

MCMC MTSFB TC G051:2025

TECHNICAL CODE

DIGITAL IDENTITY SECURITY MANAGEMENT

Developed by



Registered by



Registered date: 27 February 2025

© Copyright 2025

MCMC MTSFB TC G051:2025

Development of Technical Codes

The Communications and Multimedia Act 1998 (Laws of Malaysia Act 588) ('the Act') provides for a Technical Standards Forum designated under section 184 of the Act or the Malaysian Communications and Multimedia Commission ('the Commission') to prepare a technical code. The technical code prepared pursuant to section 185 of the Act shall consist of, at least, the requirements for network interoperability and the promotion of safety of network facilities.

Section 96 of the Act also provides for the Commission to determine a technical code in accordance with section 55 of the Act if the technical code is not developed under an applicable provision of the Act and it is unlikely to be developed by the Technical Standards Forum within a reasonable time.

In exercise of the power conferred by section 184 of the Act, the Commission has designated the Malaysian Technical Standards Forum Bhd ('MTSFB') as a Technical Standards Forum which is obligated, among others, to prepare the technical code under section 185 of the Act.

A technical code prepared in accordance with section 185 shall not be effective until it is registered by the Commission pursuant to section 95 of the Act.

For further information on the technical code, please contact:

Malaysian Communications and Multimedia Commission (MCMC)

MCMC Tower 1
Jalan Impact
Cyber 6
63000 Cyberjaya
Selangor Darul Ehsan
MALAYSIA

Tel : +60 3 8688 8000
Fax : +60 3 8688 1000
Email : stpd@mcmc.gov.my
Website: www.mcmc.gov.my

OR

Malaysian Technical Standards Forum Bhd (MTSFB)

Level 3A, MCMC Tower 2
Jalan Impact
Cyber 6
63000 Cyberjaya
Selangor Darul Ehsan
MALAYSIA

Tel : +60 3 8680 9950
Fax : +60 3 8680 9940
Email : support@mtsfb.org.my
Website: www.mtsfb.org.my

Contents

	Page
Committee representation.....	ii
Foreword	iii
0. Introduction.....	1
1. Scope	1
2. Normative references	2
3. Abbreviations.....	2
4. Terms and definitions	4
5. Overview of Digital Identity Security Management (DISM)	5
6. Benefits of Digital Identity Security Management (DISM)	6
7. Framework for Digital Identity Security Management (DISM).....	8
8. Identity management.....	9
8.1 Overview of identity management.....	9
8.2 Identity assurance	10
8.3 Identity assurance requirements	11
8.4 Identity collection, validation and verification	12
8.5 Threats and security considerations	15
9. Credential Management	16
9.1 Overview of credential management	16
9.2 Authentication assurance.....	16
9.3 Privacy requirements	21
9.4 Summary of requirements.....	21
9.5 Authenticator and verifier requirements	22
9.6 Authenticator lifecycle management	28
9.7 Threat and security considerations	32
10. Access management.....	35
10.1 Overview of access management.....	35
11. Regulatory and compliance requirements.....	40
11.1 Regulatory	41
11.2 Other regulatory and compliance requirements.....	41
11.3 Sector specific compliance.....	42
12. DISM effectiveness measurement	43
Bibliography	46

MCMC MTSFB TC G051:2025

Committee representation

This technical code was developed by the Security, Trust and Privacy Working Group of the Malaysian Technical Standards Forum Bhd (MTSFB), which consists of representatives from the following organisations:

CyberSecurity Malaysia

Digital Connect Society

FNS (M) Sdn Bhd

Malaysia Digital Economy Corporation Sdn Bhd

Smart Tech AP Sdn Bhd

Universiti Kuala Lumpur

Foreword

This technical code for Digital Identity Security Management ('Technical Code') was developed pursuant to Section 185 of the Communications and Multimedia Act 1998 (Laws of Malaysia Act 588) by the Security, Trust and Privacy Working Group of the Malaysian Technical Standards Forum Bhd (MTSFB).

This Technical Code shall continue to be valid and effective from the date of its registration until it is replaced or revoked.

(THIS PAGE IS INTENTIONALLY LEFT BLANK)

DIGITAL IDENTITY SECURITY MANAGEMENT

0. Introduction

Digital Identities (DI) are credentials (or authenticators) which are issued by Credential Service Providers (CSP) and then used (minimally) in support of user authentication into online services operated by Relying Parties (RP). DI instances are issued to human users with identities of high assurance, as vouchsafed by identity documents issued by designated authoritative parties. CSP operators are obliged to undertake identity proofing of users against such documents, validation of such user-presented identities with other designated authoritative parties, and then to implement binding of such identity to the issued authenticator. DI instances in subsequent use are subject to a lifespan of specified duration; and within that a lifecycle encompassing the possibilities of renewal, expiration, termination and (unfortunately) compromise.

The CSP and RP specifications herein are roles and actions which may be located within a single organisation or alternatively reside in different organisations. In this context, the CSP issues user-specific DI instances for subsequent use in RP-specific business cases. RP organisations would also have the flexibility to choose one or more CSP organisations from which to source their user populations.

Digital Identity Security Management (DISM) specifies CSP obligations pertaining to security actions against specific threats, and privacy protection measures against specific risks and to satisfy compliance requirements. Whenever possible; all security, privacy, identity and trust measures should be by-design or by-default; such that assurance of security and privacy is not infeasibly reliant on undue trust in operator compliance sans evidence thereof.

The DISM scope of interest is in CSP-side processes for DI instantiation and then use and management thereof over such DI lifecycle. This document does not seek to regulate RP-side use of such DI in their business processes, beyond advice that risk management pertaining to those processes should be commensurate with DI assurance as specified by the CSP at point of issue to the legitimate user. This document, in accordance with international specification and practise, articulates assurance classifications based on the stringency of DI initial enrolment and subsequent use.

This Technical Code likewise does not seek to regulate the issue of credentials without connectivity to real-world identities, i.e. employee (badge) numbers, self-asserted social media names, or communication provider identities as applicable to email or chat. We acknowledge the prevalence and practicality of credentials based on such identifiers but would point out the impossibility of assigning credible assurance to any process that does not use identity documents of high assurance and universal acceptability. The basic operational concept is that DI use is intended to be equivalent, in functional and perhaps even legal terms, to the presentment of a real-world identity document in physical interactions, hence the necessity for technological and operational stringency.

This Technical Code is not intended to replace other regulatory and industry frameworks, standards or guidelines. The use of DISM and the associated security requirements and references shall support and/or compliment the code of practice for organisations in the industry.

1. Scope

This Technical Code provides a set of requirements and references which serves as a guidance to the Communication and Multimedia Industry (CMI) and others as applicable, on Digital Identity Security Management (DISM) and the required implementation, security measures and protection from security threats and attacks.

MCMC MTSFB TC G051:2025

This Technical Code covers the following elements.

- a) Digital Identity Security Management (DISM)
 - i. Identity management.
 - ii. Credential management.
 - iii. Access management.
- b) Regulatory and compliance requirements.
- c) DISM effectiveness measurement.

2. Normative references

The following normative references are indispensable for the application of this Technical Code. For dated references, only the edition cited applies. For undated references, the latest edition of the normative references (including any amendments) applies.

MCMC MTSFB TC G042, *Information and Network Security - Malaysia Critical Security Controls (MYCSC)*

ISO/IEC WD 29115.2, *Information security, cybersecurity and privacy protection – Entity authentication assurance framework*

National Institute of Standards and Technology (NIST) SP 800-63, *Digital identity guidelines*

National Institute of Standards and Technology (NIST) SP 800-63A, *Enrolment and identity proofing*

National Institute of Standards and Technology (NIST) SP 800-63B, *Authentication and lifecycle management*

3. Abbreviations

For the purposes of this Technical Code, the following abbreviations apply.

AAL	Authentication Assurance Level
ABAC	Attribute-Based Access Control
AG	Access Governance
BNM	Bank Negara Malaysia
CMI	Communication and Multimedia Industry
CSP	Credential Service Provider
CSRF	Cross-Site Request Forgery
DAC	Discretionary Access Control
EAL	Evaluation Assurance Level
EDR	Endpoint Detection and Response
FMR	False Match Rate
GRC	Governance Risk and Compliance

MCMC MTSFB TC G051:2025

GDPR	General Data Protection Regulation (EU)
IAL	Identity Assurance Level
ICAM	Identity, Credential and Access Management
IGA	Identity Governance and Administration
INS	Information and Network Security
IoT	Internet of Things
ISMS	Information Security Management System
IT	Information Technology
JITA	Just-in-Time Access
MAC	Mandatory Access Control
MFA	Multi-Factor Authentication
MYCSC	Malaysia Critical Security Controls
NIST	National Institute of Standards and Technology
OWASP	Open Web Application Security Project
PAD	Presentation Attack Detection
PAW	Privileged Access Workstations
PCI DSS	Payment Card Industry Data Security Standard
PD	Policy Document
PDPA	Personal Data Protection Act
PII	Personally Identifiable Information
PIN	Personal Identification Number
PKI	Public Key Infrastructure
PSTN	Public Switched Telephone Network
RBAC	Role-Based Access Control
RMIT	Risk Management in Technology (BNM)
RP	Relying Party
SMS	Short Message Service
SOC	Service Organisation Control
SoD	Segregation of Duties
SSO	Single Sign-On
TEE	Trusted Execution Environment
TPM	Trusted Platform Module
URL	Uniform Resource Locator
USB	Universal Serial Bus
VOIP	Voice Over Internet Protocol

MCMC MTSFB TC G051:2025

4. Terms and definitions

For the purposes of this Technical Code, the following terms and definitions apply.

4.1 Authenticator Assurance Level (AAL)

A category describing the strength of the authentication process.

4.2 Access Management

Refers to the processes and technologies used to control and monitor network access.

4.3 Authentication

Provision of assurance that a claimed characteristic of an entity is correct

4.4 Authenticator

Something the claimant possesses and controls (typically a cryptographic module or password) that is used to authenticate the claimant's identity

4.5 Authorisation

Process to determine whether the authenticated user has permission to perform the action they have requested.

4.6 Binding

An association between a user identity and an authenticator or given subscriber session.

4.7 Biometric

Automated recognition of individuals based on their biological and behavioral characteristics.

4.8 Credential Service Provider (CSP)

A trusted entity that issues or registers subscriber authenticators and issues electronic credentials to subscribers. A Credential Service Provider (CSP) may be an independent third party or issue credentials for its own use.

4.9 Cryptographic authenticator

An authenticator where the secret is a cryptographic key.

4.10 Digital Identity (DI)

The provision of identity (ID) and identification of a person and its credentials, including the description of the user and their access privileges. The digital identity (DI) empowers users to access organisation applications, data and resources, subject to authorisation of the DI for such access.

4.11 Identity Assurance Level (IAL)

A category that conveys the degree of confidence that the applicant's claimed identity is their real identity.

4.12 Identity, Credential and Access Management (ICAM)

A security and business discipline that includes multiple technologies and business processes to help the right people or machines to access the right assets at the right time for the right reasons, while keeping unauthorised access and fraud at bay.

4.13 Identity proofing

The process by which a CSP collects, validates, and verifies information about a person.

4.14 Identity lifecycle management

Refers to the entire set of processes and technologies for maintaining and updating digital identities.

4.15 Multi-Factor Authentication (MFA)

An authentication system that requires more than one distinct authentication factor for successful authentication. Multi-factor authentication can be performed using a multi-factor authenticator or by a combination of authenticators that provide different factors. The three authentication factors are something you know, something you have, and something you are.

4.16 Managed policy

A set of rules that your IAM system follows. It documents what users, groups, and roles have access to which resources.

4.17 Privileged account management

Refers to managing and auditing accounts and data access based on the privileges of the user. A privileged user, for example, would be able to set up and delete user accounts and roles.

4.18 Relying parties

Refers to an entity that relies upon the user's authenticator(s) and credentials or a verifier's assertion of a claimant's identity, typically to process a transaction or grant access to information or a system.

4.19 Network infrastructure

Refers to all the resources of a network that make network or internet connectivity, management, business operations and communication possible. It consists of hardware and software, systems and devices and it enables computing and communication between users, services, applications and processes. Network infrastructure can be cloud, physical or virtual.

5. Overview of Digital Identity Security Management (DISM)

Digital Identity Security Management (DISM) provides a structured approach for enterprises to design, plan, and implement Identity, Credential, and Access Management (ICAM) processes, serving as a strategic guide for establishing a comprehensive digital identity management programme and developing a clear solution roadmap. The DISM focuses on enterprise identity processes, practices, policies, and information security disciplines.

An organisation enterprise identity is the unique representation of an employee, contractor, or enterprise user, which could be a critical access control to the enterprise resources to achieve its mission and business goals.

MCMC MTSFB TC G051:2025

DI is a credential, as used for online authentication but also possibly for digital signing, the initial creation and subsequent use of which is dependent on and integrated with the real-world identity of the human user who is properly assigned and authorised to use the particular credential.

In the Malaysian context, this real-world identity of an individual is as specified in identity documents of the strongest possible assurance:

a) MyKad

Issued by the *Jabatan Pendaftaran Negara* (JPN)

b) Passport

Issued by a sovereign nation or jurisdiction, with possible validation by the *Jabatan Imigresen Malaysia* (JIM) for foreign nationals physically present in Malaysia.

c) Document issued by approved authority.

These identity documents would be used for the digital identity (DI) use cases of interest:

a) CSP: that issue DIs; and

b) RP: that use such DIs to establish user identity and actions arising.

This Technical Code seeks to address a broad range of initial issue, and subsequent use process by means of classification in terms of assurance, such that RP entities that use these DI assertions are able to take into account the risks and limitations inherent in such DI assurance classifications, and then to associate such assurance levels with the appropriate authorisation and access control configurations.

6. Benefits of Digital Identity Security Management (DISM)

The advantages of DISM extend beyond security. In our digitally connected world, DISM also enhances organisational productivity. DISM's security benefits include user and device verification, identity validation, and management controls for user and device access to organisational resources.

DISM may also offer a centralised identity database that stores essential information about user identities and their attributes. This information can be utilised by all systems for access management, thereby improving business processes and information security.

When implemented correctly, DISM should provide the following benefits to the organisation. Table 6.1 below shows the benefits of DISM and their categories.

Table 1. DISM benefits by category

No.	Benefits of DISM	Description	Category
1	Improved user or customer experience and supply chain security	Information Technology (IT) administrators can create a unique digital identity for each user, which includes a set of credentials. DISM with ICAM provides secure and convenient end-user access to the organisation's applications and resources. DISM with the Single Sign-On (SSO) method allows users, customers or suppliers to access various applications with their unique identity.	Identity

Table 2. DISM benefits by category (continued)

No.	Benefits of DISM	Description	Category
2	Improved technology efficiency and faster application delivery time	Improve system integration and efficiency of application development, deployment, and management by eliminating the need for duplication and proliferation of vulnerable systems and user management.	Identity
3	Enhanced efficiency of security teams	Apart from improving the security posture, the most significant benefit of DISM is enhancing the efficiency and effectiveness of security teams.	Identity
4	Reduced IT operating costs	DISM helps organisations save operating costs by minimising the time and manpower needed to deal with user account-related issues.	Identity
5	Information sharing	DISM should facilitate collaboration and information sharing among business units and applications.	Identity
6	Improved collaboration with government and regulators	The organisation and the government/regulators may have mutually beneficial relationships enabled by DISM.	Identity
7	Reduction in password issues	By enabling easier sign-in processes, DISM prevents many password-related issues. DISM solutions may offer password or password-less management features that help security admins implement password best practices.	Credential
8	Secure MFA	DISM with effective ICAM and MFA may include technologies such as biometrics: iris scanning, fingerprint sensors, face recognition, and more. MFA ensures that the user provides at least two or more sources of evidence to confirm their identity.	Credential
9	Management of cloud-based security access across browsers and devices	DISM with cloud-based ICAM systems can provide browser-based SSO to all user applications and enable access to those same services from users' mobile devices.	Access
10	Improved security and faster time to market	DISM with the right ICAM solutions should help organisations implement robust security policies across all systems, platforms, applications, and devices. DISM enables easier identification of security violations, quick removal of inappropriate access privileges, and revocation of access when necessary.	Access
11	Data confidentiality	By restricting access to those who don't need to use certain apps or files, organisations can better secure sensitive data and enable security controls with a clearer picture of which users are associated with which applications and resources.	Access
12	Improved regulatory and industry compliance audit	Government regulations and compliance such as Personal Data Protection Act (PDPA) and General Data Protection Regulation (GDPR) hold organisations accountable for controlling access to customer and employee information.	Access
13	Reduction in human error	With ICAM in place, DISM should enable organisations to eliminate manual account and permission errors because the IT department no longer has to manually manage access rights to data.	Access

Table 3. DISM benefits by category (concluded)

No.	Benefits of DISM	Description	Category
14	Advanced tracking of malicious activity	DISM with state-of-the-art ICAM systems may offer advanced tracking of malicious behaviour using Artificial Intelligence (AI), machine learning, and risk-based authentication.	Access
15	Easy distribution of security policies and enforcement of Identity Governance and Administration (IGA)	DISM provides a common platform to apply and enforce security policies to all organisational systems with ease based on the organisation's IGA.	Access
16	Enhanced data security	Consolidating authentication and authorisation functionality on a single platform provides IT professionals with a consistent method for managing user access.	Access
17	More effective access to resources	DISM with SSO provides security and convenience to the users. When users access through a centralised platform, the use of SSO technology should limit the number of interactions users have with security backend systems.	Access

DISM enhances organisational productivity and security. It reduces password reset time, verifies user and device identities, and provides management controls. DISM also offers a centralised identity database for improved business processes and information security. Key benefits include improved user experience, enhanced security, secure MFA, cloud-based security access management, improved technology efficiency, data confidentiality, and regulatory compliance. DISM also reduces IT operating costs, minimises human error, facilitates information sharing, tracks malicious activity, and provides effective access to resources. Overall, DISM is a valuable tool in our digitally connected world.

7. Framework for Digital Identity Security Management (DISM)

DISM Framework is based on ICAM that provides a set of tools, policies, and systems that an organisation uses to enable the right individual having the right to access the right resources at the right time, for the right reason in support of the organisational business objectives. ICAM is the combination of technical systems, policies and processes that create, define, govern the utilisation, and safeguarding identity information, as well as managing the relationship between an entity and the resources to which access is granted.

The DISM framework is focusing on ICAM that provides a high-level understanding of identity, credential and access management, security requirements, capabilities and services. DISM framework for ICAM should enable an organisation to verify the users' real-world identity and issue credential, authenticate, authorise the users' role based on their identity, manage the user account, monitor users' behaviour and compliance audit. The framework creates a basic foundation for building a secure and trusted digital environment and capabilities for securing enterprise-wide information sharing based on a secure identity, credential and access management for the organisation. The physical access control mechanisms are outside the scope of this framework.

The DISM framework based on ICAM, as in Figure 1, summarises the relationship among the 3 components in managing digital identity in organisations as follows:

- a) Identity management;
- b) Credential management; and
- c) Access management.

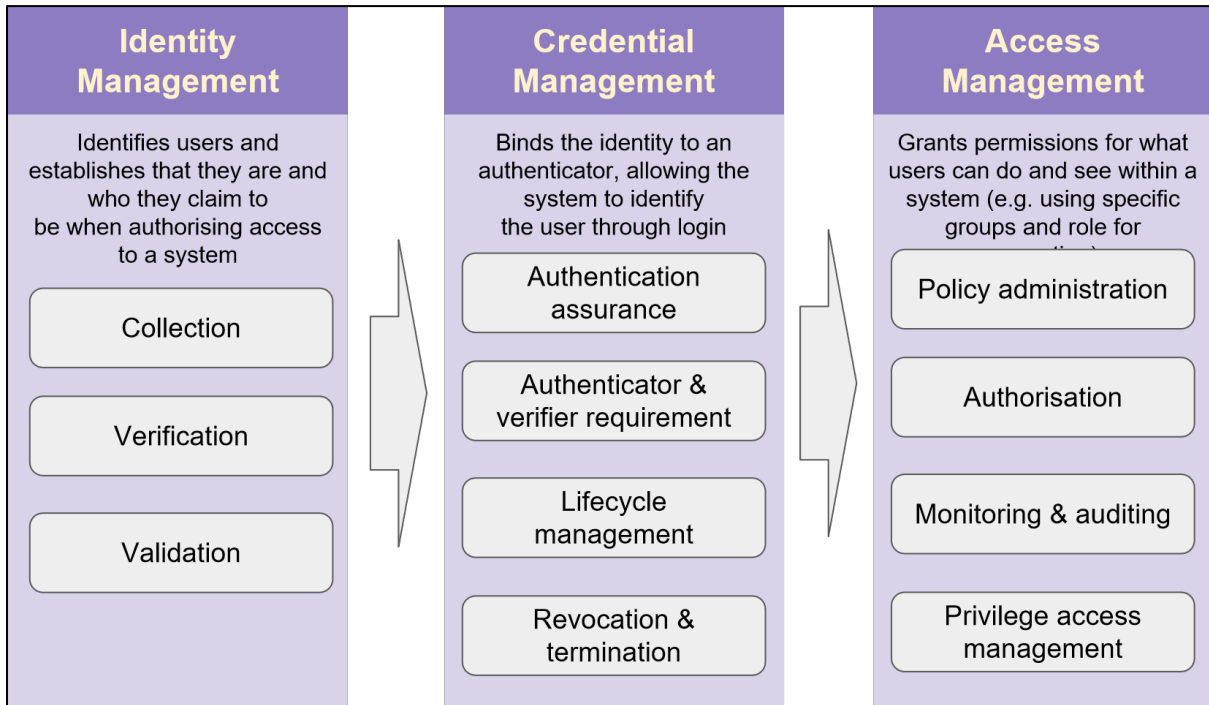


Figure 1. DISM Framework based on ICAM

8. Identity management

8.1 Overview of identity management

Identity management provides requirements for enrolment and identity proofing of users that wish to gain access to resources at each Identity Assurance Level (IAL) as follows.

- a) Collection of user identity document.
- b) Verification of the identity document at point of presentment.
- c) Validation against designated authority.

The identity document shall be presented by users to support their claim of identity. The following identity document in the Malaysian context shall be acceptable.

- a) MyKad or equivalent: with identity and biometric data recorded on and within card.
- b) Passport: for foreign nationals, in absence of above.

MCMC MTSFB TC G051:2025

- c) Approved identity document.

The identity document shall be validated by the following agencies.

- a) JPN

As issuer of MyKad and equivalents, and single authoritative source of identity information for Malaysian citizens and permanent residents.

- b) JIM

As authoritative source for foreign nationals who have undertaken legal entry into Malaysia.

- c) Others

Such as United Nations High Commissioner for Refugees (UNHCR) ID for refugees, foreign nationals not physically present in Malaysia but consuming services offered by Malaysian service providers.

Identity proofing expected outcomes are as follows.

- a) Verify that all supplied evidence is correct and genuine (e.g., not counterfeit or misappropriated).
- b) Verify that the claimed identity is associated with the real person supplying the identity evidence.
- c) Validate that the claimed identity exists to the knowledge of the authoritative source.

8.2 Identity assurance

The basic concept is that identity proofing interactions are costly, and that a RP can determine the identity assurance level commensurate with the services offered, and the associated risk appetite. To this end, the CSP shall undertake DI enrolment at one of the assurance levels enumerated below, with higher assurance denoting commensurate technological and operational stringency in the issue process.

The purpose of this document is to introduce the DI conceptual framework, as recognised by international specifications and standards, and also to update and localise the material therein. The most important of these localisations relates to the acceptability of identity documents presented by users to the CSP.

The stipulations herein are based on the universal use and acceptability of the following.

- a) MyKad, or equivalent, as issued by JPN which collects, safeguards and vouchsafes the identities of Malaysian nationals and residents.
- b) Passports, as issued by sovereign nations and jurisdictions to their nationals and dependents in real-world business cases.

Note this universality and acceptability does not exist everywhere, hence the significant complexity in NIST 800-63A pertaining to the evidentiary strength of various documents submitted for identity verification and validation. The arrangement of this section otherwise refers extensively from NIST 800-63A.

The other major departure from NIST 800-63A is in the specification of minimal requirements for DI enrolment at even the lowest level of assurance, which are as follows.

a) Identity Assurance Level 1 (IAL1)

Evidence supports the real-world existence of the claimed identity and verifies that the applicant is appropriately associated with this real-world identity. IAL1 requires either remote or physical identity proofing.

b) Identity Assurance Level 2 (IAL2)

Strong evidence supports the real-world existence of the claimed identity and verifies that the applicant is appropriately associated with this real-world identity. IAL2 requires either remote or physical identity proofing, with subsequent validation with the appropriate issuer or authoritative source. A CSP that supports IAL2 can support IAL1 enrolment per user request.

c) Identity Assurance Level 3 (IAL3)

Physical presence is required for identity proofing. Identifying attributes must be verified by an authorised CSP process. A CSP that supports IAL3 can support IAL1 and IAL2 identity attributes per user request.

The specification sequence process is illustrated in Figure 2 below.



Figure 2. Specification sequence process

8.3 Identity assurance requirements

8.3.1 Identity Assurance Level 1 (IAL1)

IAL1 allows both remote and in-person identity verification without specific requirements for validation, as detailed below.

- a) The organisation may request one or more self-asserted attributes from the applicant to support their service offering.
- b) The organisation is required to undertake best-effort identity verification commensurate with the use case risk classification and is also obliged to undertake record-keeping of suitable stringency.
- c) The organisation may choose to accept an identity document of equivalent assurance level to the specified MyKad or passport, if deemed suitable for the use case logic.
- d) An IAL2 or IAL3 CSP should support RPs that only require IAL1, if the user consents.

8.3.2 Identity Assurance Level 2 (IAL2)

IAL2 allows remote or in-person identity proofing. IAL2 supports a wide range of acceptable identity proofing techniques so as to:

- a) increase user adoption;

MCMC MTSFB TC G051:2025

- b) decrease false negatives (legitimate applicants that cannot successfully complete identity proofing); and
- c) detect to the best extent possible the presentation of fraudulent identities by a malicious applicant.

The CSP shall collect MyKad or passport or approved identity document in either physical or image form. The CSP shall verify identity document of the applicant's binding to identity evidence via a strong process.

This document intentionally omits all Knowledge-Based Verification (KBV) processes stipulated in NIST 800-63A. No KBV process shall be deemed acceptable for DI issue within the context of this document.

This document in addition limits the acceptable identity documents to either MyKad or passport or approved identity document, with further limitation to collection of name and identity number.

The CSP shall validate identity document with a process that can achieve the same strength as the evidence presented. To this end, the only authorities sufficiently authoritative for validation purposes are as following.

- a) JPM for validation of MyKad or equivalent documents.
- b) JIM for validation of passports for foreign nationals that are present in Malaysia, or previously were.
- c) Authority for other approved identity document.

The CSP shall support in-person or remote identity proofing. The CSP should offer both in-person and remote proofing. The CSP may collect biometrics for the purposes of non-repudiation and re-proofing, subject to privacy protection considerations.

8.3.3 Identity Assurance Level 3 (IAL3)

The CSP shall verify identity evidence of the applicant's binding to identity evidence via a process that is considered to be superior. Table 2 shows the requirements for IAL.

Table 2. Requirements for Identity Assurance Level (IAL)

Requirement	IAL1	IAL2	IAL3
Presence	Online or physical	Online or physical	Physical only
Evidence	Strong proof	Strong proof and commensurate validation occur	Superior proof and commensurate validation occur
Verification	Verified via process regarded as fair	Verified via process regarded as strong.	Verified via process regarded as superior.
Validation	No validation	Validated via process of equivalent stringency as the evidence presented.	Same as IAL2

8.4 Identity collection, validation and verification

8.4.1 Identity collection

Identity collection is undertaken by means of transcription from identity documents presented as evidence. Given the DI objective of supporting online use cases, this collection shall be limited to the following identity:

- a) name; and

b) identity number in context of identity document.

8.4.2 Identity verification

The goal of identity verification is to confirm and establish a linkage between the claimed identity and the physical existence of the subject presenting the evidence.

8.4.3 Identity verification methods

Table 3 below details the verification methods necessary to achieve a given identity verification strength.

Table 3. Strength level for identity verification methods

Identity verification methods	Strength
Evidence verification was not performed, or verification failed. Unable to confirm that the applicant is the owner of the claimed identity.	Unacceptable
Applicant has been confirmed as having access to the evidence provided to support the claimed identity.	Weak
Applicant ownership of the claimed identity has been confirmed by: a) physical comparison of the applicant to the identity evidence provided to support the claimed identity; or b) biometric comparison of the applicant to the identity evidence.	Fair
Applicant ownership of the claimed identity has been confirmed by biometric comparison, using appropriate technologies, of the applicant to the identity evidence provided to support the claimed identity. Biometric comparison can be performed remotely.	Strong
Applicant ownership of the claimed identity has been confirmed by biometric comparison of the applicant to the identity evidence provided to support the claimed identity, Physical biometric comparison shall be performed at the location of the user via process of equivalent stringency.	Superior

8.4.4 Validating identity evidence

Once the CSP obtains the identity evidence, the accuracy, authenticity, and integrity of the evidence and related information is checked against authoritative sources in order to determine that the presented evidence meeting the following criteria.

- a) Genuine, authentic, and not a counterfeit, fake, or forgery.
- b) Contains information that is correct.
- c) Contains information that can be validated against authoritative source.

Table 4 lists strengths, ranging from unacceptable to superior, of identity validation performed by the CSP to validate the evidence presented for the current proofing session and the information contained therein.

Table 4. Required validating strength for methods performed by CSP

No.	Method performed by the CSP	Strength
1.	Evidence validation was not performed, or validation failed	Unacceptable
2.	Evidence confirmed as valid by authoritative source.	Weak

MCMC MTSFB TC G051:2025

Table 4. Required validating strength for methods performed by CSP *(continued)*

No.	Method performed by the CSP	Strength
3.	a) Evidence confirmed as valid by authoritative source; b) Evidence confirmed as genuine using appropriate technologies, via integrity of physical security features to extent that evidence is not fraudulent or modified; or c) Evidence confirmed as genuine by cryptographic integrity and source verification.	Fair
4.	Evidence confirmed as valid by authoritative source, together with either of the following method: a) evidence confirmed as genuine using appropriate technologies, via integrity of physical security features to extent that evidence is not fraudulent or modified; or b) evidence confirmed as genuine by cryptographic integrity and source verification.	Strong
5.	a) Evidence confirmed as valid by authoritative source; b) Evidence confirmed as genuine using appropriate technologies, via integrity of physical security features to extent that evidence is not fraudulent or modified; and c) Evidence confirmed as genuine by cryptographic integrity and source verification.	Superior

8.4.5 Identity proofing requirements

8.4.5.1 In-person identity proofing

In-person proofing at IAL3 can be satisfied in either of the two following ways:

- a) physical interaction with the applicant, supervised by an operator, or by means of computerised process acknowledgement to be of superior stringency; or
- b) remote interaction with the applicant, supervised by an operator.

8.4.5.1.1 General requirement

Both computerised and operator identity proofing requires verification of live user biometric data as presented, against reference biometric data contained in the identity evidence.

8.4.5.1.2 Requirements for supervised remote in-person proofing

CSPs can employ remote proofing processes to achieve comparable levels of confidence and security to in-person events. The following requirements establish comparability between in person transactions where the applicant is in the same physical location as the CSP to those where the applicant is remote. Supervised remote identity proofing and enrolment transactions shall meet the following requirements, in addition to the IAL3 validation and verification requirements regarded to be of superior stringency.

- a) CSP shall monitor the entire identity proofing session, from which the applicant shall not depart. For example, by a continuous high-resolution video transmission of the applicant.

- b) CSP shall have a live operator participate remotely with the applicant for the entirety of the identity proofing session.
- c) CSP shall require all actions taken by the applicant during the identity proofing session to be clearly visible to the remote operator.
- d) CSP shall require that all digital verification of evidence (e.g., via chip or wireless technologies) be performed by integrated scanners and sensors.
- e) CSP shall require operators to have undergone a training program to detect potential fraud and to properly perform a supervised remote proofing session.
- f) CSP shall employ physical tamper detection and resistance features appropriate for the environment in which it is located. For example, a kiosk located in a restricted area or one where it is monitored by a trusted individual requires less tamper detection than one that is located in a semi-public area such as a shopping mall concourse.
- g) CSP shall ensure that all communications occur over a mutually authenticated protected channel.

8.5 Threats and security considerations

There are two general categories of threats to the enrolment process which are impersonation, and either compromise or malfeasance of the infrastructure provider. This clause focuses on impersonation threats, as infrastructure threats are addressed by traditional computer security controls (e.g., intrusion protection, record keeping, independent audits) and are outside the scope of this document.

Threats to the enrolment process include impersonation attacks and threats to the transport mechanisms for identity proofing, authenticator binding, and credential issuance. Table 5 below lists the threats related to enrolment and identity proofing.

Table 5. Enrolment and identity proofing threats

Activity	Threat or attack	Example
Enrolment	Falsified identity proofing evidence	Applicant claims an incorrect identity by using a forged identity document
	Fraudulent use of another’s identity	Applicant uses an identity document of a different individual.
	Enrolment repudiation	Subscriber denies enrolment, claiming that they did not enrol with the CSP.

8.5.1 Threat mitigation strategies

Enrolment threats can be deterred by making impersonation more difficult to accomplish or by increasing the likelihood of detection. This recommendation deals primarily with methods for making impersonation more difficult; however, it does prescribe certain methods and procedures that may help prove who perpetrated an impersonation. At each level, methods are employed to determine that a person with the claimed identity exists, that the applicant is the person entitled to the claimed identity, and that the applicant cannot later repudiate the enrolment. As the level of assurance increases, the methods employed provide increasing resistance to casual, systematic, and insider impersonation. Table 6 lists strategies for mitigating threats to the enrolment and issuance processes.

Table 6. Enrolment and issuance threat mitigation strategies

Activity	Threat or attack	Mitigation strategy
Enrolment	Falsified identity evidence	CSP validates physical security features of presented evidence.
		CSP validates personal details in the evidence with the issuer or other authoritative source.
	Fraudulent use of another identity	CSP verifies identity evidence and biometric of applicant against information obtained from authoritative source.
	Enrolment repudiation	CSP retains record of credential issue.

9. Credential Management

9.1 Overview of credential management

Credential management is how an organisation binds the identity to an authenticator, manages the lifecycle of the authenticator and allows the system to identify the user through authentication mechanism.

Credential management is performed by CSP. The function of CSP can be handled within the organisation or alternatively outsourced to a third-party provider.

For online services in which return visits are applicable, a successful authentication provides reasonable risk-based assurances that the subscriber accessing the service today is the same as that which accessed the service previously. The robustness of this confidence is described by an Authentication Assurance Level (AAL).

The ongoing authentication of subscribers is central to the process of associating a subscriber with their online activity. Subscriber authentication is performed by verifying that the claimant controls one or more credentials or authenticators associated with a given subscriber. A successful authentication results in the assertion of an identifier, either pseudonymous or non-pseudonymous, and optionally other identity information, to the RP.

This Technical Code provides recommendations on types of authentication processes, including choices of authenticators, that may be used at various AAL. It also provides recommendations on the lifecycle of authenticators, including revocation in the event of loss or theft.

9.2 Authentication assurance

This Technical Code applies to digital authentication of subjects to systems over a network. It does not address the authentication of a person for physical access (e.g., to a building), though some credentials used for digital access may also be used for physical access authentication. This Technical Code also requires that federal systems and service providers participating in authentication protocols be authenticated to subscribers. The strength of an authentication transaction is characterized by an ordinal measurement known as the AAL. Stronger authentication (a higher AAL) requires malicious actors to have better capabilities and expend greater resources in order to successfully subvert the authentication process. Authentication at higher AALs can effectively reduce the risk of attacks.

This Technical Code refers extensively from NIST 800-63B, but omits certain authenticator types and technologies, which are known to be problematic. This includes, for instance, One-Time Password (OTP) authentication based on possession of a phone number to which a verifier-originated secret is transmitted via Short Message Service (SMS) or alternative secondary channel. A high-level summary of the technical requirements for each of the AALs is provided below.

- a) AAL1 provides some assurance that the claimant controls an authenticator bound to the subscriber's account. AAL1 requires either single-factor or MFA using a wide range of available authentication technologies. Successful authentication requires that the claimant prove possession and control of the authenticator through a secure authentication protocol.
- b) AAL2 provides high confidence that the claimant controls authenticator(s) bound to the subscriber's account. Proof of possession and control of two distinct authentication factors is required through secure authentication protocol(s). Approved cryptographic techniques are required at AAL2 and above.
- c) AAL3 provides very high confidence that the claimant controls authenticator(s) bound to the subscriber's account. Authentication at AAL3 is based on proof of possession of a key through a cryptographic protocol. AAL3 authentication shall use a hardware-based authenticator and an authenticator that provides verifier impersonation resistance; the same device may fulfil both these requirements. In order to authenticate at AAL3, claimants shall prove possession and control of two distinct authentication factors through secure authentication protocol. Approved cryptographic techniques are required.

9.2.1 Authenticator Assurance Level 1 (AAL1)

AAL1 provides some assurance that the claimant controls an authenticator bound to the subscriber's account. AAL1 requires either single-factor or MFA using a wide range of available authentication technologies. Successful authentication requires that the claimant prove possession and control of the authenticator through a secure authentication protocol.

9.2.1.1 Permitted authenticator types

AAL1 authentication shall occur using any of the following authenticator types.

- a) Memorised secret.
- b) Out-of-band device.
- c) Single factor OTP device.
- d) Single factor cryptographic software.
- e) Single factor cryptographic device.
- f) Multi-factor cryptographic software.
- g) Multi-factor cryptographic device.

9.2.1.2 Authenticator and verifier requirements

Cryptographic authenticators used at AAL1 shall use approved cryptography. Software-based authenticators that operate within the context of an operating system may, where applicable, attempt to detect compromise (e.g., by malware) of the user endpoint in which they are running and should not complete the operation when such a compromise is detected.

Communication between the claimant and verifier (using the primary channel in the case of an out-of-band authenticator) shall be via an authenticated protected channel to provide confidentiality of the authenticator output and resistance to man-in-the-middle (MitM) attacks.

MCMC MTSFB TC G051:2025

9.2.1.3 Reauthentication

Periodic reauthentication of subscriber sessions shall be performed. At AAL1, reauthentication of the subscriber should be repeated at least once per 30 days during an extended usage session, regardless of user activity. The session should be terminated (i.e., logged out) when this time limit is reached.

9.2.1.4 Security controls

The CSP shall employ appropriately tailored security controls or industry standard. The CSP shall ensure that the minimum assurance-related controls for low impact systems, or equivalent, are satisfied.

9.2.1.5 Records retention policy

The CSP shall comply with its respective records retention policies in accordance with applicable laws, regulations, and policies. If the CSP opts to retain records in the absence of any mandatory requirements, the CSP shall conduct a risk management process, including assessments of privacy and security risks, to determine how long records should be retained and shall inform the subscriber of that retention policy.

9.2.2 Authenticator Assurance Level 2 (AAL2)

AAL2 provides high confidence that the claimant controls authenticators bound to the subscriber's account. Proof of possession and control of two distinct authentication factors is required through secure authentication protocols. Approved cryptographic techniques are required at AAL2 and above.

9.2.2.1 Permitted authenticator types

At AAL2, authentication shall occur by the use of either a multi-factor authenticator or a combination of two single-factor authenticators. A multi-factor authenticator requires two factors to execute a single authentication event, such as a cryptographically secure device with an integrated biometric sensor that is required to activate the device.

When a multi-factor authenticator is used, any of the following may be used.

- a) Multi-factor OTP device.
- b) Multi-factor cryptographic software.
- c) Multi-factor cryptographic device.

When a combination of two single-factor authenticators is used, it shall include a Memorised Secret authenticator and one possession-based (i.e., "something you have") authenticator from the following list.

- a) Look-up secret.
- b) Out-of-band device.
- c) Single-factor OTP device.
- d) Single-factor cryptographic software.
- e) Single-factor cryptographic device.

NOTE: When biometric authentication meets the requirements, the device has to be authenticated in addition to the biometric - a biometric is recognized as a factor, but not recognized as an authenticator by itself. Therefore, when conducting authentication with a biometric, it is unnecessary to use two authenticators

because the associated device serves as “something you have,” while the biometric serves as “something you are.”

9.2.2.2 Authenticator and verifier requirements

Cryptographic authenticators used at AAL2 shall use approved cryptography. Authenticators shall be validated to meet the requirements of MyCV Security Level 2 and Common Criteria Evaluation Assurance Level (EAL) 3. Software-based authenticators that operate within the context of an operating system may, where applicable, attempt to detect compromise of the platform in which they are running (e.g., by malware) and should not complete the operation when such a compromise is detected. At least one authenticator used at AAL2 shall be replay resistant. Authentication at AAL2 should demonstrate authentication intent from at least one authenticator. Communication between the claimant and verifier (the primary channel in the case of an out-of band authenticator) shall be via an authenticated protected channel to provide confidentiality of the authenticator output and resistance to MitM attacks. Verifiers operated at AAL2 shall be validated to meet the requirements of MyCV Security Level 2 and Common Criteria EAL3.

When a device such as a smartphone is used in the authentication process, the unlocking of that device (typically done using a PIN or biometric) shall not be considered one of the authentication factors. Generally, it is not possible for a verifier to know that the device had been locked or if the unlock process met the requirements for the relevant authenticator type. When a biometric factor is used in authentication at AAL2, the performance requirements stated in Clause 6.5.2.3 shall be met, and the verifier should make a determination that the biometric sensor and subsequent processing meet these requirements.

9.2.2.3 Reauthentication

Periodic reauthentication of subscriber sessions shall be performed. At AAL2, authentication of the subscriber shall be repeated at least once per 12 hours during an extended usage session, regardless of user activity. Reauthentication of the subscriber shall be repeated following any period of inactivity lasting 30 minutes or longer. The session shall be terminated (i.e., logged out) when either of these time limits is reached. Reauthentication of a session that has not yet reached its time limit may require only a memorised secret or a biometric in conjunction with the still-valid session secret. The verifier may prompt the user to cause activity just before the inactivity timeout.

9.2.2.4 Security controls

The CSP shall employ appropriately tailored security controls or industry standard. The CSP shall ensure that the minimum assurance-related controls for moderate impact systems or equivalent are satisfied.

9.2.2.5 Records retention policy

The CSP shall comply with its respective records retention policies in accordance with applicable laws, regulations, and policies. If the CSP opts to retain records in the absence of any mandatory requirements, the CSP shall conduct a risk management process, including assessments of privacy and security risks to determine how long records should be retained and shall inform the subscriber of that retention policy.

9.2.3 Authenticator Assurance Level 3 (AAL3)

AAL3 provides very high confidence that the claimant controls authenticator(s) bound to the subscriber’s account. Authentication at AAL3 is based on proof of possession of a key through a cryptographic protocol. AAL3 authentication shall use a hardware-based authenticator and an authenticator that provides verifier impersonation resistance - the same device may fulfil both these requirements. In order to authenticate at AAL3, claimants shall prove possession and control of two distinct authentication factors through secure authentication protocol(s). Approved cryptographic techniques are required.

MCMC MTSFB TC G051:2025

9.2.3.1 Permitted authenticator types

AAL3 authentication shall occur by the use of one of a combination of authenticators. Possible combinations are as follows.

- a) Multi-factor cryptographic device.
- b) Single-factor cryptographic device used in conjunction with memorised secret.
- c) Multi-factor OTP device (software or hardware) used in conjunction with a single-factor cryptographic device.
- d) Multi-factor OTP device (hardware only) used in conjunction with a single-factor cryptographic software.
- e) Single-factor OTP device (hardware only) used in conjunction with a multi-factor cryptographic software authenticator.
- f) Single-factor OTP device (hardware only) used in conjunction with a single-factor cryptographic software authenticator.

9.2.3.2 Authenticator and verifier requirements

Communication between the claimant and verifier shall be via an authenticated protected channel to provide confidentiality of the authenticator output and resistance to MitM attacks. At least one cryptographic device authenticator used at AAL3 shall be verifier impersonation resistant and shall be replay resistant. All authentication and reauthentication processes at AAL3 shall demonstrate authentication intent from at least one authenticator. Authenticators used at AAL3 shall be cryptographic modules validated at MyCV Security Level 3 or higher and Common Criteria EAL4. Verifiers at AAL3 shall be validated at MyCV Security Level 3 or higher and Common Criteria EAL4. Verifiers at AAL3 shall be verifier compromise resistant with respect to at least one authentication factor. The Security Level represents the assurance level of MyCV certification for cryptography module that is based on criteria defined in the ISO/IEC 19790 Security requirements for cryptographic modules standard.

Hardware-based authenticators and verifiers at AAL3 should resist relevant side-channel (e.g., timing and power-consumption analysis) attacks. Relevant side-channel attacks shall be determined by a risk assessment performed by the CSP. When a device such as a smartphone is used in the authentication process, presuming that the device is able to meet the requirements above, then the unlocking of that device shall not be considered to satisfy one of the authentication factors. This is because it is generally not possible for verifier to know that the device had been locked nor whether the unlock process met the requirements for the relevant authenticator type.

When a biometric factor is used in authentication at AAL3, the verifier shall make a determination that the biometric sensor and subsequent processing meet the performance requirements stated in Clause 9.5.2.3.

9.2.3.3 Reauthentication

Periodic reauthentication of subscriber sessions shall be performed. At AAL3, authentication of the subscriber shall be repeated at least once per 12 hours during an extended usage session, regardless of user activity. Reauthentication of the subscriber shall be repeated following any period of inactivity lasting 15 minutes or longer. Reauthentication shall use both authentication factors. The session shall be terminated (i.e., logged out) when either of these time limits is reached. The verifier may prompt the user to cause activity just before the inactivity timeout.

9.2.3.4 Security controls

The CSP shall employ appropriately tailored security controls or industry standard. The CSP shall ensure that the minimum assurance-related controls for high impact systems or equivalent are satisfied.

9.2.3.5 Records retention policy

The CSP shall comply with its respective records retention policies in accordance with applicable laws, regulations, and policies. If the CSP opts to retain records in the absence of any mandatory requirements, the CSP shall conduct a risk management process, including assessments of privacy and security risks, to determine how long records should be retained and shall inform the subscriber of that retention policy.

9.3 Privacy requirements

If CSPs process attributes for purposes other than identity proofing, authentication, or attribute assertion (collectively “identity service”), related fraud mitigation, or to comply with law or legal process, CSPs shall implement measures to maintain predictability and manageability commensurate with the privacy risk arising from the additional processing and compliance to Personal Data Protection Act. Measures may include providing clear notice, obtaining subscriber consent, or enabling selective use or disclosure of attributes. When CSPs use consent measures, CSPs shall not make consent for the additional processing a condition of the identity service.

9.4 Summary of requirements

Table 7 below summarises requirements for each AAL.

Table 7. Summary of requirement for Authentication Assurance Level (AAL)

Requirement	AAL1	AAL2	AAL3
Permitted authenticator types	a) Memorised Secret b) Out-of-Band c) SF OTP Device d) MF OTP Device e) SF Crypto Software f) SF Crypto Device g) MF Crypto Software h) MF Crypto Device	a) MF OTP Device b) MF Crypto Software c) MF Crypto Device d) Memorised Secret plus: i) Look-Up Secret ii) Out-of-Band iii) SF OTP Device iv) SF Crypto Software v) SF Crypto Device	a) MF Crypto Device; b) SF Crypto Device plus Memorised Secret; c) SF OTP Device plus MF Crypto Device or Software; d) SF OTP Device plus SF Crypto Software plus Memorised Secret
Minimum security strength of secret key and its algorithm	112-bit	128-bit for MyCV Security Level 2	192-bit for MyCV Security Level 3 or 256-bit for MyCV Security Level 4
MyCV & common criteria certification	Not required	MyCV Security Level 2 & Common Criteria EAL3	MyCV Security Level 3 or 4 & Common Criteria EAL4
Reauthentication	30 days	12 hours or 30 minutes inactivity; may use one authentication factor	12 hours or 15 minutes inactivity shall use both authentication factors

Table 7. Summary of requirement for Authentication Assurance Level (AAL) (continued)

Requirement	AAL1	AAL2	AAL3
MitM resistance	Required	Required	Required
Verifier impersonation resistance	Not required	Not required	Required
Verifier compromise resistance	Not required	Not required	Required
Replay resistance	Not required	Not required	Required
Authentication Intent	Not required	Recommended	Required
Records retention policy	Required	Required	Required
Privacy controls	Required	Required	Required

9.5 Authenticator and verifier requirements

This clause provides the detailed requirements specific to each type of authenticator. With the exception of reauthentication requirements specified in Clause 9.4 and the requirement for verifier impersonation resistance at AAL3 described in Clause 9.5.2.5, the technical requirements for each of the authenticator types are the same regardless of the AAL at which the authenticator is used.

9.5.1 Requirements by authenticator type

9.5.1.1 Memorised secrets

A Memorised Secret authenticator - commonly referred to as a password or, if numeric, a PIN - is a secret value intended to be chosen and memorised by the user. Memorised secrets need to be of sufficient complexity and secrecy that it would be impractical for an attacker to guess or otherwise discover the correct secret value. A memorised secret is “something you know”.

9.5.1.1.1 Memorised secret authenticators

Memorised secrets shall be at least 8 characters in length if chosen by the subscriber. Memorised secrets chosen randomly by the CSP, or verifier shall be at least 6 characters in length and may be entirely numeric. If the CSP or verifier disallows a chosen memorised secret based on its appearance on a blacklist of compromised values, the subscriber shall be required to choose a different memorised secret. No other complexity requirements for memorised secrets should be imposed.

9.5.1.2 Out-of-band devices

An out-of-band authenticator is a physical device that is uniquely addressable and can communicate securely with the verifier over a distinct communications channel, referred to as the secondary channel. The device is possessed and controlled by the claimant and supports private communication over this secondary channel, separate from the primary channel for e-authentication. An out-of-band authenticator is something you have.

The out-of-band authenticator can operate in one of the following ways.

- a) The claimant transfers a secret received by the out-of-band device via the secondary channel to the verifier using the primary channel. For example, the claimant may receive the secret on their mobile device and type it (typically a 6-digit code) into their authentication session.
- b) The claimant transfers a secret received via the primary channel to the out-of-band device for transmission to the verifier via the secondary channel. For example, the claimant may view the secret on their authentication session and either type it into an app on their mobile device or use a technology such as a barcode or QR code to affect the transfer.
- c) The claimant compares secrets received from the primary channel and the secondary channel and confirms the authentication via the secondary channel.

The secret's purpose is to securely bind the authentication operation on the primary and secondary channel. When the response is via the primary communication channel, the secret also establishes the claimant's control of the out-of-band device.

This document expressly prohibits authentication by means of secrets initially generated verifier-side, transmitted to the authenticator-side via the secondary channel, and then replayed into the primary channel. Authentication secrets used by such devices should originate within the authenticator itself.

9.5.1.2.1 Out-of-band authenticators

The out-of-band authenticator shall establish a separate channel with the verifier in order to retrieve the out-of-band secret or authentication request. This channel is considered to be out-of band with respect to the primary communication channel (even if it terminates on the same device) provided the device does not leak information from one channel to the other without the authorisation of the claimant. The out-of-band device should be uniquely addressable and communication over the secondary channel shall be encrypted. Methods that do not prove possession of a specific device, such as Voice-Over-IP (VOIP) or email, shall not be used for out-of-band authentication. The out-of-band authenticator shall uniquely authenticate itself in one of the following ways when communicating with the verifier.

- a) Establish an authenticated protected channel to the verifier using approved cryptography. The key used shall be stored in suitably secure storage available to the authenticator application (e.g., keychain storage, Trusted Platform Module (TPM), Trusted Execution Environment (TEE), secure element).
- b) Authenticate to a public mobile telephone network using a Subscriber Identity Module (SIM) card or equivalent that uniquely identifies the device. This method shall only be used if a secret is being sent from the verifier to the out-of-band device via the Public Switched Telephone Network (PSTN) (SMS or voice).

If a secret is sent by the verifier to the out-of-band device, the device should not display the authentication secret while it is locked by the owner (i.e., requires an entry of a PIN, passcode, or biometric to view). However, authenticators should indicate the receipt of an authentication secret on a locked device. If the out-of-band authenticator sends an approval message over the secondary communication channel rather than by the claimant transferring a received secret to the primary communication channel, it shall do one of the following.

- a) The authenticator shall accept transfer of the secret from the primary channel which it shall send to the verifier over the secondary channel to associate the approval with the authentication transaction. The claimant may perform the transfer manually or use a technology such as a barcode or QR code to affect the transfer.

MCMC MTSFB TC G051:2025

- b) The authenticator shall present a secret received via the secondary channel from the verifier and prompt the claimant to verify the consistency of that secret with the primary channel, prior to accepting a yes or no response from the claimant. It shall then send that response to the verifier.

This document expressly prohibits authentication by means of secrets initially generated verifier-side, transmitted to the authenticator-side via the secondary channel, and then replayed into the primary channel. Authentication secrets used by such devices should originate within the authenticator itself.

9.5.1.3 Single-factor OTP device

A single-factor OTP device generates OTPs. This category includes hardware devices and software-based OTP generators installed on devices such as mobile phones. These devices have an embedded secret that is used as the seed for generation of OTPs and does not require activation through a second factor. The OTP is displayed on the device and manually input for transmission to the verifier, thereby proving possession and control of the device. An OTP device may, for example, display 6 characters at a time. A single-factor OTP device is something you have.

Single-factor OTP devices are similar to look-up secret authenticators with the exception that the secrets are cryptographically and independently generated by the authenticator and verifier and compared by the verifier. The secret is computed based on a nonce that may be time-based or from a counter on the authenticator and verifier.

9.5.1.3.1 Single-factor OTP authenticators

Single-factor OTP authenticators contain two persistent values. The first is a symmetric key that persists for the device's lifetime. The second is a nonce that is either changed each time the authenticator is used or is based on a real-time clock.

The secret key and its algorithm shall provide at least the minimum-security strength as specified in Clause 6.4.5. The nonce shall be of sufficient length to ensure that it is unique for each operation of the device over its lifetime. OTP authenticators, particularly software-based OTP generators should discourage and shall not facilitate the cloning of the secret key onto multiple devices.

The authenticator output is obtained by using an approved block cipher or hash function to combine the key and nonce in a secure manner. The authenticator output may be truncated to as few as 6 decimal digits (approximately 20 bits of entropy).

If the nonce used to generate the authenticator output is based on a real-time clock, the nonce shall be changed at least once every 2 minutes. The OTP value associated with a given nonce shall be accepted only once.

9.5.1.4 Single-factor cryptographic software

A single-factor software cryptographic authenticator is a cryptographic key stored on disk or some other "soft" media. Authentication is accomplished by proving possession and control of the key. The authenticator output is highly dependent on the specific cryptographic protocol, but it is generally some type of signed message. The single-factor software cryptographic authenticator is "something you have".

9.5.1.4.1 Single-factor cryptographic software authenticators

Single-factor software cryptographic authenticators encapsulate one or more secret keys unique to the authenticator. The key shall be stored in suitably secure storage available to the authenticator application (e.g., keychain storage, TPM, or TEE if available). The key shall be strongly protected against unauthorised disclosure by the use of access controls that limit access to the key to only those software components on the device requiring access. Single-factor cryptographic software

authenticators should discourage and shall not facilitate the cloning of the secret key onto multiple devices.

9.5.1.5 Single-factor cryptographic devices

A single-factor cryptographic device is a hardware device that performs cryptographic operations using protected cryptographic key(s) and provides the authenticator output via direct connection to the user endpoint. The device uses embedded symmetric or asymmetric cryptographic keys and does not require activation through a second factor of authentication. Authentication is accomplished by proving possession of the device via the authentication protocol. The authenticator output is provided by direct connection to the user endpoint and is highly dependent on the specific cryptographic device and protocol, but it is typically some type of signed message. A single-factor cryptographic device is something you have.

9.5.1.5.1 Single-factor cryptographic device authenticator

Single-factor cryptographic device authenticators encapsulate one or more secret keys unique to the device that shall not be exportable (i.e., cannot be removed from the device). The authenticator operates by signing a challenge nonce presented through a direct computer interface (e.g., a Universal Serial Bus (USB) port). Alternatively, the authenticator could be a suitably secure processor integrated with the user endpoint itself (e.g., a hardware TPM). Although cryptographic devices contain software, they differ from cryptographic software authenticators in that all embedded software is under control of the CSP, or issuer and that the entire authenticator is subject to all applicable MyCV requirements at the AAL being authenticated.

The secret key and its algorithm shall provide at least the minimum-security length as specified in Clause 9.4 of this Technical Code. The challenge nonce shall be at least 64 bits in length. Approved cryptography shall be used.

Single-factor cryptographic device authenticators should require a physical input (e.g., the pressing of a button) in order to operate. This provides defence against unintended operation of the device, which might occur if the endpoint to which it is connected is compromised.

9.5.1.6 Multi-factor cryptographic software

A multi-factor software cryptographic authenticator is a cryptographic key stored on disk or some other "soft" media that requires activation through a second factor of authentication. Authentication is accomplished by proving possession and control of the key. The authenticator output is highly dependent on the specific cryptographic protocol, but it is generally some type of signed message. The multi-factor software cryptographic authenticator is something you have, and it shall be activated by either something you know or something you are.

9.5.1.6.1 Multi-factor cryptographic software authenticators

Multi-factor software cryptographic authenticators encapsulate one or more secret keys unique to the authenticator and accessible only through the input of an additional factor, either a memorised secret or a biometric. The key should be stored in suitably secure storage available to the authenticator application (e.g., keychain storage, TPM, TEE). The key shall be strongly protected against unauthorised disclosure by the use of access controls that limit access to the key to only those software components on the device requiring access. Multi-factor cryptographic software authenticators should discourage and shall not facilitate the cloning of the secret key onto multiple devices. Each authentication operation using the authenticator shall require the input of both factors.

The unencrypted key and activation secret or biometric sample and any biometric data derived from the biometric sample such as a probe produced through signal processing shall be zeroised immediately after an authentication transaction has taken place.

MCMC MTSFB TC G051:2025

9.5.1.7 Multi-factor cryptographic devices

A multi-factor cryptographic device is a hardware device that performs cryptographic operations using one or more protected cryptographic keys and requires activation through a second authentication factor. Authentication is accomplished by proving possession of the device and control of the key. The authenticator output is provided by direct connection to the user endpoint and is highly dependent on the specific cryptographic device and protocol, but it is typically some type of signed message. The multi-factor cryptographic device is something you have, and it shall be activated by either something you know or something you are.

9.5.1.7.1 Multi-factor cryptographic device authenticators

Multi-factor cryptographic device authenticators use tamper-resistant hardware to encapsulate one or more secret keys unique to the authenticator and accessible only through the input of an additional factor, either a memorised secret or a biometric. The authenticator operates by using a private key that was unlocked by the additional factor to sign a challenge nonce presented through a direct computer interface (e.g., a USB port). Alternatively, the authenticator could be a suitably secure processor integrated with the user endpoint itself (e.g., a hardware TPM). Although cryptographic devices contain software, they differ from cryptographic software authenticators in that all embedded software is under control of the CSP or issuer, and that the entire authenticator is subject to any applicable MyCV and Common Criteria requirements at the selected AAL.

The secret key and its algorithm shall provide at least the minimum-security length specified in Clause 9.4 of this Technical Code. The challenge nonce shall be at least 64 bits in length. Approved cryptography shall be used.

Each authentication operation using the authenticator should require the input of the additional factor. Input of the additional factor may be accomplished via either direct input on the device or via a hardware connection (e.g., USB, smartcard).

The unencrypted key and activation secret or biometric sample and any biometric data derived from the biometric sample such as a probe produced through signal processing shall be zeroised immediately after an authentication transaction has taken place.

9.5.2 General authenticator requirements

The following subclause describe general requirements for authenticators.

9.5.2.1 Physical authenticators

CSPs shall provide subscriber instructions on how to appropriately protect the authenticator against theft or loss. The CSP shall provide a mechanism to revoke or suspend the authenticator immediately upon notification from subscriber that loss or theft of the authenticator is suspected.

9.5.2.2 Rate limiting (throttling)

When required by the authenticator type descriptions in Clause 6.5.1 of this Technical Code, the verifier shall implement controls to protect against online guessing attacks. Unless otherwise specified in the description of a given authenticator, the verifier shall limit consecutive failed authentication attempts on a single account to no more than 100.

9.5.2.3 Use of biometrics

The use of biometrics (something you are) in authentication includes both measurement of physical characteristics (e.g., fingerprint, iris, facial characteristics) and behavioural characteristics (e.g., typing cadence). Both classes are considered biometric modalities, although different modalities may differ in the extent to which they establish authentication intent as described in Clause 6.5.2.9 of this Technical Code.

For a variety of reasons, this document supports only limited use of biometrics for authentication. These reasons include the following.

- a) The biometric False Match Rate (FMR) does not provide confidence in the authentication of the subscriber by itself. In addition, FMR does not account for spoofing attacks.
- b) Biometric comparison is probabilistic, whereas the other authentication factors are deterministic.
- c) Biometric template protection schemes provide a method for revoking biometric credentials that is comparable to other authentication factors (e.g., Public Key Infrastructure (PKI) certificates and passwords). However, the availability of such solutions is limited, and standards for testing these methods are under development.
- d) Biometric characteristics do not constitute secrets. They can be obtained online or by taking a picture of someone with a camera phone (e.g., facial images) with or without their knowledge, lifted from objects someone touches (e.g., latent fingerprints), or captured with high resolution images (e.g., iris patterns). While Presentation Attack Detection (PAD) technologies (e.g., liveness detection) can mitigate the risk of these types of attacks, additional trust in the sensor or biometric processing is required to ensure that PAD is operating in accordance with the needs of the CSP and the subscriber.

Therefore, the limited use of biometrics for authentication is supported with the following requirements and guidelines.

- a) Biometrics shall be used only as part of MFA with a physical authenticator (something you have).
- b) An authenticated protected channel between sensor (or an endpoint containing a sensor that resists sensor replacement) and verifier shall be established, and the sensor or endpoint shall be authenticated prior to capturing the biometric sample from the claimant.
- c) Based on ISO/IEC 2382-37, the biometric system shall operate with an FMR of 1 in 1000 or better. This FMR shall be achieved under conditions of a conformant attack (i.e., zero-effort impostor attempt) as defined in ISO/IEC 30107-1.
- d) The biometric system should implement PAD. Testing of the biometric system to be deployed should demonstrate at least 90 % resistance to presentation attacks for each relevant attack type (i.e., species), where resistance is defined as the number of thwarted presentation attacks divided by the number of trial presentation attacks. Testing of presentation attack resistance shall be in accordance with Section 12 of ISO/IEC 30107-3. The PAD decision may be made either locally on the claimant's device or by a central verifier.

MCMC MTSFB TC G051:2025

The biometric system shall allow no more than 5 consecutive failed authentication attempts or 10 consecutive failed attempts if PAD meeting the above requirements is implemented. Once that limit has been reached, the biometric authenticator shall either do the following.

- a) Impose a delay of at least 30 seconds before the next attempt, increasing exponentially with each successive attempt (e.g., 1 minute before the following failed attempt, 2 minutes before the second following attempt).
- b) Disable the biometric user authentication and offer another factor (e.g., a different biometric modality, a PIN or passcode if it is not already a required factor) if such an alternative method is already available.

The verifier shall make a determination of sensor and endpoint performance, integrity, and authenticity. Acceptable methods for making this determination include but are not limited to the following.

- a) Authentication of the sensor or endpoint.
- b) Certification by an approved accreditation authority.
- c) Runtime interrogation of signed metadata (e.g., attestation).

Biometric comparison can be performed locally on claimant's device or at a central verifier. Since the potential for attacks on a larger scale is greater at central verifiers, local comparison is preferred. If comparison is performed centrally, the following action is needed.

- a) Use of the biometric as an authentication factor shall be limited to one or more specific devices that are identified using approved cryptography. Since the biometric has not yet unlocked the main authentication key, a separate key shall be used for identifying the device.
- b) Biometric revocation, referred to as biometric template protection in ISO/IEC 24745, shall be implemented.
- c) All transmission of biometrics shall be over the authenticated protected channel.

Biometric samples collected in the authentication process may be used to train comparison algorithms or with user consent for other research purposes. Biometric samples and any biometric data derived from the biometric sample such as a probe produced through signal processing shall be zeroized immediately after any training or research data has been derived.

9.6 Authenticator lifecycle management

A number of events can occur over the lifecycle of a subscriber's authenticator that affect that authenticator's use. These events include binding, loss, theft, unauthorised duplication, expiration, and revocation. This clause describes the actions to be taken in response to those events.

9.6.1 Authenticator binding

Authenticator binding refers to the establishment of an association between a specific authenticator and a subscriber's account, enabling the authenticator to be used possibly in conjunction with other authenticators to authenticate for that account.

Authenticators shall be bound to subscriber accounts by either:

- a) issuance by the CSP as part of enrolment; or
- b) associating a subscriber-provided authenticator that is acceptable to the CSP.

In the context of this Technical Code, these guidelines refer to the binding rather than the issuance of an authenticator as to accommodate both options.

Throughout the digital identity lifecycle, CSPs shall maintain a record of all authenticators that are or have been associated with each identity. The CSP shall also verify the type of user-provided authenticator (e.g., single-factor cryptographic device vs. multi-factor cryptographic device) so verifiers can determine compliance with requirements at each AAL.

The record created by the CSP shall contain the date and time the authenticator was bound to the account. The record should include information about the source of the binding (e.g., IP address, device identifier) of any device associated with the enrolment. If available, the record should also contain information about the source of unsuccessful authentications attempted with the authenticator.

When any new authenticator is bound to a subscriber account, the CSP shall ensure that the binding protocol and the protocol for provisioning the associated key(s) are done at a level of security commensurate with the AAL at which the authenticator will be used. For example, protocols for key provisioning shall use authenticated protected channels or be performed in person to protect against man-in-the-middle attacks. Binding of multi-factor authenticators shall require MFA or equivalent (e.g., association with the session in which identity proofing has been just completed) be used in order to bind the authenticator. The same conditions apply when a key pair is generated by the authenticator and the public key is sent to the CSP.

9.6.1.1 Binding at enrolment

The following requirements apply when an authenticator is bound to an identity as a result of a successful identity proofing transaction.

The CSP shall bind at least one, and should bind at least two, physical (something you have) authenticators to the subscriber's online identity, in addition to a memorised secret or one or more biometrics. Binding of multiple authenticators is preferred in order to recover from the loss or theft of the subscriber's primary authenticator.

At IAL2 and above, identifying information is associated with the digital identity and the subscriber has undergone an identity proofing process. As a result, authenticators at the same AAL as the desired IAL shall be bound to the account.

If enrolment and binding cannot be completed in a single physical encounter or electronic transaction (i.e., within a single protected session), the following methods shall be used to ensure that the same party acts as the applicant throughout the processes.

- a) For remote transactions
 - i) The applicant shall identify themselves in each new binding transaction by presenting a temporary secret which was either established during a prior transaction, or sent to the applicant's phone number, email address, or postal address of record.
 - ii) Long-term authenticator secrets shall only be issued to the applicant within a protected session.

MCMC MTSFB TC G051:2025

b) For in-person transactions

- i) The applicant shall identify themselves in person by use of a biometric information from authoritative sources, such as JPN or JIM.
- ii) If the CSP issues long-term authenticator secrets during a physical transaction, then they shall be loaded locally onto a physical device that is issued in person to the applicant or delivered in a manner that confirms the address of record.

9.6.1.2 Post-enrolment binding

The following subclause describe the binding of an authenticator to a subscriber's account.

9.6.1.2.1 Binding of an additional authenticator at existing AAL

CSPs should permit the binding of additional authenticators to a subscriber's account. Before adding the new authenticator, the CSP shall first require the subscriber to authenticate at the AAL (or a higher AAL) at which the new authenticator will be used. When an authenticator is added, the CSP should send a notification to the subscriber via a mechanism that is independent of the transaction binding the new authenticator (e.g., email to an address previously associated with the subscriber). The CSP may limit the number of authenticators that may be bound in this manner.

9.6.1.2.2 Adding an additional factor to a single-factor account

If the subscriber's account has only one authentication factor bound to it (i.e., at IAL1 or AAL1) and an additional authenticator of a different authentication factor is to be added, the subscriber MAY request that the account be upgraded to AAL2. The IAL would remain at IAL1. Before binding the new authenticator, the CSP shall require the subscriber to authenticate at AAL1. The CSP should send a notification of the event to the subscriber via a mechanism independent of the transaction binding the new authenticator (e.g., email to an address previously associated with the subscriber).

9.6.1.2.3 Replacement of a lost authentication factor

If a subscriber loses all authenticators of a factor necessary to complete MFA and has been identity proofed at IAL2 or IAL3, that subscriber shall repeat the identity proofing process. An abbreviated proofing process, confirming the binding of the claimant to previously supplied evidence, may be used if the CSP has retained the evidence from the original proofing process pursuant to a privacy risk assessment. The CSP shall require the claimant to authenticate using an authenticator of the remaining factor, if any, to confirm binding to the existing identity. Reestablishment of authentication factors at IAL3 shall be done in person and shall verify the biometric against authoritative sources such as JPN or JIM.

The CSP should send a notification of the event to the subscriber. This may be the same notice as is required as part of the proofing process.

9.6.1.3 Binding to a subscriber-provided authenticator

A subscriber may already possess authenticators suitable for authentication at a particular AAL. For example, they may have a two-factor authenticator from a social network provider, considered AAL2 and IAL1, and would like to use those credentials at an RP that requires IAL2.

CSPs should, where practical, accommodate the use of subscriber-provided authenticators in order to relieve the burden to the subscriber of managing a large number of authenticators. Binding of these authenticators shall be done as described in Clause 9.6.1.2.1 of this Technical Code. In situations where the authenticator strength is not self-evident (e.g., between single-factor and multi-factor authenticators of a given type), the CSP should assume the use of the weaker authenticator unless it is able to

establish that the stronger authenticator is in fact being used (e.g., by verification with the issuer or manufacturer of the authenticator).

9.6.1.4 Renewal

The CSP should bind an updated authenticator an appropriate amount of time before an existing authenticator's expiration. The process for this should conform closely to the initial authenticator binding process (e.g., confirming address of record). Following successful use of the new authenticator, the CSP may revoke the authenticator that it is replacing.

9.6.2 Loss, theft, damage, and unauthorised duplication

Compromised authenticators include those that have been lost, stolen, or subject to unauthorised duplication. Generally, one must assume that a lost authenticator has been stolen or compromised by someone that is not the legitimate subscriber of the authenticator. Damaged or malfunctioning authenticators are also considered compromised to guard against any possibility of extraction of the authenticator secret. One notable exception is a memorised secret that has been forgotten without other indications of having been compromised, such as having been obtained by an attacker.

Suspension, revocation, or destruction of compromised authenticators should occur as promptly as practical following detection. Agencies should establish time limits for this process.

To facilitate secure reporting of the loss, theft, or damage to an authenticator, the CSP should provide the subscriber with a method of authenticating to the CSP using a backup or alternate authenticator. This backup authenticator shall be either a memorised secret or a physical authenticator. Either may be used, but only one authentication factor is required to make this report. Alternatively, the subscriber may establish an authenticated protected channel to the CSP and verify information collected during the proofing process. The CSP may choose to verify an address of record (i.e., email, telephone, postal) and suspend authenticator(s) reported to have been compromised. The suspension shall be reversible if the subscriber successfully authenticates to the CSP using a valid (i.e., not suspended) authenticator and requests reactivation of an authenticator suspended in this manner. The CSP may set a time limit after which a suspended authenticator can no longer be reactivated.

9.6.3 Expiration

CSPs may issue authenticators that expire. If and when an authenticator expires, it shall not be usable for authentication. When an authentication is attempted using an expired authenticator, the CSP should give an indication to the subscriber that the authentication failure is due to expiration rather than some other cause.

The CSP shall require subscribers to surrender or prove destruction of any physical authenticator containing attribute certificates signed by the CSP as soon as practical after expiration or receipt of a renewed authenticator.

9.6.4 Revocation and termination

Revocation of an authenticator sometimes referred to as termination, especially in the context of authenticators, refers to removal of the binding between an authenticator and a credential the CSP maintains.

CSPs shall revoke the binding of authenticators promptly when an online identity ceases to exist (e.g., subscriber's death, discovery of a fraudulent subscriber), when requested by the subscriber, or when the CSP determines that the subscriber no longer meets its eligibility requirements.

The CSP shall require subscribers to surrender or certify destruction of any physical authenticator containing certified attributes signed by the CSP as soon as practical after revocation or termination

MCMC MTSFB TC G051:2025

takes place. This is necessary to block the use of the authenticator's certified attributes in offline situations between revocation or termination and expiration of the certification.

9.7 Threat and security considerations

9.7.1 Authenticator threats

An attacker who can gain control of an authenticator will often be able to masquerade as the authenticator's owner. Threats to authenticators can be categorized based on attacks on the types of authentication factors that comprise the authenticator.

- a) Something may be disclosed to an attacker. The attacker might guess a memorised secret. Where the authenticator is a shared secret, the attacker could gain access to the CSP or verifier and obtain the secret value or perform a dictionary attack on a hash of that value. An attacker may observe the entry of a PIN or passcode, find a written record or journal entry of a PIN or passcode, or may install malicious software (e.g., a keyboard logger) to capture the secret. Additionally, an attacker may determine the secret through offline attacks on a password database maintained by the verifier.
- b) Something be lost, damaged, stolen from the owner, or cloned by an attacker. For example, an attacker who gains access to the owner's computer might copy a software authenticator. A hardware authenticator might be stolen, tampered with, or duplicated. Out-of-band secrets may be intercepted by an attacker and used to authenticate their own session.
- c) Something may be replicated. For example, an attacker may obtain a copy of the subscriber's fingerprint and construct a replica.

This Technical Code assumes that the subscriber is not colluding with an attacker who is attempting to falsely authenticate to the verifier. With this assumption in mind, the threats to the authenticator(s) used for digital authentication are listed in Table 8, along with some examples.

Table 8. Authenticator threats used for digital authentication

Authenticator threat/attack	Description	Example
Assertion manufacture or modification	The attacker generates a false assertion	Compromised CSP asserts identity of a claimant who has not properly authenticated
	The attacker modifies an existing assertion	Compromised proxy that changes AAL of an authentication assertion
Theft	A physical authenticator is stolen by an Attacker.	A hardware cryptographic device is stolen.
		An OTP device is stolen.
		A look-up secret authenticator is stolen.
		A cell phone is stolen.
Duplication	The subscriber's authenticator has been copied with or without their knowledge.	Passwords written on paper are disclosed.
		Passwords stored in an electronic file are copied.
		Software PKI authenticator (private key) copied.
		Look-up secret authenticator copied.
		Counterfeit biometric authenticator manufactured.

Table 8. Authenticator threats used for digital authentication *(continued)*

Eavesdropping	The authenticator secret or authenticator output is revealed to the attacker as the subscriber is authenticating.	Memorised secrets are obtained by watching keyboard entry.
		Memorised secrets or authenticator outputs are intercepted by keystroke logging software.
		A PIN is captured from a PIN pad device.
		A hashed password is obtained and used by an attacker for another authentication (pass-the hash attack).
	An out-of-band secret is intercepted by the attacker by compromising the communication channel.	An out-of-band secret is transmitted via unencrypted Wi Fi and received by the attacker.
Offline cracking	The authenticator is exposed using analytical methods outside the authentication mechanism.	A software PKI authenticator is subjected to dictionary attack to identify the correct password to use to decrypt the private key.
Side channel attack	The authenticator secret is exposed using physical characteristics of the authenticator.	A key is extracted by differential power analysis on a hardware cryptographic authenticator.
		A cryptographic authenticator secret is extracted by analysis of the response time of the authenticator over a number of attempts.
Phishing or pharming	The authenticator output is captured by fooling the subscriber into thinking the attacker is a verifier or RP.	A password is revealed by subscriber to a website impersonating the verifier.
		A memorised secret is revealed by a bank subscriber in response to an email inquiry from a phisher pretending to represent the bank.
		A memorised secret is revealed by the subscriber at a bogus verifier website reached through DNS spoofing.
Social engineering	The attacker establishes a level of trust with a subscriber in order to convince the subscriber to reveal their authenticator secret or authenticator output.	A memorised secret is revealed by the subscriber to an officemate asking for the password on behalf of the subscriber's boss.
		A memorised secret is revealed by a subscriber in a telephone inquiry from an attacker masquerading as a system administrator.
		An out of band secret sent via SMS is received by an attacker who has convinced the mobile operator to redirect the victim's mobile phone to the attacker.
Online guessing	The attacker connects to the verifier online and attempts to guess a valid authenticator output in the context of that verifier.	Online dictionary attacks are used to guess memorised secrets.
		Online guessing is used to guess authenticator outputs for an OTP device registered to a legitimate claimant.

Table 8. Authenticator threats used for digital authentication (concluded)

Endpoint compromise	Malicious code on the endpoint proxies' remote access to a connected authenticator without the subscriber's consent.	A cryptographic authenticator connected to the endpoint is used to authenticate remote attackers.
	Malicious code on the endpoint causes authentication to other than the intended verifier.	Authentication is performed on behalf of an attacker rather than the subscriber.
		A malicious app on the endpoint reads an out-of-band secret sent via SMS and the attacker uses the secret to authenticate.
Malicious code on the endpoint compromises a multi factor software cryptographic authenticator.	Malicious code proxy's authentication or exports authenticator keys from the endpoint.	
Unauthorised binding	An attacker is able to cause an authenticator under their control to be bound to a subscriber's account.	An attacker intercepts an authenticator or provisioning key en route to the subscriber.

9.7.2 Threat Mitigation Strategies

Related mechanisms that assist in mitigating the threats identified above are summarised in Table 9.

Table 9. Mitigating Authenticator Threats

Authenticator threat or attack	Threat mitigation
Theft	Use multi-factor authenticators that need to be activated through a memorised secret or biometric.
	Use a combination of authenticators that includes a memorised secret or biometric.
Duplication	Use authenticators from which it is difficult to extract and duplicate long-term authentication secrets.
Eavesdropping	Ensure the security of the endpoint, especially with respect to freedom from malware such as key loggers, prior to use.
	Avoid use of non-trusted wireless networks as unencrypted secondary out-of-band authentication channels.
	Authenticate over authenticated protected channels (e.g., observe lock icon in browser window).
	Use authentication protocols that are resistant to replay attacks such as <i>pass-the-hash</i> .
	Use authentication endpoints that employ trusted input and trusted display capabilities.
Offline cracking	Use an authenticator with a high entropy authenticator secret.
	Store memorised secrets in a salted, hashed form, including a keyed hash.
Side channel attack	Use authenticator algorithms that are designed to maintain constant power consumption and timing regardless of secret values.
Phishing or pharming	Use authenticators that provide verifier impersonation resistance.

Table 9. Mitigating Authenticator Threats (continued)

Social engineering	Avoid use of authenticators that present a risk of social engineering of third parties such as customer service agents.
Online guessing	Use authenticators that generate high entropy output.
	Use an authenticator that locks up after a number of repeated failed activation attempts.
Endpoint compromise	Use hardware authenticators that require physical action by the subscriber.
	Maintain software-based keys in restricted-access storage.
Unauthorised binding	Use MitM-resistant protocols for provisioning of authenticators and associated keys.

9.7.3 Authenticator recovery

The weak point in many authentication mechanisms is the process followed when a subscriber loses control of one or more authenticators and needs to replace them. In many cases, the options remaining available to authenticate the subscriber are limited, and economic concerns (e.g., cost of maintaining call centers) motivate the use of inexpensive, and often less secure, backup authentication methods. To the extent that authenticator recovery is human assisted, there is also the risk of social engineering attacks. To maintain the integrity of the authentication factors, it is essential that it is not possible to leverage an authentication involving one factor to obtain an authenticator of a different factor. For example, a memorised secret must not be usable to obtain a new list of look-up secrets.

9.7.4 Session attacks

The above discussion focuses on threats to the authentication event itself, but hijacking attacks on the session following an authentication event can have similar security impacts. The session management is essential to maintain session integrity against attacks, such as XSS. In addition, it is important to sanitise all information to be displayed (e.g., Open Web Application Security Project (OWASP) XSS-prevention) to ensure that it does not contain executable content. These guidelines also recommend that session secrets be made inaccessible to mobile code in order to provide extra protection against exfiltration of session secrets.

Another post-authentication threat, Cross-Site Request Forgery (CSRF), takes advantage of users' tendency to have multiple sessions active at the same time. It is important to embed and verify a session identifier into web requests to prevent the ability for a valid Uniform Resource Locator (URL) or request to be unintentionally or maliciously activated.

10. Access management

10.1 Overview of access management

Access Management is how an organisation authenticates enterprise identities and authorises appropriate access to protected services. Policy administration is a combination of laws, regulations, rules, and agency policies that secures access to agency services. Organisations should determine the requirements for an individual to access each resource category as it may be as simple or as complex as needed.

Examples of notice for access requirements are as follows.

- a) "Grant access to anyone on this list of people."
- b) "Grant access to any agency employee or contractor with an authenticated MyKad card, issued by JPN"

MCMC MTSFB TC G051:2025

- c) “Grant access to anyone who is a Malayan Banking Berhad employee, Manager grade or higher, and holds a Certified Information Systems Security Professional (CISSP) certification”

In providing access services, it can be challenging to conduct an application discovery and inventory for both physical and logical access.

10.1.1 User access authorisation

Authorisation is the process of deciding whether to allow someone to access or an entity to access the enterprise resource. Access requirements usually dictate whether the organisation should allow someone/an entity to do the following.

- a) Read or modify a certain document.
- b) Access an organisation’s intranet.
- c) Enter an organisation’s facility or location.

Usually, authorisation occurs immediately after authentication. When user log in to a service, the user shall present their credentials. The service then confirms that the user credentials are valid (authentication) and grants or denies access based on the user-assigned permissions (authorisation).

Authorisations are based on progressive, fine-grained access models. Most organisations implement role-based access and move toward more fine-grained access such as attribute-based or risk adaptive access control towards Zero Trust cyber security architecture based on the use cases.

The User Access Authorisation ensures that a verified user can only access the applications and resources they need for their specific role. The Access Management may include additional components such as SSO and Access Governance (AG) role models, which consist of a matrix that enforces Role-Based Access Control (RBAC). The role models are visualised as a digital chart that outlining the hierarchical user structures related to access. SSO allows the users to access all the resources after logging in once to avoid repeated authentication attempts and reduce poor password security when accessing different systems and apps.

The authorisation decisions on access to infrastructure and/or resources shall enable the organisation authority to restrict access to infrastructure or resources locally or in the enterprise based on the evaluation of applicable policies as in the enterprise governance. Controlling infrastructure and resource access is highly critical to protecting private and confidential information from unauthorised users.

Access can be established by the creation of user accounts and user roles with access permissions or by using user attributes and access control policies. The process of authorisation usually involves a user request to access a resource and an evaluation of the security context of the transaction. The outcome of this evaluation is an access control decision that indicates whether the user who tries to interact with the resource follows the policies and governance requirements for its access.

10.1.2 Policy administration

Policy administration is the process of creating, updating, deleting, and auditing the access policies in an organisation. Policy administration helps to ensure that the access policies are consistent, accurate, and aligned with the business objectives and security requirements of the organisation. Policy administration also helps to maintain the compliance and accountability of the access management system.

Policy administration lifecycle consists of four stages, namely, design, implementation, evaluation and change. The lifecycle begins when the access policies shall be defined and documented, based on the analysis of business requirements and risk management. Policy design shall involve resources and

services identifications as well as the users and devices that needs to the access. This includes the setting of policy objectives, scope and enforcement mechanism,

Deployment and activation of policies in the access management is done in policy implementation stage. This should involve the configurations of policy attributes, settings and parameters within the policy engine, which evaluates and enforces the access policies. In this stage, testing and verification of policy shall be conducted to ensure the functional effectiveness and acceptable performance of such implementation.

The access policies shall be monitored and reviewed, occasionally, based on feedback and data gathered by the access management system. Policy evaluation should involve measuring and analysing the policy effectiveness, efficiency, and compliance, using various metrics and indicators, such as access logs, audit reports, and performance reports. This includes resolving any policy issues, error and conflicts.

Policy change shall be invoked when there is a change in organisation or business requirement where the access policies are modified and updated. This shall involve the revising and/or enhancing the relevant policy rules and conditions, based on the feedback and data gathered from the policy evaluation. This shall involve the redeployment and reactivating the updated policies in the policy engine.

Policy administration should use some form of centralized and standardized policy framework to ensure consistent and coherent policy creation and management. Role-based and attribute-based policy models should be used to allow flexibility and dynamic policy assignment and enforcement. These can be based on user and device characteristics and context. Policy lifecycle management tool may help to automate and streamline the administration processes, such as creation, deployment modification and monitoring of policies.

10.1.3 User monitoring and auditing

The User Monitoring and Auditing provides the capabilities to support internal, active management and to review the organisation's operations and processes via a comprehensive activity log. Activity logs may be used to compile business intelligence reporting and audit trails, perform access reviews, ensure correct roles and fix any inefficient IAM processes or issues and improve the IGA. The User Monitoring and Auditing should also support the regulatory compliance and audit requirements.

Table 10 showing various access control models, arranged by control granularity. These accesses shall be monitored and having the audit capability which can fulfil the following objectives.

- a) User identity and access verification and validation.
- b) Ability to detect and prevent access violation and breach.
- c) Ability to identify and resolve issue and incidents relating to access management.
- d) Assist in optimising and refining access management processes and performance.
- e) Compliance with access policies and regulations.

Table 10. Access Control models

Granularity	Access	Model description	Example
Least	ACL	A static list of entities with their access rights	Allow Ali Abu access to email application.
More	RBAC	Access based on a user's static pre-defined role	Ali Abu is assigned the user role "New Employee" which grants access to email and SharePoint.
More	Attribute-Based Access Control (ABAC)	Access based on a user's assigned attributes which may be static or dynamic	Allow Ali Abu to access email if on organisation's device (device attribute) and in Malaysia (location attribute).
Most	Risk Adaptive Access Control (RAAC)	Access based on dynamic risk factors	If Ali Abu is in assigned work location, allow email access from any managed device. If Ali Abu is not in assigned work location, only allow email access from organisation's device.

10.1.4 Privileged Access Management (PAM)

Privileged Access Management (PAM) is a critical aspect of digital identity management, especially within the financial and telecommunication industry, where safeguarding sensitive data and systems is paramount. PAM involves the identification, monitoring, and control of access privileges to critical systems and data. Effective PAM ensures that only authorised personnel have elevated access to essential resources, thereby minimising the risk of data breaches and cyber-attacks.

Implementing PAM includes establishing strict access controls, regularly auditing access logs, and employing MFA for privileged accounts which enables organisation to enhance their security posture, ensuring that access to critical systems is tightly controlled and continuously monitored, aligning with global best practices for information security and identity assurance. Organisation should implement the access control best practices as described in Table 11.

Table 11. Privileged Access Management (PAM) security controls

Security controls	Description
Access controls and policies	Establish stringent access control policies that define the criteria for granting privileged access. This includes role-based access control (RBAC) to ensure that users only receive access permissions necessary for their job functions.
Least privilege principle	Enforce the principle of least privilege, ensuring that users have the minimum level of access required to perform their duties. This reduces the risk of misuse or accidental exposure of sensitive information.
Privileged session management	Monitor and record all privileged sessions to maintain an audit trail of actions taken by users with elevated privileges. This helps in detecting and responding to suspicious activities in real-time.
Regular audits and reviews	Conduct regular audits and reviews of privileged accounts to ensure that access rights are up-to-date and reflect current job responsibilities. This includes deactivating accounts that are no longer needed.

Table 11. Privileged Access Management (PAM) security controls *(continued)*

Segregation of duties	Implement segregation of duties to prevent conflicts of interest and reduce the risk of fraud. This involves dividing critical tasks among multiple users so that no single individual has control over all aspects of a critical function.
Just-in-Time Access (JITA)	Utilise just-in-time access controls to grant privileged access temporarily. This ensures that elevated access is available only when necessary and for a limited time, reducing the window of opportunity for potential abuse.
Privileged Access Workstations (PAWs)	Designate secure, hardened workstations for privileged users to perform sensitive tasks. PAWs are isolated from the rest of the network, reducing the risk of malware or other security threats compromising privileged accounts.
User training and awareness	Provide comprehensive training and awareness programs for users with privileged access. This includes educating them on the importance of security best practices and the potential risks associated with misuse of privileged access.
Incident response and management	Develop and implement an incident response plan specifically for privileged access breaches. This ensures a swift and effective response to any security incidents involving privileged accounts, minimising potential damage.

10.1.5 Security requirements

Three key aspects of access management security requirements are authorisation, access control policies, and monitoring and logging. These aspects are essential for ensuring access management is implemented effectively, securely, and compliant with relevant standards and regulations.

Authorisation is based on the user's identity, role, permissions, and context. Authorisation ensures that users can only access and manipulate the resources and data that they are entitled to, and that they cannot perform actions that are prohibited or restricted.

Some forms of access control such as RBAC and ABAC shall be implemented. In RBAC, users are assigned to roles which define their permissions and access levels. Roles should be defined based on the principle of least privilege, meaning that users should only have the minimum permissions and access levels required to perform their tasks. As for ABAC, attributes used as a deciding factor such as department and location, shall be defined and documented. Policies should allow for granular control, with the ability to provide precise access management based on multiple attributes.

The separation of duties principle should be able to be enforced, where users cannot perform conflicting or incompatible tasks that may compromise the security or integrity of the system. For example, a user who can create or modify a resource or data cannot also approve or verify it.

Dynamic authorisation, where the access and permissions of a user can be adjusted based on the context of the request should be supported. For example, a user may have different access and permissions depending on the time, location, device, or network of the request.

Access control policies are the rules and conditions that govern how access management is implemented and enforced. Access control policies define who can access what, when, where, how, and why. Access control policies help to ensure that access management is consistent, transparent, and auditable.

MCMC MTSFB TC G051:2025

a) Access Control Lists (ACLs)

ACLs shall specify permissions for each resource, including files, databases, and applications. Permissions shall be assigned to individual users or groups based on documented policies. ACLs shall define specific actions (e.g., read, write, execute) that can be performed on resources.

b) Mandatory Access Control (MAC)

A centralized authority shall set access control policies and must not be altered by end-users. Resources and users shall be classified into defined security levels (e.g., top secret, secret, confidential). MAC shall be implemented in environments that require high security, such as government or military sectors.

c) Discretionary Access Control (DAC)

Resource owners shall have the authority to set access policies for their resources. DAC policies should provide flexibility and be suitable for environments where strict control is not necessary. Users should be responsible for managing access to their resources, following organisational guidelines.

To ensure effective and secure access management that complies with relevant standards and regulations, the following measures shall be implemented.

- a) All the access and activities of users shall be monitored and logged. Examples of these include the user's identity, role, permissions, context, request, response, resource, time, date, location, device, and network.
- b) Access and activity logs should be stored in a secure and centralised location, protected from unauthorised access, modification, deletion, or loss. Regular backup should be performed on access and activity logs and with appropriate backup retention policy, as required by the organisation's policy and regulations.
- c) The access and activity logs shall be analysed periodically and on-demand, using various tools and techniques, such as dashboards, alerts, notifications, or reports. Upon request, the access and activity logs should be provided to the authorised stakeholders, such as the system owners, administrators, users, and auditors.
- d) Real-time monitoring systems shall be implemented to detect and alert suspicious activities immediately. Behavioural analytics should be used to identify abnormal access patterns indicative of potential security breaches.
- e) Integration with automated incident response tools should be established to take immediate action upon detecting unauthorised access.

11. Regulatory and compliance requirements

DI and credentials need to be protected as the first line of defence in the digital world. Thus, DISM provides a comprehensive protection of personal data across all stages of handling and processing, reducing the risk of data breaches and unauthorised access that meets the regulatory and industry compliance requirements. DISM also enable organisation to monitor the activities of authorised users and maintain audit logs for reference for investigation and compliance audit.

For an underlying baseline regulatory and compliance requirement, reference should be made to Clause A.2.3 of MCMC MTSFB TC G009 as well as MCMC MTSFB TC G042.

Below are some current recommended and relevant regulatory, sector specific and compliance standards which should be taken into consideration as part of DISM.

11.1 Regulatory

11.1.1 Personal Data Protection Act 2010, Malaysia (PDPA)

The PDPA then came into force in Malaysia on 15 November 2013. The objective is to protect personal data of individuals with respect to commercial transactions. The PDPA was gazetted in June 2010 is an Act that regulates the processing of personal data in regard to commercial transactions. The penalty for non-compliance is between RM100k to 500k and/or between 1 to 3 years imprisonment.

The PDPA's Security Principle mandates the protection of personal data against loss, misuse, and unauthorised access by data controllers and data processors such as third-party service providers. A reasonable and practical security measures to protect personal data from loss, misuse, modification, destruction, accidental access/disclosure requires an effective access and data protection security controls. For example, the ID and Password management and the access control shall be well established and practiced.

11.2 Other regulatory and compliance requirements

Most governments expect organisations to provide a robust, flexible and secure DISM. Regulatory compliance acts such as Sarbanes-Oxley Act (SOX), Gramm-Leach-Bliley Act (GLBA), and Health Insurance Portability and Accountability Act (HIPAA) mandate organisations within the applicable industry to be accountable for protecting access to customer and employee information.

DISM shall help organisations to comply with these regulations by automating user access to networks, data and applications. DISM systems assist organisation to comply with regulatory requirements and relieve IT support from manual, unsecure and ineffective identity management. With the shortages of cybersecurity workforce combined with the penalties for non-compliance with industry regulations can cost an organisation millions of dollars.

Besides PDPA, other recommended but optional regulatory and compliance standards that the DISM may be required to comply with include the following.

11.2.1 General Data Protection Regulation 2018, EU (GDPR)

The EU GDPR was enforced in May 2018, affecting every organisation that does business within EU countries and/or has European customers. GDPR is the toughest privacy and security law in the world. The GDPR will levy harsh fines against those who violate its privacy and security standards, with penalties reaching into tens of millions of euros.

The GDPR requires strong security and user access controls. GDPR mandates that organisations protect the personal data and privacy of European Union citizens. For data breach incident, the organisation has 72 hours to tell the data subjects or face penalties. This notification requirement may be waived if use technological safeguards, such as encryption, to render data useless to an attacker.

Organisations shall handle data securely by implementing appropriate technical and organisational measures. Technical measures mean anything from requiring users to use two-factor authentication on accounts where personal data are stored to data processing with cloud service providers that use end-to-end encryption. Organisational measures such as staff trainings, data privacy policy employee/user handbook/manual, or limiting access to personal data to only users who needs it.

11.2.2 ISO/IEC 27001 and 27002 ISMS Requirements

ISO/IEC 27001 is one of the best-known standards for information security management systems (ISMS). It defines requirements for companies of any size and from all sectors of activity with guidance

MCMC MTSFB TC G051:2025

for establishing, implementing, maintaining and continually improving an ISMS. Conformity with ISO/IEC 27001 means that an organisation or business has put in place a system to manage risks related to the security of data owned or handled by the company, and that this system respects all the best practices and principles enshrined in this International Standard.

Relevant sections from ISO27001 that could be referenced on in relation to DIMS includes section A.9 - Access Control, A.10 - Cryptographic Controls and A.15 Supplier Relationship.

While ISO/IEC 27001 outlines the requirements for an ISMS, ISO/IEC 27002 offers best practices and control objectives related to key cybersecurity aspects including access control, cryptography, human resource security, and incident response. The standard serves as a practical blueprint for organisations aiming to effectively safeguard their information assets against cyber threats. By following ISO/IEC 27002 guidelines, companies can take a proactive approach to cybersecurity risk management and protect critical information from unauthorised access and loss.

Relevant sections from ISO27002 that could be referenced on in relation to DIMS includes section A.9.2 - Identity and Authentication, A.13.2 - Handling Sensitive Information and A.18.1 - Compliance with Legal and Regulatory Requirements.

11.2.3 Service Organisation Control 2 (SOC 2) Requirements

The System and Organisation Controls (SOC) is a set of standards designed by the American Institute of Certified Public Accountants (AICPA) and documented in the Trust Services Criteria (TSC). It creates a level of confidence and trust for organisations when they engage a third-party to provide important services. A SOC 2 report would provide detailed information and assurance that a service provider has put in the necessary controls by conducting an evaluation on its data protection systems and procedures in relation to security, availability, processing integrity, confidentiality and privacy.

Under the SOC2 criteria, logical access controls include the requirements to assign unique identification for all users, and implementation of strong authentication mechanisms with MFA where appropriate. For Account Management, organisations need to establish processes to manage user accounts, including creation, modification, and deletion. Ensure that only authorised individuals can create and modify user accounts. Define roles and assign access rights based on the principle of least privilege. Regularly review and update roles and access rights.

11.3 Sector specific compliance

11.3.1 Risk Management in Technology 2020 & 2023, BNM Malaysia (RMiT)

Bank Negara Malaysia (BNM)'s Risk Management in Technology (RMiT) Policy Document (PD) came into effect on 1 January 2020. The policy intended to formalize the risk management programs used when adopting cloud and other technological innovations in Malaysian Financial Institutions (FIs). BNM issued an updated new PD on Risk Management in Technology on 1 June 2023. The updated PD supersedes the previous policy document on 1 January 2020 except for paragraphs 10.49, 10.50, 10.51 and 10.52 which will remain applicable until 31 May 2024.

Technology risk refers to risks emanating from the use of IT and the Internet. These risks arise from failures or breaches of IT systems, applications, platforms or infrastructure, which could result in financial loss, disruptions in financial services or operations, or reputational harm to a financial institution.

The RMiT mandate a financial institution shall implement an appropriate access controls policy for the identification, authentication and authorisation of users (internal and external users such as third-party service providers). This must address both logical and physical technology access controls which are commensurate with the level of risk of unauthorised access to its technology systems.

A financial institution shall also employ robust authentication processes to ensure the authenticity of identities in use. Authentication mechanisms shall be commensurate with the criticality of the functions and adopt at least one or more of these three basic authentication factors, namely, something the user knows (e.g. password, PIN), something the user possesses (e.g. smart card, security device) and something the user is (e.g. biometric characteristics, such as a fingerprint or retinal pattern).

The RMIT also require that all financial institutions shall implement robust risk management controls above the minimum regulatory standards to deliver efficient financial services securely and prevent the exploitation of weak links in interconnected networks and systems with robust cyber fortification to preserve public confidence in the financial systems. The latest key updates to the RMIT PD include:

- a) Additional guidance to strengthen financial institution's cloud risk management capabilities.
- b) A shift to a risk-based approach in cloud consultation and notification process with corresponding updates in the risk assessment and submission requirement.
- c) The use of MFA security control is denoted as a standard requirement.
- d) The Frequently Asked Questions document has been revised to aid the implementation of the revised policy requirements.

11.3.2 Payment Card Industry Data Security Standard (PCI DSS) requirements

The Payment Card Industry Data Security Standard (PCI DSS) defines security requirements to protect environments where payment account data is stored, processed, or transmitted. PCI DSS provides a baseline of technical and operational requirements designed to protect payment account data.

PCI DSS access controls are designed to restrict access to cardholder data to only those individuals on a Need-to-Know basis. These controls include the implementation of authentication methods, user identification, and access authorisation processes to ensure that cardholder data is protected from unauthorised access and breaches, thereby maintaining the integrity and confidentiality of sensitive information.

PCI DSS contains rigorous access controls measures with that includes MFA and enhanced user identification management such as:

- a) Systematic User Identification

Assigning a unique ID to each person with computer access ensures that actions on critical data can be traced to individual users.

- b) Restriction of Access to Cardholder Data

Access rights must be set according to job classification and function, limiting exposure to sensitive data.

12. DISM effectiveness measurement

Organisations need to take proactive measures to align their processes, policies, and data quality in order to fully leverage the benefits and functionality of DISM based on ICAM (Identity, Credential, and Access Management). ICAM solutions are valuable tools for automating routine administrative IT tasks, enhancing security, and managing cybersecurity risk. However, simply implementing these technologies is not a comprehensive practice that instantly resolves all organisation's challenges. Therefore, the Table 12 below provides sample measures such as "User Authentication Success Rate" and "Number of Unauthorised Access Attempts" for an effective ICAM solution. Each row in the table represents a key area of focus, its description, the metrics used to measure its effectiveness, and

MCMC MTSFB TC G051:2025

examples of KPIs that can be used to track performance over time. This comprehensive approach ensures a holistic view of the organisation's security posture and aids in continuous improvement.

Table 12. Key focus area and related metrics

Key focus area	Description	Metrics	Examples of KPIs
Operational efficiency	ICAM streamlines access management processes by automating user provisioning, authentication, and authorisation tasks. This improves operational efficiency, reduces administrative overhead, and enhances user experience. Organisations are free to pursue efficiency objectives, and the expectation is the efficiency and time saving will increase with familiarity.	Metrics for operational efficiency could include reduced time taken for user provisioning, decreased administrative overhead costs, user satisfaction scores and average time to resolve compliance issues.	Time to Provision/De-provision User Access, Number of Active Digital Identities, User satisfaction score, Number of helpdesk tickets related to user access issues.
Security enhancement	ICAM helps protect critical data and meet legal obligations by ensuring only authorised individuals have the necessary and correct access to resources and digital assets within a company's systems.	Security enhancement can be measured by the reduction in security incidents or breaches, effectiveness of authentication mechanisms, and the effectiveness of multi-factor authentication (MFA) adoption.	User Authentication Success Rate, Number of Unauthorised Access Attempts.
Regulatory compliance	ICAM should help the organisation comply with various regulatory standards. This can be measured by the number of compliance issues or breaches that occur.	Compliance can be measured by the number of compliance issues resolved, the number of breaches prevented, the level of adherence to regulatory standards, audit findings and the number of non-compliance incidents.	Percentage of access reviews completed on time, number of compliance training sessions conducted, percentage of employees passing compliance training.
Risk management	ICAM should help manage risks associated with unauthorised access to resources. This can be measured by the number of security incidents or breaches that occur.	Risk management effectiveness can be measured by the reduction in security incidents or breaches, and the effectiveness of risk mitigation strategies.	Number of orphan accounts

Table 12. Key focus area and related metrics *(continued)*

<p>Governance and leadership</p>	<p>The effectiveness of ICAM is reflected in how well it is governed and led, encompassing the development and enforcement of operational policies, the strategic categorisation and assignment of tasks, and effective stakeholder identification and communication. Strong governance ensures that ICAM aligns with organisational goals, efficiently utilises resources, and complies with regulatory and security requirements.</p>	<p>Governance and leadership can be measured by the effectiveness of policies and procedures, stakeholder satisfaction, and the alignment of ICAM with organisational objectives.</p>	<p>Access request approval time</p>
<p>Performance management</p>	<p>The progress, effectiveness, and improvements of the ICAM program can be measured and reported. This includes managing risks associated with handling Personally Identifiable Information (PII).</p>	<p>Performance can be measured by the progress toward ICAM goals, the effectiveness of the ICAM program, and the improvements made over time.</p>	<p>Number of roles defined in RBAC system, number of Segregation of Duties (SoD) violations detected, percentage of users with MFA.</p>

MCMC MTSFB TC G051:2025

Bibliography

- [1] MCMC MTSFB TC G009, *Information and Network Security - Requirements*
- [2] Bank Negara Malaysia (BNM), *Risk Management in Technology (RMiT) Policy Document*
- [3] ISO/IEC 27002:2022, *Information security, cybersecurity and privacy protection - Information security controls*
- [4] Recommendation ITU-T X.1051, *Information technology - Security techniques - Information security management guidelines for telecommunications organisations based on ISO/IEC 27002*
- [5] Recommendation ITU-T X.1151, *Guideline on secure password-based authentication protocol with key exchange*
- [6] Recommendation ITU-T X.1152, *Secure end-to-end data communication techniques using trusted third-party services*
- [7] Recommendation ITU-T X.1153, *Management framework of a one-time password-based authentication service*
- [8] Recommendation ITU-T X.1154, *General framework of combined authentication on multiple identity service provider environments*
- [9] Recommendation ITU-T X.1158, *Multi-factor authentication mechanisms using a mobile device*
- [10] Recommendation ITU-T X.1254, *Entity authentication assurance framework*
- [11] Recommendation ITU-T X.1277, *Universal authentication framework*
- [12] Recommendation ITU-T X.1278, *Client to authenticator protocol/Universal 2-factor framework*
- [13] Recommendation ITU-T X.1280, *Framework for out-of-band server authentication using mobile devices*
- [14] Recommendation ITU-T X.1450, *Guidelines on hybrid authentication and key management mechanisms in the client-server model*
- [15] ETSI TR 103 305-1, CYBER; *Critical Security Controls for Effective Cyber Defence; Part 1: The Critical Security Controls*
- [16] European Union Agency for Cybersecurity (ENISA), *Digital Identity Standards*
- [17] Canadian Centre for Cyber Security, *Identity, Credential, and Access Management (ICAM)*
- [18] Payment Card Industry Security Standards Council, *Payment Card Industry Data Security Standard: Requirements and Testing Procedures*
- [19] Edarasystem.com, *Unveiling the Advantages of the ICAM Investigation Process*
- [20] Journal of Information Science. 1-15. 10.1177/01655515231160026, *Digital information security management policy in academic libraries: A systematic review*

- [21] BusinessBasics Australia, *What is ICAM benefits of ICAM incident investigation*
- [22] Computers 2024, 13, 41, *Security and Privacy of Technologies in Health Information Systems: A Systematic Literature Review*.
<https://doi.org/10.3390/computers13020041>
- [23] Cengage Learning, *Management of Information Security, 6th Edition*

MCMC MTSFB TC G051:2025

Acknowledgements

Security, Trust and Privacy Working Group

Working Group Leaders

Mr Thaib Mustafa (Chair)	Smart Tech AP Sdn Bhd
Prof Dr Shahrulniza Musa (Vice Chair)	Universiti Kuala Lumpur
Ms Norkhadhra Nawawi (Secretary)	FNS (M) Sdn Bhd

Drafting Committee Members

Mr Ng Kang Siong (Draft Lead)	Digital Connect Society
Ms Alisa Rafiqah Adenan (Secretariat)	Malaysian Technical Standards Forum Bhd
Dr Maslina Daud	CyberSecurity Malaysia
Ms Norkhadhra Nawawi	FNS (M) Sdn Bhd
Mr Thaib Mustafa	Smart Tech AP Sdn Bhd
Dr Amna Saad	Universiti Kuala Lumpur

Contributors

Ts Lee Hwee Hsiung	CyberSecurity Malaysia
Mr Tan Tze Meng	Malaysia Digital Economy Corporation Sdn Bhd
Dr Ahmad Shahrafidz Khalid	Universiti Kuala Lumpur
<i>Mr Goh Ser Yoong</i>	<i>Advance.AI</i>
<i>Mr Alwyn Goh</i>	<i>Goopletech.com</i>
<i>Mr Wong Wai Kong</i>	<i>Ypsilon System Sdn Bhd</i>