2) triggers/cases for certificates revocation and suspension are predefined, 3) suspended certificates are either invalidated permanently (via revoking them) or revalidated (against pre-defined criteria) without undue delay. *[Objective:* *1) Relying parties are made aware, without undue delay, of Digital Certificates which are no longer considered trusted or valid to mitigate the risk of their use.* *2) Only valid, trusted and compliant Digital Certificates can be considered as effective in protecting data and proving the identity of users, devices and services.* *3) Digital Certificates that are orphaned' (i.e. the need for their use is no longer present) or can no longer be trusted (for example: due to private key compromise, owner compromise, flaws in the used cryptography or Digital Certificate itself) are revoked so they cannot be used or misused and the risk of identity spoofing or data compromise is mitigated.]*

Process Owner [of the DCM Process] **must**:	
DCM-450	Ensure that CRLs: 1) are published in predefined timelines (except point (3)), 2) are supplemented with metadata allowing verification for integrity, validity, source and time/date of their publication, 3) are updated and re-published without undue delay in the case of DCs suspension or revocation due to ICS incidents or risk events. *[Objective: Relying parties are made aware, without undue delay, of Digital Certificates which are no longer considered trusted or valid to mitigate the risk of their use.]*

Process Owner [of the DCM Process] **must**:	
DCM-315	*[moved under section for Requesting and Issuing Digital Certificates]*
DCM-320	*[moved to section for General Provisions for Digital Certificates]*
DCM-330	*[merged with DCM-320]*
DCM-350	*[consolidated under DCM-370]*
DCM-370	*[moved to section for General Provisions for Digital Certificates]*
DCM-380	*[consolidated under DCM-370]*
DCM-385	*[moved under section for DC suspension, revocation and renewals]*
DCM-390	*[consolidated under DCM-410]*
DCM-400	[consolidated under DCM-410 & 470]
DCM-410	*[moved under section for DC suspension, revocation and renewals]*
DCM-430	*[consolidated under DCM-410]*
DCM-440	*[consolidated under DCM-470]*
DCM-450	*[moved under section for DC suspension, revocation and renewals]*
DCM-460	*[consolidated under DCM-450]*
DCM-470	*[moved under section for DC suspension, revocation and renewals]*
DCM-480	*[consolidated under DCM-450]*
DCM-490	*[moved under section for Ensuring ICA resiliency]*

3.5 Control Area: Operational and Technical Security Controls

3.5.1 Ensuring ICA resiliency

Process Owner [of the DCM Process] **must**:	
DCM-490	Publish and deliver notification to impacted stakeholders (such as Digital Certificate Owners, Information Asset Owners, System Owners, etc) about: 1) any ICA downtime caused by planned maintenance – in advance allowing for preparation, 2) any ICA downtime caused by disaster – without undue delay, 3) ICA data loss, data leakage, private key compromises, unauthorized access – without due delay. *[Objective:* *1) Relying parties are informed about incidents or risk events corresponding with Digital Certificates so remediation and containment of such events can be initiated.* *2) Relying parties are made aware, without undue delay, of Digital Certificates which are no longer considered trusted or valid to mitigate the risk of their use.]*
DCM-570	Define, test and document (to the sufficient level of details) for the pre-defined disaster/incident case-scenarios: 1) communication plans for informing impacted stakeholders about CA related incidents or risk events, 2) remediating action plan(s) to minimise the security or business impact of CA related incidents or risk events. *[Objective: Remediation of Digital Certificates corelated incidents and risk events is effective and timely so the impact of such events is reduced.]*
DCM-580	Ensure that there is a procedure for ICA termination to ensure required obligations and liability (as defined by applicable controls of this Standard) of the ICA is preserved by a successor instance for a transition period or a secure termination of all services. *[For example: private keys, including backup copies, certification key material, Digital Certificates, customer data.]* *[Objective: PKI service is delivered in a continuous, reliable and effective manner ensuring its objectives are delivered successfully.]*

3.5.2 Top keys generation

Process Owner [of the DCM Process] **must**:	
DCM-510	Ensure the keys generation for all Internal CAs (i.e. root and sub-CAs) follows applicable requirements from the ICS Cryptography Standard (for key ceremonies) and is: 1) performed with a defined key generation procedure (including that key pair renewal and the corresponding ICA Digital Certificate is done before the private key usage period of the previous CA certificate ends), 2) performed with a defined key backup procedure. *[Objective:* *1) Top keys for CA(s) are generated in a manner ensuring they are protected from disclosure, loss, misuse and manipulation.* *2) PKI service is delivered in a continuous, reliable and effective manner ensuring its objectives are delivered successfully.]* *[Reference: ICS Cryptography Standard]*

Process Owner [of the DCM Process] **must**:	
DCM-520	Ensure that the generation of a new key pair and the corresponding ICA Digital Certificate is done before the private key usage period of the previous CA certificate ends. *[Objective: PKI service is delivered in a continuous, reliable and effective manner ensuring its objectives are delivered successfully.]*
DCM-540	*[consolidated under DCM-220]*
DCM-550	*[moved to section for General Provisions for Digital Certificates]*
DCM-570	*[moved to section for Ensuring ICA resiliency]*
DCM-580	*[moved to section for Ensuring ICA resiliency]*

3.5.3 Control Area: Role Management

Process Owner [of the DCM Process] **must**:	
DCM-590	*[covered under IAM Standard]*
DCM-600	*[covered under IAM Standard]*

3.6 Control Area: Procurement of External Digital Certificates

Information System/Technology Infrastructure/Application Owner **must**:	
DCM-610	Ensure that, for any Digital Certificate from an external unapproved CA, is requested and procured in line with applicable procedure defined by the DCM PO/ICA team (as per the DCM-620). *[Reference: DCM-620]* *[Objective:* *1) Only valid, trusted and compliant Digital Certificates can be considered as effective in protecting data and proving the identity of users, devices and services.* *2) Requests for Digital Certificates are diligently verified to ensure they are issued to authorised and trusted parties and use in line with their issuing purpose.* 3) *Digital Certificates types and their attributes correspond with the purpose of their use, anticipated ICS risk of that use as well as industry best practices and regulatory requirements.* *4) Digital Certificates used in the Group are under robust governance and use strong and effective cryptography to ensure required level of trust in terms of data protection and proving the identity of users, devices and services.]*
DCM-040	*[consolidated under DCM-610]*
DCM-630	Obtain ICA Team approval for correct technical usage of externally procured Digital Certificate type. *[Objective:* 1) *Digital Certificate's types and their attributes correspond with the purpose of their use, anticipated ICS risk of that use as well as industry best practices and regulatory requirements.* *2) Only valid, trusted and compliant Digital Certificates can be considered as effective in protecting data and proving the identity of users, devices and services.]*

Process Owner [of the DCM Process] **must**:	
DCM-620	Define, document and deploy an approach to procurement of Digital Certificates from external/Public CA(s) considering verification of applicable security requirements (i.e. CP/CPS) such as: 1) integrity of the Digital Certificate through its entire lifecycle (registration, renewal, revocation, expiry), 2) security of root and issuing CA including physical, organisational, access and audit logging and monitoring control, 3) use of strong cryptography and industry standards for keys generation and management. *[Objective:* 1) *Digital Certificate's types and their attributes correspond with the purpose of their use, anticipated ICS risk of that use as well as industry best practices and regulatory requirements.* 2) *Only valid, trusted and compliant Digital Certificates can be considered as effective in protecting data and proving the identity of users, devices and services.]*
DCM-635	Ensure that: 1) all external CAs that passed the assessment (as defined in the DCM Process) with a positive result will be listed by ICA Team as trusted, 2) an external Digital Certificate issuance request will be placed to a trusted external CA listed by ICA Team. *[Objective: Only valid, trusted and compliant Digital Certificates can be considered as effective in protecting data and proving the identity of users, devices and services.]*
DCM-640	*[consolidated under DCM-635.]*
DCM-650	Ensure that external trusted Public CA/CAs undergo CP/CPS re-assessment (performed by ICA Team as per DCM-620) every year or when a major infrastructure change is implemented by that CA. *[Reference: DCM-620]* *[Objective: Only valid, trusted and compliant Digital Certificates can be considered as effective in protecting data and proving the identity of users, devices and services.]*

3.7 Control Area: Transport Layer Security Guidelines

Process Owner [of the DCM Process] **must**:	
DCM-700	Define, document, maintain and publish Transport Layer Security guidelines to outline security principles for the acceptable Cryptographic Cipher suites for the TLS Protocol deployments, considering available inputs as per VPM-350. *[Objective: Group data is effectively protected from disclosure and manipulation via use of secure communication protocols and standards.]* *[Reference: VPM-350]*

4 INFORMATION & SUPPORT

4.1 General Information and Support

For queries relating to this Security Standard please contact the ICS Standards team via: *ICSStandards*

4.2 Reporting Non-Compliance

As a general guideline, any non-compliance against the Applications and underlying Technology Infrastructure in CMDB should follow the ICS Non-Compliance Register (ICS NCR) process. Further assessment of these non-compliance should follow the issue management process, i.e. iTrack for issues with remediation plan or ICS Dispensation when there is an explicit decision not to remediate the issue.

4.3 Breach of this Standard

- Failure to comply with this Standard may result in formal action under the Group Disciplinary Standard, that for serious breaches could include termination of employment.
- Any actual or suspected breaches must be reported immediately to your People Leader or to your Compliance representative from the Group.
- All breaches of this Standard must be reported to the Document Owner of the Standard.

5 GLOSSARY

The ICS Standards Glossary has been defined and is available via the *GovPoint* – see the *Technology Glossary* via the *GovPoint Glossary* reference.

6 REGULATORY / INDUSTRY REFERENCES

All Regulatory/Industry References are available via the *ICS Master Control List* document published on: *Control Framework Library*

Appendix A – Version Control Table

Name	Changes made	Materiality	Approved by	Version number	Approval Date	Effective Date
CISO ICS Policy	New Standard	New Standard	Gareth Carrigan, Global Head, ICS Governance, Policy and Risk	1.0	28-Jun-19	28-Jun-19
Yogesh Kumar Venkatesan	To align with recent Org change, reference to CISO amended to CISRO accordingly within the document.	Non-material	Liz Banbury, Head, ICS Policy	1.1	30-Dec-19	30-Dec-19
Bali Chandramouli	Correction of duplicate numbering from Section “3.1 Control Area: Operational and Technical Security Controls” To “3.5 Control Area: Operational and Technical Security Controls”.	Non-material	Liz Banbury, Global Head, ICS Policy and Risk	1.2	10-Feb-20	30-Dec-19
CISRO ICS Policy	Annual Review		Liz Banbury	2.0	02-Oct-20	02-Oct-20
CISRO ICS Policy	DCM-350 amended in line with ICSCR-1Sep2021-1 Editorial changes	Non-material	Samantha Finan, Global Head, ICS Policy, Standards and Reporting	2.1	10-Dec-21	01-Jan-22
CISRO ICS Policy	1. Editorial: document template updated 2. ICSCR-14Oct2021-1: DCM-700 and DCM-710 added (plus Table 2) 3. ICSCR-3Feb2022-1: DCM-370 updated Non-inclusive terminology replaced	Material	Samantha Finan, Global Head, ICS Policy, Standards and Reporting	3.0	22-Jun-22	01-Jul-22
CISRO ICS Policy	Editorial changes: 1. Document template updated in line with the Template for Group Standards, v5.6	Material	Paul Hoare Head, ICS Policy and Best Practice	4.0	03-Nov-23	01-Jan-24

Name	Changes made	Materiality	Approved by	Version number	Approval Date	Effective Date
	2. Document references updated 3. People Manager role updated to People Leader, TDR Architecture updated to SACA. New controls: 1. DCM-145 (ICSCR-28Jul23-1) Controls amended: 1. DCM-020, DCM-140, DCM-315, DCM-610, DCM-040, DCM-620 (ICSCR-28Jul23-1) 2. Accountable role corrected for DCM-120, DCM-125, DCM-130, DCM-140, DCM-150, DCM-160, DCM-170, DCM-190, DCM-195, DCM-200, DCM-201, DCM-210, DCM-220, DCM-221, DCM-222, DCM-230, DCM-240, DCM-250, DCM-260, DCM-270, DCM-280, DCM-290, DCM-300, DCM-310, DCM-315, DCM-320, DCM-330, DCM-350, DCM-370, DCM-380, DCM-385, DCM-390, DCM-400, DCM-410, DCM-430, DCM-440, DCM-450, DCM-460, DCM-470, DCM-480, DCM-490, DCM-510, DCM-520, DCM-540, DCM-550, DCM-570, DCM-580, DCM-590, DCM-600, DCM-					

Name	Changes made	Materiality	Approved by	Version number	Approval Date	Effective Date
	610, DCM-040, DCM-630, DCM-620, DCM-635, DCM-640, DCM-650 (ICSCR-28Jul23-1) Removed: 1. DCM-010 removed as relocated to AUS (ICSCR-18Feb2022-1) 2. DCM-030, DCM-050, DCM-051 (ICSCR-28Jul23-1)					
OTCR ICS Policy	Editorial: 1. Document template aligned with Template for Group Standards v5.7 2. Document references updated (as per the ICS RTF consolidation under ERMF) Material: 1. ICS controls simplification in line with the principles and strategic approach for ICS Standards simplification (ICSCR-10Apr24-1) 2. Consideration of ICSCR-21Mar24-1, ICSCR-21Mar24-2, ICSCR-21Mar24-3 3. Control requirements supplemented for Digital Certificates within Technology Assets and products (in terms of general requirements) 4. Introduction of requirements for DC templates and	Material	Mark Strange Global Head, OTCR, TTO	5.0	16-Sep-24	17-Feb-25

Name	Changes made	Materiality	Approved by	Version number	Approval Date	Effective Date
	trust anchors management					
Anna Kowal-Hughes **[ICS Standards]**	Editorial changes: 4. Document template updated in line with Template for Group Standards, V 7.0 5. Document references updated 6. Roles references updated in line with the new org structure	Non-material	Jamie Cowan Head, ICS Risk Framework & Governance	5.1	04-Dec-24	17-Feb-25