MACP – Lab Qualification Criteria (V1.0)

Enrolment Devices

DOCUMENT 3 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

Introduction

The issuance of identity is a complex process, and biometrics play a crucial role in establishing uniqueness in digital identity systems like MOSIP. The quality of biometric images captured greatly impacts the efficiency and effectiveness of deduplication and authentication functions. **To provide independent certification for biometric devices used in MOSIP systems, BixeLab has collaborated with MOSIP to develop a modular, globally adoptable biometric device certification framework**.

The framework aims to:

1. Provide standardised assessment criteria and standard operating procedures for testing biometric devices and solutions.
2. Establish standardised MOSIP biometric device certification programs that can provide independent certifications to MOSIP users.

MOSIP accredited laboratories will be utilised to certify that biometric devices meet MOSIP requirements for biometric quality. This document outlines the Laboratory Qualification Criteria that must be met by laboratories seeking MOSIP accreditation for biometric compliance testing. A council will review the records and documentation submitted during the certification process to verify that the criteria have been met. Accredited laboratories under the MOSIP Advanced Compliance Program (MACP) will produce a report certifying if the vendor has met the base requirements outlined in the MOSIP Biometric Device Certification Framework for Quality. The pre-requisites for biometric device providers and laboratories applying for MOSIP accreditation are listed in the respective documents.

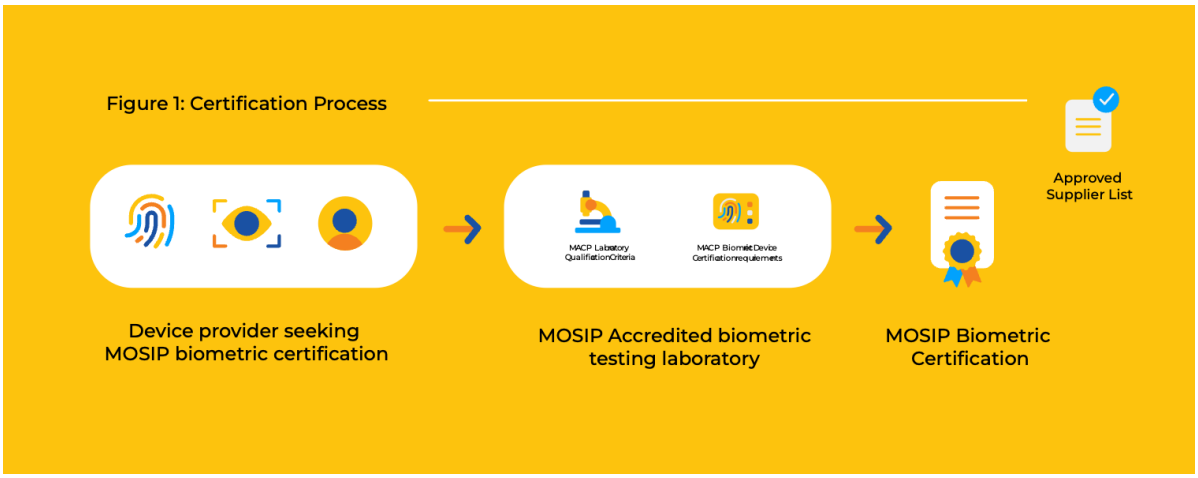
Significance of the Framework

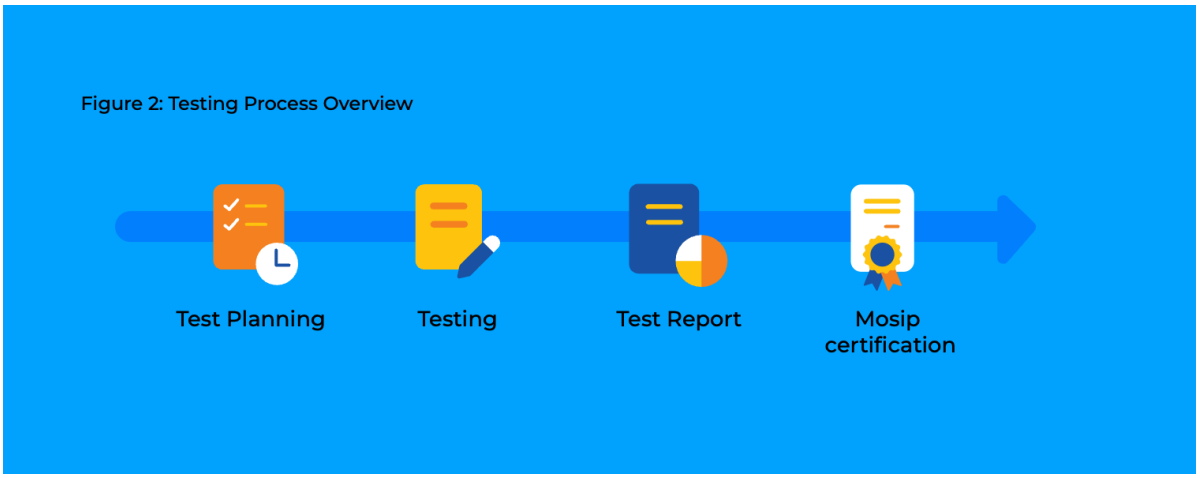
The MOSIP Advanced Compliance Program's certifications are independent from other certification programs and specific to the MOSIP framework and mission. Unlike other accreditation and certification programs that focus on mobile and financial transactions or have broader laboratory capabilities, MOSIP accreditation and certification are based solely on MOSIP's compliance requirements. There is an ongoing effort to create a global standard (IEEE P3167) based on the existing MOSIP standards which means that the scope of the certification can eventually spread on to non-MOSIP platforms as well.

Laboratories seeking accreditation under the MOSIP Advanced Compliance Program must demonstrate their ability to conduct biometric testing specifically designed to provide MOSIP adopters with confidence that the biometric technology they choose will meet their minimum performance requirements. However, it should be noted that the certification does not guarantee that the biometric devices are optimal for any particular use case in a country. Therefore, it is highly recommended to perform additional on-site operational testing to ensure that the devices meet local operational conditions and requirements.

Scope

This document provides a comprehensive overview of the laboratory accreditation criteria. The criteria have been designed to be both stringent and to allow a broader range of organisations to perform MOSIP compliance testing. Figure below provides an overview of the biometric device certification process under the MACP framework for quality testing.





Guidance

This section provides guidance for the laboratories seeking MOSIP Accreditation. In order to ensure that the testing methods used in the laboratory are adequate, it is important to assess the laboratory's qualifications. These criteria are designed to allow for a wider range of testing laboratories to participate. Other requirements are listed in the sections below.

The laboratory seeking MOSIP accreditation must meet the following pre-requisites:

Independence

To guarantee impartiality, the laboratory must be an independent entity with no conflict of interest. Some examples of conflict of interest are as follows:

- financial interests, personal/professional relationships, political or ideological beliefs, privacy/ethical concerns

Certification

To ensure that the methods used in the laboratory are adequate, it is essential to confirm that the laboratory is certified to either ISO/IEC 17025 or a relevant national body (e.g., NIST NVLAP). The validity of the certification must also be verified (ISO/IEC 17025 re-accreditation cycle is typically 3 years). [Note that MOSIP advisory committee will set MACP biometric re-certification cycles].

Well-being of Human Subjects

The laboratory should have policies and procedures in place to guarantee the well-being of human subjects during testing. Lab's policies and procedures for dealing with human test crew in a safe and ethical manner can be reviewed and approved by country specific ethics boards/ national review boards. Advisory council can review the approval letters received by the lab.

Biometric Expertise

The laboratory should collectively have a minimum of two years of demonstrated expertise in biometric evaluation. Technical experts as engaged by MOSIP admissions committee may verify the experience through interviews for example.

Proficiency in Testing

The laboratory must provide evidence of proficiency in standardised ISO compliant biometric testing and reporting.

Testing Capabilities

The laboratory must have the necessary testing capabilities for face, fingerprint, and iris modalities. The lab should be able to complete testing within the required timeline and have the necessary resources, personnel, and equipment to complete large-scale testing.

Documentation

The laboratory must have the necessary documentation to demonstrate compliance with MOSIP MACP requirements, that all testing is conducted according to applicable national legislation, and that all collected data is secure and protected.

Reporting

The laboratory should have the ability to provide timely, accurate, and transparent reporting. The lab should have the ability to provide detailed, comprehensive reports and reports that are compliant with applicable national legislation.

Laboratory Qualification Criteria

A laboratory must satisfy all of the following criteria in order to be officially allowed to conduct MOSIP accreditations. The criteria below must be supported by documented evidence, approved by the advisory council, and subject to an on-site inspection.

Key Considerations

- The laboratory must be able to demonstrate that the business is more than 1 year old.
- The management and ownership structure must be made known to MOSIP prior to accreditation of the laboratory.
- An accredited laboratory, in order to maintain its accreditation shall demonstrate periodically its technical capability and evaluation quality.

Technical Capability

The laboratory must demonstrate technical capability to conduct testing of biometric devices in the face, fingerprint, and iris modalities (new modalities will be added to the framework in future). This requires compliance with the following ISO/IEC programs and MOSIP specifications:

- ISO/IEC 19794 series (Biometric Specification – MOSIP Docs 1.1.5)
- ISO/IEC 29794-2:2017 (Biometric Sample Quality – Finger Image Data)
- ISO/IEC 29794-6:2015 (Biometric Sample Quality – Iris Image Data)
- ISO/IEC 29794-5:2010 (Technical Report for Biometric Sample Quality – Face Image Data)
- ISO/IEC 24358 (Specifications for face-aware capture subsystems)
- NFIQ 2 for enrolment and NFIQ 1 for authentication fingerprint devices
- ISO/IEC 19795-1:2021 (Biometric Performance Testing and Reporting)
- ISO/IEC 19795-2:2007 (Biometric Performance Technology and Scenario Testing and Reporting)

The laboratory must:

- provide evidence of having performed biometric device testing within the past two years.
- have a robust system in place for tracking and documenting test results.

Quality Assurance

The laboratory must:

- have accreditation from an internationally recognised national information security body based on ISO/IEC 17025 (testing).
- have an established quality management system to ensure consistent and reliable delivery of services.
- provide evidence of a nominated Quality Manager.
- have a process for continuous improvement of laboratory services.
- have an established asset management system.

Security

The laboratory must:

- demonstrate a secure environment for the testing of biometric devices, including:
    - Physical and logical security measures
    - Personnel background check policies
    - Confidential data protection practices
    - A laboratory security policy
- have a secure system for data management and storage.
- follow best practices for protecting biometric data and other sensitive information.

The laboratory must:

- be able to demonstrate compliance to information security management standards such as ISO/IEC 27001.
- Provide evidence of a nominated Quality Manager, and lab/security manager.

Regulatory Compliance

The laboratory must:

- demonstrate compliance with all applicable laws and regulations governing biometric device testing.
- provide evidence of having obtained all necessary certifications, licenses, and permits.

Staff Qualifications

The laboratory must:

- have at least three key personnel (senior responsible officer, quality manager, security/lab manager) with necessary qualifications and experience.
- have a lab personnel development plan in place.
- have a process for ongoing training and development of all lab personnel.

Resources

The laboratory must:

- have the necessary resources and equipment to carry out device testing and certification, including:
    - Laboratory structure and design area
- have a system for maintaining equipment and resources.
- have a system for tracking usage and performance of equipment.

Processes

The laboratory must:

- have clear processes for device testing and certification.
- have a system for monitoring and evaluating the effectiveness of processes.
- have a process for ensuring the accuracy and integrity of test results.

Cost

The laboratory must:

- have different pricing structures available.
- have a process for invoicing and payments.

Note: The MOSIP Advisory Committee may accept a biometric testing laboratory's prior accreditation from relevant international accrediting authorities, such as NIST under the National Voluntary Laboratory Accreditation Program or Fast Identity Online (FIDO) Biometric Component Certification program, as validation that the laboratory has met the requirements for MOSIP accreditation. In this case, the laboratory must provide proof of accreditation along with a traceability matrix that maps the MOSIP requirements to the specifications from the NIST/NVLAP or FIDO accreditation. This enables the laboratory to avoid the need to provide individual evidence for MOSIP accreditation.

Glossary

Biometric Device: A device used for capturing biometric data (e.g., face, fingerprint, iris) for the purposes of identity verification and enrolment.

Biometric Performance Testing: A standardised process for evaluating the accuracy and effectiveness of a biometric system in operational scenarios, following standards such as ISO/IEC 19795.

Biometric Sample Quality: The assessment of the quality of biometric data captured (e.g., fingerprint, face, iris) based on predefined criteria, such as ISO/IEC 29794 series.

Certification: The process by which an accredited laboratory verifies that a biometric device complies with the standards and specifications set forth by MOSIP or other regulatory frameworks.

Conformance Testing: Testing conducted to confirm that a biometric device meets the required technical standards and performance criteria for use in identity systems.

Enrolment: The process of capturing biometric data from an individual to create a template for future identification or verification in a system.

Failure to Enrol (FTE): The percentage of subjects for whom the system fails to generate a biometric template of sufficient quality during the enrolment process.

ISO/IEC 17025: An international standard specifying the general requirements for the competence of testing and calibration laboratories.

MOSIP (Modular Open-Source Identity Platform): A foundational digital identity system that enables countries to build robust, secure, and scalable identity solutions. The MACP framework is aligned with MOSIP's standards for biometric quality.

NFIQ (NIST Fingerprint Image Quality): A standardised metric used to evaluate the quality of fingerprint images to ensure they are suitable for use in biometric systems.

Presentation Attack: An attempt to use a fake or altered biometric sample (such as a fingerprint or face) to spoof a biometric system.

Scenario Testing: Testing that simulates real-world conditions to evaluate the performance and robustness of a biometric device under varied operational conditions.

Template Protection: Techniques used to safeguard biometric templates (e.g., encrypted data) to ensure the security and privacy of enrolled individuals.

Appendix

Draft Certification Letter Template

Certificate (Draft) of Conformity

MOSIP Advanced Compliance Framework (MACP)

Biometric Device Requirements for Quality

Certificate No.: _____

Device Provider:

Product:

Software Version:

Hardware Version:

Test Standards:

Test Standards version and year for release:

Validity Period: [The MOSIP admissions committee may require providers to undergo re-certification processes every 2 years. This serves as a checkpoint for the provider to confirm that no changes have been made since their previous certification].

This certificate of conformity attests that a sample of the product in question has been evaluated and found to be in compliance with MOSIP biometric device quality requirements. Technical report and documentation supporting this determination are available from MOSIP.

[Placeholder: description for the number of samples testing, and other necessary technical information required to provide clear and concise overview of the testing performed, methodology used, device profile information, and outcomes achieved].

Note that this certificate only covers the specific device and related version tested. The holder of this certificate may use this document to demonstrate conformity with MOSIP biometric compliance requirements.

[Placeholder: general URL for evaluated products]

Senior Responsible Officer

Date