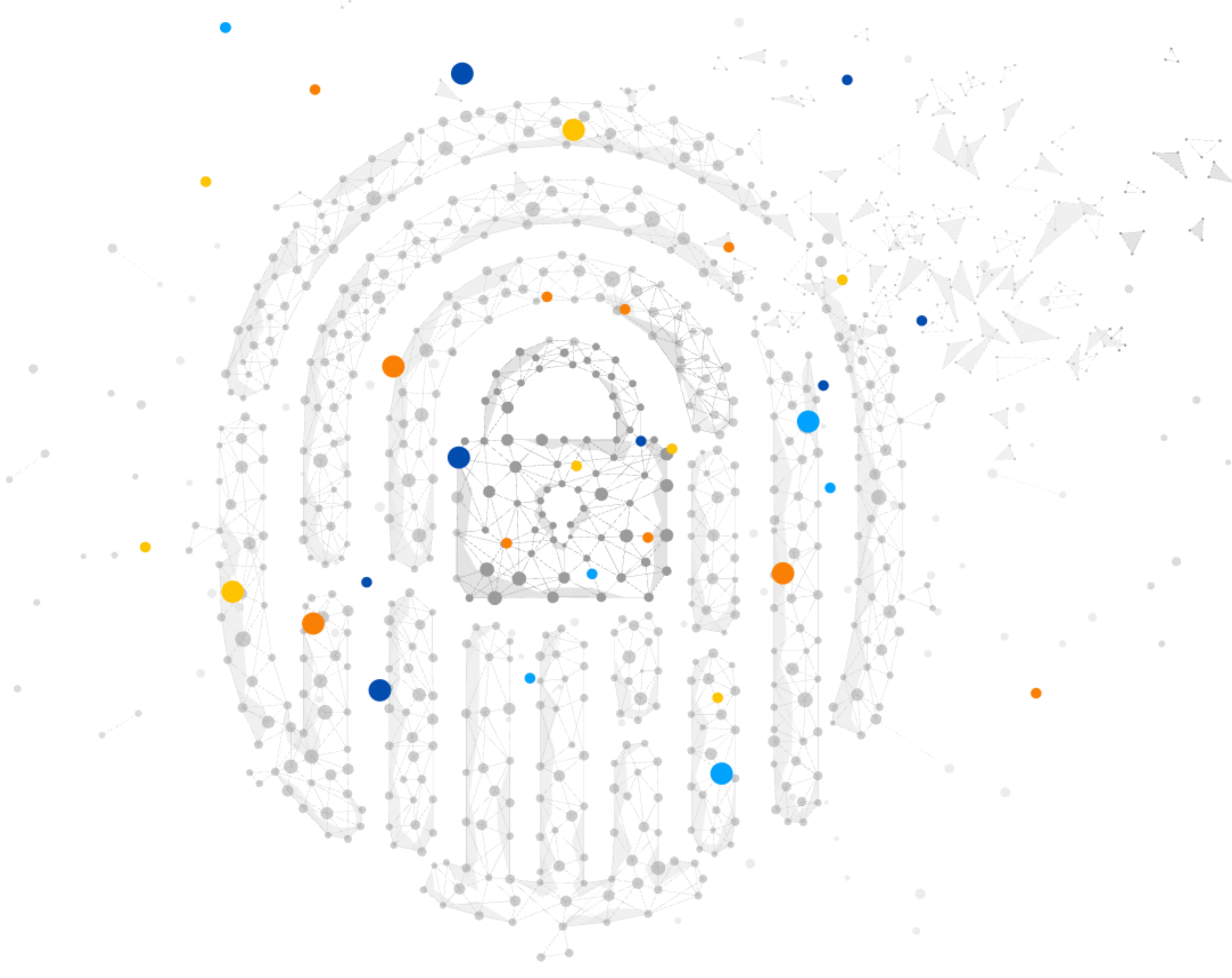
MACP – Framework (V1.0)

Enrolment Devices

DOCUMENT 1 OUT OF 3*



Created in collaboration with BixeLab, with assistance from the members of the Biometric Working Group

*For latest documentation, visit the Biometric Certification Framework on GitHub.

Gates Foundation Norad Pratiksha Trust TATA TRUSTS

Table of Contents

1. Introduction

It is fairly universally accepted that issuance of identity is a complex exercise. In digital identity systems based on platforms like MOSIP, biometrics, where needed, provide an essential integrity measure for establishing uniqueness. As MOSIP adoptions accelerate across the world, a growing community of partners and vendors are geared up to make MOSIP-compliant biometric devices and solutions available worldwide.

It is important to recognise that the quality of biometric images acquired helps determine the overall efficiency of a system, and has a direct impact on a system’s ability to perform deduplication and authentication functions. In order to provide an independent “certification” or “assurance” mechanism for the biometric devices that MOSIP users are deploying, MOSIP has initiated the drafting of a modular, globally adoptable, certification framework.

The objective of this effort, is to:

1. Arrive at a framework that provides standardised assessment criteria and standard operating procedures to test devices/solutions against these criteria

2. Enable the establishment of standardised MOSIP biometric device certification programmes which are capable of providing independent certifications to MOSIP users.

The vision is to arrive at a framework for the assessment of full compliance at the levels of image quality, software interfaces, and hardware-based security implementation levels, in a way that offers meaningful and realistic results. Adopting countries should be able to rely on these results while making decisions on biometric devices in their ecosystems.

An independent mechanism for biometric certification will offer users the flexibility to rely on empanelled, independent laboratories to ascertain the quality of devices. This will reduce the risks and effort associated with establishing full-fledged programmes, which may be resource-intensive and time-consuming.

The decided-upon standard assessment criteria have to be independently adoptable by global laboratories; those that can support both global and geography-specific needs for compliance; that MOSIP-adopting countries can rely on. These labs will offer an MACP (MOSIP Advanced Compliance Programme) certification; that will be structured with country needs in mind and developed in consultation with the ecosystem.

The framework will be developed in a staged manner, and the output of the work will be published regularly to the ecosystem for their feedback.

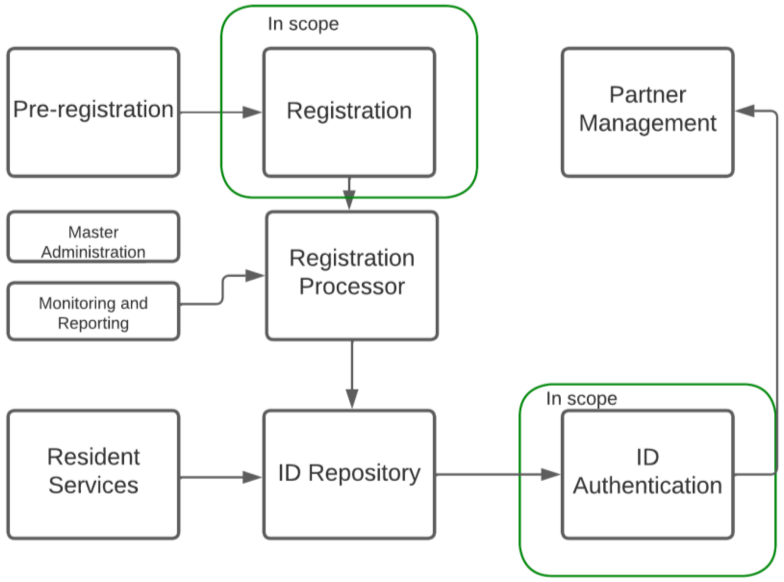
1.1 Objectives

High quality enrolment standards must be set so that biometric enrolment and matching can be used accurately in a wide variety of environments and supporting most, if not all, demographics. It is necessary to have a certification standard that can ensure consistency in the capture quality across different modalities. This also applies to authentication devices.

This document sets out the MOSIP Advanced Compliance Program (MACP) requirements applicable to qualified third-party testing laboratories providing certification of eligible biometric device providers against the respective MACP specifications. A more comprehensive end-to-end framework will be created as the MACP matures over time.

1.2 Scope

Current specifications only relate to requirements set out in this framework for qualified testing labs undertaking biometric device testing related to quality. All other certification activities that are not related to quality testing are out of scope for the current project.



Here, "Registration" corresponds to an individual providing their biometrics to the biometric capture device for enrolment[1].

1.1.1 Within Scope

- Specifications for testing for compliance to the MACP quality standards for face, finger, and iris modalities
- Sample quality compliance report
- Standards compliant delivery of biometric samples

[1] The terms 'enrolment' is used throughout the document for consistency and simplicity.

1.1.2 Outside of Scope for This Document

- All non-quality certification including:
    - Accuracy and vulnerability components within the MOSIP ecosystem architecture
    - Biometric algorithm requirements
    - Security and fraud control requirements
    - Risk management, usability testing
    - Durability testing
    - Technical testing
    - General IT requirements
    - Privacy, and governance
    - All relevant non-quality related parameters and their assessment framework will be appended to the master certification framework document. Quality is one section in the overall framework.

2. Biometric Device Requirements for SBI 1.0/L0

Biometric device requirements include:

Any biometric device tested for MACP compliance will be integrated with the MOSIP Software. Therefore, verification that the biometric device is communicating with the MOSIP structure properly is the first step towards ensuring compliance to MOSIP requirements.

Other requirements are listed in the sections below.

2.1 Quality Specifications

Table 1: MACP Quality Specifications Overview

Criteria	Description
Test Planning	
Test Plan	The test plan document is compliant with section 3.2 of this document
Testing	
Test Execution	The test execution is informed by section 3.2 of this document and requirements on Image Quality and Image Formats.
Image Quality	Image acquisition errors such as failure to enrol which is the expected proportion of the population for whom the system is unable to generate repeatable templates. This will include those unable to present the required biometric feature, those unable to produce an image of sufficient quality at enrolment. The failure to enrol rate will depend on the enrolment policy. For example, in the case of failure to enrol, enrolment might be re-attempted later. **Quality** **1. Compliance** a. **Face/Finger/Iris:** Current MOSIP Compliance specifications for ISO/IEC 19794 series (Biometric Specification - MOSIP Docs 1.1.5) **2. Best Practice** **a. Compliance to the specifications of Image Quality Standards and Technical Reports is considered best practice:** i. ISO/IEC 29794-2:2017- Biometric Sample Quality (Finger Image Data)

Criteria	Description
Test Planning	
	ii. ISO/IEC 29794-6:2015- Biometric Sample Quality (Iris Image Data) iii. ISO/IEC 29794-5:2010- Technical Report for Biometric Sample Quality (Face Image Data)[2] iv. ISO/IEC 24358: Specifications for face-aware capture subsystems v. Compliance to NFIQ 2 for enrolment and NFIQ 1 for authentication fingerprint devices
Image Formats	Image formats are compliant with the MOSIP Docs 1.1.5 Biometric Specification: Image Formats for Fingerprint, Iris, and Face Capture (as applicable)
Test Reporting	
Test Report	The test report document is compliant with section 3.3 of this document

3. Testing for MACP: Biometric Compliance

3.1 Laboratory Qualification Criteria

Note: Please see the detailed documentation here: https://github.com/mosip/biometric-certification-framework

[2] Working draft to be published

Biometric testing must be conducted by a qualified, third-party, biometrics testing entity which, at minimum, displays the following characteristics:

- Be a certified ISO 17025 laboratory
- Has the ability to provide relevant policies and procedures for working with human test subjects that have been approved by a relevant national body. The lab shall implement this policy to:
  - ensure the physical and psychological well-being of human subjects throughout testing.
  - act as a safeguard to prevent against ethical judgement errors
  - ensure that human subject testing complies with applicable national legislation
- At a minimum has personnel with demonstrated expertise in biometric evaluation (more than two years), and can provide evidence of proficiency in standardised ISO compliant biometric testing and reporting
- Is able to show evidence that they are an independent entity with no apparent or actual conflict of interest

3.2 Test Planning

The test plan document shall be informed by the recommendations of the following standards and frameworks, as applicable for the test type planned i.e., scenario, technology type evaluation, in conjunction with other applicable standards and frameworks:

- ISO/IEC 19795-1 (2021)
- ISO/IEC 19795-2 (2007)
- ISO/IEC 19795-3 (2007)

The tables below provide guidance and recommendations for the testing laboratories to prepare the original test plan. The test planning is directed by the MACP compliance requirements as listed in Table 1 MACP Quality Specifications Overview, and is constrained by characteristics of the biometric device tested and specific requirements which should not be altered for the purpose of testing.

The test plan shall not specify the method(s) by which the biometric device implements its functions, as it is the responsibility of the biometric device to perform its functions in its own way.

To prepare for an MACP evaluation test plan, the evaluator should refer to the table below to determine:

- Which recommendations are implemented
- Which approach is used to verify MACP compliance and what it entails for the data collected

Deviations must be included in the final test report, along with a reasonable justification.

Comments from WG on Device Profile for face modality:

> “Some of this should be informed by ISO/IEC 24358 – Face-aware capture subsystem specifications”

Note: It is key to note that in real-world laboratory testing, a device profile approach for various deployment use cases is proposed. These device profiles will be included over time in the framework itself and informed by the exploratory testing undertaken on various device types to have requirements in relation to number of people, environmental conditions etc.

Table 2: Summary of recommendations for test plan preparation

Item	Requirement Category	Description	Specification	
Target of evaluation[3]	Requirements for the biometric device to be tested for MACP Compliance	Single operating threshold	YES	
		Documented device enrolment policy covering the maximum number of enrolment attempts allowed in a transaction		
	Data accessibility	Ability to export results		
Data Collection	Subject Diversity[4]	Collected data should be diverse with regard to age[5]	**Age**	**Distribution**
			18-30	25-40%
			31-50	25-40%
			51-70	25-40%
		Collected data should be diverse with regard to gender	**Gender**	**Distribution**
			Male	40-60%
			Female	40-60%

[3] ISO/IEC 19795-9 (2019)

[4] ISO/IEC 19795-5 (2011)

[5] The age group and gender demographic distributions are informed by the ISO/IEC 19795-5 standard. As the framework matures overtime, considerations can be made to modify these distributions in accordance with the target deployment use-case. For instance, inclusion of under 18 age groups for national identity use case.

		Collected data should be diverse with regard to ethnic origin *Comments from WG: feasible ways to avoid multiple runs per demographic.* *"one approach could be country PoC's"*	A biometric system tuned to a specific target population can perform less well if used with a different ethnic mix. Hence, the dataset to be utilised for testing shall be reflective of the target populations' ethnic origins
	Subject Training	The evaluator should provide written or verbal instructions to the participating test subjects	YES
	Subject Collection	Minimum number of subjects	The evaluator must employ at least 10 unique and demographically diverse individuals. Due to practical limitations on test corpus size for quality assessment the core focus must be on testing under various environmental conditions that affect quality. For each modality there will be a device profile that will specify the range of conditions to be tested.
	Test Case suitability	Are the planned test cases relevant for the selected device profile	YES

		Are the planned test cases representative of the biometric device use case?		
		Do the planned test cases allow the evaluator to understand how the solution performs in less optimal environmental conditions (e.g., poorer lighting, high humidity, poor user compliance)		
		During test planning and dataset collection, have considerations been made for factors influencing quality e.g., environmental variables, age of samples etc.?		
Lab Evaluation	Methodology and biometric failure criteria	Biometric	Failure to Enrol (FTE)	For FTEs: explanation on what constitutes the FTE is recommended. FTE should be calculated to get an indication of usability.
		Quality		**Required:** Biometric images for various modalities are

			represented and exchanged as per the Image formats in MOSIP Docs 1.1.15. **Recommended:** Compliance to the image quality specifications (as applicable) in: a. ISO/IEC 29794-2:2017- Biometric Sample Quality (Finger Image Data) b. ISO/IEC 29794-6:2015- Biometric Sample Quality (Iris Image Data) c. ISO/IEC 29794-5:2010- Technical Report for Biometric Sample Quality (Face Image Data)
	Test Plan structure	Test plan structure follows recommendations in Table 3	YES

Table 3: Summary of recommendations for Test Plan structure

Item	Subheading	Description
Preface	Glossary	Terms, definitions, and abbreviations and related documents for referencing compliance
	Related Documents	
Introduction	Purpose, scope, users	

Item	Subheading	Description
	Applicable device profile	Provide an overview the expected outcomes of the evaluation, a primer on the test strategy and characteristics of the data that will be used in the evaluation.
	Limitations	
Test Strategy	Data collection	The test strategy will provide the background to the system under test and the approach taken for testing. This will identify the incoming requirements to achieve the testing objectives and the expected outputs based on limitations identified.
	Execution	
	Reporting	
Data privacy and management	PII Handling SOP and privacy policy	Handling of PII utilised for the evaluation
System overview	System Under Test	Description of the system under test. The system under test demonstrates compliance to the specifications discussed in Deviations must be included in the final test report, along with a reasonable justification. Comments from WG on Device Profile for face modality. "Some of this should be informed by ISO/IEC 24358 – Face-aware capture subsystem specifications" **Note:** It is key to note that in real-world laboratory testing, a device profile approach for various deployment use cases is proposed. These device profiles will be included over time in the framework itself and informed by the exploratory testing undertaken on various device types to have requirements in relation to number of people, environmental conditions etc. Table 2 Summary of recommendations for test plan preparation

Item	Subheading	Description
Data	Dataset Preparation	Description of the dataset used in the testing; attributes of the test data based on the requirements established. Planned data to demonstrate compliance to specifications discussed in Table 2
	Datasets	
	Naming convention	
	Suitability	
Pre-testing	Pre-test readiness review	Pre-testing and set up description to ensure correct system operation and configuration
Test Method	Calculation of metrics	Test method to measure metrics to demonstrate compliance to specifications discussed in Deviations must be included in the final test report, along with a reasonable justification. Comments from WG on Device Profile for face modality. "Some of this should be informed by ISO/IEC 24358 – Face-aware capture subsystem specifications" **Note**: It is key to note that in real-world laboratory testing, a device profile approach for various deployment use cases is proposed. These device profiles will be included over time in the framework itself and informed by the exploratory testing undertaken on various device types to have requirements in relation to number of people, environmental conditions etc. Table 2 Summary of recommendations for test plan preparation
Test Cases	Test Case Setup	

Item	Subheading	Description
	Unconstrained Testing	Individual test cases to measure the system performance

3.3 Reporting the Results

Table below provides a summary of guidance and recommendations for test report produced as a result of MACP evaluation.

The guidance and recommendations herein are in accordance with various ISO/IEC 19795 series standards for testing and reporting.

Deviations can be made in depending on the type of evaluation and the modality used, with legitimate explanation for deviation is provided in the test report.

Table 4: Recommendations on reporting the results

Item	Subheading	Description
Preface	Glossary	Terms, definitions, and abbreviations and related documents for referencing compliance
	Related Documents	
	Notices	
Introduction	Purpose, scope, users	Provide an overview the expected outcomes of the evaluation, a primer on the test strategy and characteristics of the data that will be used in the evaluation.
	Limitations	
Scenario description	Device Profile Utilised	Evaluator references the device profile used
	System Under Test	

Item	Subheading	Description
	Definition of Test Criteria	Description of system under test, summary of operating environment, summary of pretesting activities for set up, additional information concerning continual audit checks of the system configuration, expected outputs. The goal of test will be to evaluate performance within the concept of operations, hence it should be designed and executed so that it mimics the functional and procedural aspects of such concept of operations. System information such as manufacturer, model, version, and firmware as applicable must be reported. A chronological record of the test events should also be covered by this report.
	Concept of Operations	
	System Information	
	Configuration audits	
	Test observation and problem log, Test log	
	Expected outputs	
Data	Characteristics of Data	The test report should document whether the data utilised meets the requirements of the MACP testing. Examples of data collection may be provided in the form of spreadsheets and logs
	Data Collection	
	Pretesting with data and final test data for analysis	
Performance Results ***Note***: *benchmarks will be determined based on modality and feedback based on*	Interim Analysis Results	Evaluator provides basis and narrative for management of interim analysis. For the final analysis, the performance results are reported in accordance with the recommendations in Table 1
	Final Analysis Results	
	Overall assessment of the biometric device tested	

Item	Subheading	Description
exploratory evaluations to set the baseline	Conformance to the test plan	
Test Cases	Detailed test results for the test cases	The test cases planned and executed for MACP compliance may be informed by: - NIST Fingerprint Image Quality (NFIQ) Compliance for fingerprint - IREX II for iris - ISO/IEC 29794-5 (WD) which establishes requirements for face image quality based on ISO/IEC 39794-5 standard for face modality. The test cases must be planned and executed in the manner which ensures verification of biometric device performance against the specific requirements listed in Table 1
	Summary of test results, findings, and recommendations	
Deviations and exclusions	Deviations from the test cases/procedures	Explanations associated with any deviations made from the planned test cases or the requirements of this compliance framework must be provided in the test report.
Full Test Plan		As per Table 2 and Table 3

3.4 Certification Validity Period and Renewal

The validity cycle will be set at up to two years. Even without design or software changes, all certified devices must undergo a renewal process with the accredited laboratory at the end of their validity cycle.

- The renewal process may only require documentation review confirming that no substantive changes have occurred.
- If minor changes are present, the renewal may require limited testing under Delta Certification to validate continued compliance.
- Full re-certification is only required if substantive changes have been made as described above.

3.5 Re-Certification

A device that has already obtained MACP certification must undergo re-certification if one or more of the following occur:

1. **Algorithmic Changes**
   - Any update or replacement of the biometric capture, feature extraction, matching, or quality assessment algorithm that may affect capture characteristics, image quality, or interoperability with MOSIP specifications.
2. **Sensor or Hardware Design Changes**
   - Replacement or redesign of the biometric sensor (e.g., change in camera type, fingerprint platen, or illumination source).
   - Any alteration to optical components, lenses, or coatings that may influence biometric capture.
3. **Environmental and Form Factor Changes**
   - Modifications to casing, housing, ruggedisation, or ergonomics that materially impact capture performance (e.g., indoor-only to outdoor-capable).

Note: In some cases, such changes may qualify for Delta Certification instead of full re-certification (see below).

3.6 Delta Certification

Delta Certification applies where minor modifications have been made that do not impact the core biometric capture technology. In these cases, the certification effort is limited to the changed component, while the baseline certification remains valid. Examples include:

- A core certified module (sensor + algorithm) being deployed in a new form factor (e.g., desktop vs. handheld) but using the same operating system and capture pipeline.
- Minor software updates that alter workflow or user interface without modifying capture, feature extraction, or image quality metrics.
- Device firmware upgrades that improve efficiency or compatibility without changing core biometric capture characteristics.

This approach reduces duplication of effort while ensuring interoperability and compliance with MOSIP specifications

3.7 Dispute Resolution

Any disputes related to certification outcomes, test results, or interpretations of criteria shall be resolved by a Certification Review Committee convened by MOSIP.

- The Committee will include representatives from the Biometric Working Group and other relevant stakeholders.
- The Committee’s role is to review evidence, deliberate independently, and provide a binding resolution.
- This ensures transparency, fairness, and accountability in the certification process.

3.8 Adoption Guideline for Countries

The MACP biometric device certification programme is newly introduced and is in the process of being adopted across MOSIP implementations. To ensure smooth adoption and sufficient readiness from vendors and laboratories, the following guideline applies:

- Unless there is an in house certification methodology in place, Countries adopting MOSIP are recommended to include MACP certification as a requirement for vendors to demonstrate compliance before devices are deployed in the field
- At this stage, it is not recommended to make MACP certification a pre-requirement for vendor participation or procurement. Instead, vendors may be engaged first, and then required to undergo certification prior to field deployment.
- This phased approach will allow time for vendors and laboratories to align with the certification programme while ensuring that only compliant devices are eventually deployed in operational environments.

Validity of this guideline:

This guideline shall remain valid **until the end of April 2026**, after which MOSIP will review the maturity of the certification programme and the broader ecosystem. A revised guideline will be published at that stage, which may update the requirement to recommend pre-certification at the procurement stage.

Annex: Comparing Other Certifications

Several established certification programmes exist today, such as FBI PIV in the United States and STQC in India. These provide important assurances of biometric device performance, and vendors with these certifications have already demonstrated compliance with recognised international benchmarks.

However, MACP has a different focus and is designed to address specific requirements for MOSIP deployments:

1. **Scope of Evaluation**
   - **FBI PIV / STQC**: Primarily validate sensor hardware performance and image quality against baseline standards (e.g., NIST-defined metrics for fingerprints, or image capture quality under defined conditions).
   - **MACP**: Extends beyond device-level checks to include compliance with the Standard Biometric Interface (SBI), ensuring that both the capture and the subsequent processing, packaging, and exchange of biometric images meet MOSIP's open standards.
2. **System Integration**
   - **FBI PIV / STQC**: Certify devices as standalone units that meet capture quality specifications.
   - **MACP**: Ensures that devices are interoperable within MOSIP ecosystems, where biometric images are not only captured but also passed through SBI-defined processes for deduplication, authentication, and interoperability across vendors.
3. **Processing Considerations**

  - **FBI PIV / STQC**: Emphasise image quality thresholds at the point of capture.
  - **MACP**: Recognises that a significant portion of biometric data handling occurs during acquisition and SBI processing (e.g., metadata inclusion, image formatting, error handling). Certification therefore validates processed outputs.

Summary

FBI PIV and STQC remain valuable benchmarks for biometric device quality and are complementary to MACP. What makes MACP different is its emphasis on SBI compliance and ecosystem interoperability, ensuring that devices not only capture high-quality images but also integrate reliably into MOSIP’s modular, standards-driven digital identity systems.