नेपाल सरकार
गृह मन्त्रालय
राष्ट्रिय परिचयपत्र तथा पञ्जीकरण विभाग
(सामाजिक सुरक्षा शाखा)
फोन : ४४११५६१, ४४६४६८६, ४४६२०५६, ४२००८९५
फ्याक्स : ४२०००१४
सिंहदरबार काठमाडौं
Website : www.donidcr.gov.np
E-mail : info@donidcr.gov.np
ss@donidcr.gov.np

पत्र संख्या : २०८२/०८३
चलानी नं. :९१२

२०८२/१०/२०
ने.सं. ११४६ सिल्लागा २ द्वितीया, सोमबार ।

बिषय :- IRIS Device व्यवस्थापन सम्बन्धमा ।

श्री स्थानीय तह सबै ।

सामाजिक सुरक्षा भत्ता प्राप्त गर्ने लाभग्राहीहरुको पहिचान, दर्ता तथा नवीकरणलाई व्यवस्थित बनाउन राष्ट्रिय परिचय व्यवस्थापन सूचना प्रणालीसँगको अन्तर आवद्धतामार्फत जैविक प्रमाणीकरण (Biometric verification) मार्फत हुँदै आएको विदितै छ । भत्ता प्राप्त गर्ने लाभग्राहीहरु विशेषगरी ज्येष्ठ नागरिकहरुको हकमा औंठा छाप (Finger Print) बाट प्रमाणीकरण कार्य गर्न असहज भएको भनी कतिपय स्थानीय तहहरुबाट गुनासो आउने गरेको सन्दर्भमा IRIS Device मार्फत समेत प्रमाणीकरण (Verification) गर्नको लागि राष्ट्रिय परिचय व्यवस्थापन सूचना प्रणाली सुरक्षा मापदण्ड, २०८२ को अनुसूची २ मा स्वीकृत न्यूनतम मापदण्ड अनुसार देहाय बमोजिमको IRIS Device सम्बन्धित स्थानीय तहबाटै आवश्यकतानुसार खरिद, जडान तथा सञ्चालन गर्न विभागको मिति २०८२/१०/१९ को निर्णयानुसार अनुरोध छ।

देहाय:

IRIS

S.N.	Criteria	Value
1.	Image size	160*160 to 300*300 pixels
2.	Image format	JPEG/TIFF/PNG
3.	Compression Ratio	1:10
4.	Image Representation	Base 64 string
5.	Standard	ISO/IEC 19794-6:2011 or above
6.	Security Features	No catching and storage of the captured iris image in the device

नोट : VERSP-MIS प्रणालीमा IRIS Device जडान तथा सञ्चालन गर्न Device and Service Interface Specification for Biometric Device (IRIS) Integration संलग्न गरिएको छ । साथै यस सम्बन्धमा आवश्यक थप सहजीकरणका लागि विभागको सूचना प्रविधि शाखा तथा Vital Event Registration and Social Protection (VERSP-MIS) टिमसँग सम्पर्क गर्नु हुन ।

(जुना [illegible]का खत्री)
शाखा अधिकृत

Device and Service Interface Detail for Biometric Device (IRIS) Integration

Author:

Department of National ID and Civil Registration

Singahdurbar, Kathmandu

Document Release Version: 1.0

Date: 22nd January, 2026

Document Control

Attributes	Values
Title	Device and Service Interface Detail for Biometric Device (IRIS) integration
Author	Department of National ID and Civil Registration

Revision History

Version	Date	Changes	Status
1.0			

Table of Content

Introduction:

This document defines the technical requirements and standards for biometric device (IRIS) to be used for NID biometric verification of social security allowance receiving beneficiaries through VERSP-MIS. It covers the workflow, working mechanism, service interface specification for the development of client service, iris specification and vendor compliance requirement.

Background:

VERSP-MIS is a centralized online system that consists of two integrated systems

a. vital event registration
b. social security allowance distribution.

VERSP-MIS is integrated with National ID system for biometric verification of beneficiaries. Beneficiaries visit the ward office of local level to get enrolled or renewed for being eligible for accepting social security allowance. During enrollment/ renew beneficiaries biometric is captured using biometric devices (fingerprint, iris) and it is validated against the record saved in National ID system.

Problem:

a. There are lot of vendors and devices with different SDK and working principle to capture the biometric
b. It is time consuming for DoNIDCR to analyze the code, SDK of each vendor and integrate it in the system.

Solution:

a. DoNIDCR will develop a common device integration library and implement it in VERSP-MIS.
b. All vendors have to develop their client services according to the technical document provided by DoNIDCR (common library) to integrate with VERSP-MIS.

Section A: Technical Specification

a. Workflow:

The workflow of the integration service interface is as below:

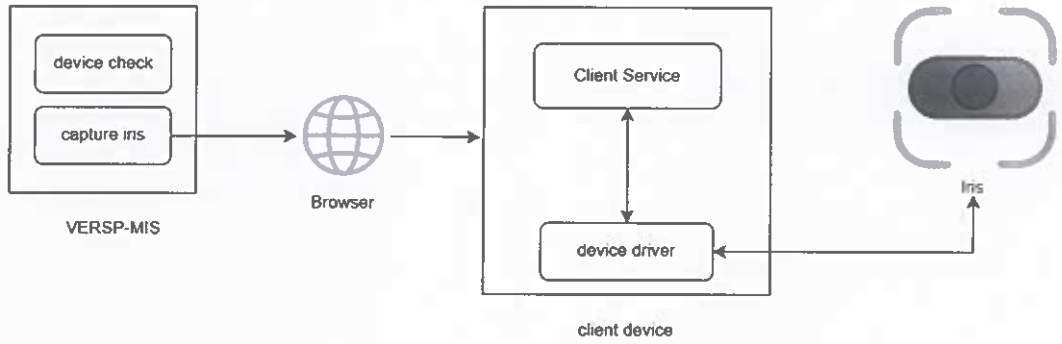

Fig: Overall workflow for the integration

Components:

A. VERSP-MIS: VERSP-MIS is a centralized online system that is being used throughout the nation for the purpose of social security allowance distribution. VERSP-MIS is integrated with National ID system for biometric verification of social security allowance receiving beneficiaries.
B. Browser: VERSP-MIS system is a web-based application which is accessed through DoNIDCR secure VPN using a web browser.
C. Client Device: It is a desktop/laptop device that will be used by local level user to access the VERSP-MIS.
D. Iris device: It is an iris scanning device that will be connected to the client device for capturing the iris.
E. Device driver: It is the device related driver software provided by the device manufacturer
F. Client service: It is a windows service that operates as an intermediary between biometric devices and the web-based application. These services act as a bridge between the physical hardware (connected via USB) and the web browser, which cannot access USB hardware directly for security reasons. The service runs a small local web server on the Windows machine, listening on a specific loopback port. The browser-based application sends an **HTTP POST or GET request** to http://127.0.0.1:[PORT]/endpoint or https://localhost:[PORT]/endpoint to access specified function and data from device.

b. Basic requirement:

1. Device supplier shall develop and provide a "client service Setup" to their clients.
2. Local level users shall install a client service setup provided by device vendor on the PC that has the Iris device connected.
3. After installation client service should be listed in the windows service list (services.msc) and it should run a lightweight web server (e.g., http://localhost: xxxx).
4. The service shall expose REST-based APIs for iris operations.
5. The service shall be developed to accept and return JSON response to a http request as specified in the Section A below.
6. If device is not able to capture biometric or any error occurs than it should return device specific error.
7. The quality and capture time will be set by DoNIDCR to support different type of devices and different qualities of beneficiaries biometric.

c. Working Mechanism:

1. Device Check:
   MIS user can check the device status to verify whether device is working and is ready to capture biometric. For this process user initiates, a request from VERSP-MIS, which will call the service endpoint and the service should provide appropriate response.

2. Biometric Capture process:
   a. Capture Request:
   When the service is running and device is functional, the MIS user will select the iris verification method and click on capture biometric button available in VERSP-MIS to initiates the biometric capture process.

   When capture button is clicked then application will trigger the service end points as described in the section below to capture the biometric of individuals.

   b. Request resolver:
   The device client services will be running in the client machine at XXXX port. So, when application sends (device check, capture) request to the service endpoints, it communicates with device and provide response accordingly. The request and response format is defined in the annex section.

3. Error handler: The client service should handle device related exception in an efficient manner and provide relevant error message. It should log exception in a file which will help to identify the root cause.

d. Iris Device Service Interface Specification

Basic Parameters:

a. The base URL: **http://localhost:9443**
b. Timeout: 15 sec

1. Get Device info:

This endpoint is called to fetch the information of the connected device.

Endpoint: baseurl/irisdeviceinfo
Method: Http Post
Data type: JSON

Request:
A HTTP post request must be made to the above endpoint.

Response:

```
{
  "status":"success",
  "message":"Device ready",
  "data": {
    "deviceType":"Dual Iris",
    "manufacturer":"ABC",
    "model":"ABC_123",
    "serialNumber":"xx123"
  }
}
```

Response parameters description:

Object	Element	Data type	Description	Possible values
	status	String	Response status	Refer to enum table
	message	String	Device related message	Refer to enum table
data	deviceType	String	The type of device	Refer to enum table
	manufacturer	String	Device manufacturer	ABC
	model	String	Device model	ABC_M40
	serialNumber	String	Device serial number	2213A

Ajax call sample:

Request:

```
$.ajax({
   url: "baseurl/irisdeviceinfo",
   method: "POST",
   contentType: "application/json",
   data: JSON.stringify({}),
   dataType: "json",
   success: function (res) {
      console.log("Device Info:", res);
   },
   error: function (xhr, status, error) {
      console.error("Error getting device info:", error);
   }
});
```

2. **Capture Iris**

Endpoint: baseurl/captureiris
Method: Http Post
Data type :Json

Request:
A HTTP post request must be made to the above endpoint.

Response:

```
{
  "status":"success",
  "message":"Iris captured successfully",
  "data": {
    "lefteyeBase64":"iVBORw0KGgoAAAANSUhEUgAA...",
    "righteyeBase64":"iVBORw0KGgoAAAANSUhEUgAA...",
    "qualityScore":88,
    "manufacturer":"ABC",
    "model":"ABC_123",
    "serialNumber":"xx123"
  }
}
```

Response parameters description:

Object	Element	Data type	Description	Possible values
	status	String	Response status	Refer to enum table
	message	String	Device related message	Refer to enum table
data	lefteyeBase64	String	Base64-encoded image data	
	righteyeBase64	String	Base64-encoded image data	
	qualityScore	String	numerical value indicating the quality of a captured biometric sample	
	manufacturer	String	Device manufacturer	ABC
	model	String	Device model	ABC_M40
	serialNumber	String	Device serial number	2213A

Ajax Call Sample:

```
$.ajax({
    url: "baseurl/captureiris",
    method: "POST",
    contentType: "application/json",
    data: JSON.stringify({}),
    dataType: "json",
    success: function (res) {
        console.log("Iris Capture:", res);
        if (res.data && res.data.imageBase64) {
            document.getElementById("irisImage").src = "" +
res.data.efteyeBase64;
        }
    },
    error: function (xhr, status, error) {
        console.error("Error capturing iris:", error);
    }
});
```

ENUM table:

1. status

SN	Values	Description
1	Success	If device is ready and functional to capture
2	Failure	If an error arise then it should be in failure status

2. message

SN	Values	Description
1	Device ready	if status is success
2	Capture timeout	If a quality iris cannot be captured in specified time
3	Iris Captured Successfully	If a quality iris is captured

3. deviceType

SN	Values	Description
1	single iris	Single iris scanner
2	dual iris	Dual iris scanner

e. Iris Device Specification

This specification is as per the "National Identity Card Management Information System Security Standard, 2082" of the Department of National Identity and Civil Registration. All devices must comply with this specification.

SN	Criteria	Compliance	Value
1	Image Size	Mandatory	160 x 160 to 300 x 300 pixels
2	Image Format	Mandatory	JPEG / TIFF / PNG
3	Image Representation	Mandatory	Base64 string
4	Standard	Mandatory	ISO/IEC 19794-6:2011 or above
5	Compression Ratio	Mandatory	1:10
6	Security Features	Mandatory	No caching and storage of the captured iris image in the device
7	Software	Mandatory	Drivers, client service
8	Documentation	Mandatory	Vendor should provide a document complying to all the terms in the disclaimer section

Section B: DoNIDCR Responsibility

1. **Development of VERSP-MIS system for IRIS integration**
   - DoNIDCR will develop all the required modules in VERSP-MIS which are needed for the purpose of capturing beneficiaries biometric as per the technical specification.
2. **Central Monitoring & Enforcement**
   - The Department of National ID and Civil Registration (DoNIDCR) shall continuously monitor biometric data transactions sent from client service software to the main server.
   - Monitoring shall include, but not be limited to:
     - data integrity validation,
     - transmission patterns,
     - anomaly detection,
     - unauthorized access attempts,
     - suspected data leakage or misuse.
   - If any security vulnerability, policy violation, or abnormal behavior is detected from a specific client service software instance, the Department shall have the authority to immediately disable, suspend, or block the concerned client service from communicating with the main server.
   - Upon such action:
     - biometric data transmission from the affected client shall be automatically rejected,
     - the client software shall not be permitted to resume operation until the vulnerability is resolved and formally approved by the Department.
   - The vendor shall cooperate fully with the Department during investigation, remediation of the client service software.
   - Any attempt to bypass monitoring, security controls, or disable enforcement mechanisms shall be considered a serious security violation and subject to legal and contractual action.

Section C: Security & Legal Compliance Requirements

1. **Biometric Data Storage Restriction**
   - The vendor developing the local client service for iris integration shall not store any biometric data, including iris images, iris templates, or derived biometric information:
     - on local disk,
     - in application cache,
     - in memory beyond the active processing session,
     - in logs or temporary files.
   - All biometric data shall be processed only in volatile memory and shall be permanently discarded immediately after successful transmission to the main system or upon failure.
2. **Access Control & Authorization**
   - The local client service shall accept requests only from authorized web applications.
   - Requests from unknown origins shall be rejected.
   - The service shall not provide any administrative or debug interfaces accessible to end users.
3. **Logging & Auditing**
   - The system shall not log biometric data or any information that can reconstruct biometric identity.
   - Logs, if maintained, shall be limited to operational events such as:
     - device initialization,
     - capture success/failure,
       - error codes (without sensitive data).
4. **Third-Party SDK & Vendor Responsibility**
   - The vendor shall ensure that the device SDK used does not internally store biometric data beyond the capture process.
   - Any SDK-level caching or persistence shall be disabled or explicitly documented and approved.
   - The vendor shall be fully responsible for compliance violations arising from SDK behavior.

5. **Data Retention & Disposal**
    - No biometric data shall be retained on the client machine after transaction completion.
    - In case of system crash or failure, the service shall ensure automatic cleanup of residual data upon restart.
6. **Inspection & Compliance Assurance**
    - The system shall be subject to security audit or inspection by the procuring public entity.
    - The vendor shall provide written assurance confirming non-storage and lawful handling of biometric data.
7. **Compliance with Laws of Nepal**
    - The vendor shall comply with all applicable laws, policies, and regulations of Nepal.

Additional Security & Performance Requirements

(Client Service Software – Iris Integration)

1. **Malware, Backdoor & Code Integrity**
    - The client service software shall not contain any backdoor, hidden functionality, malicious code, spyware, adware, or unauthorized remote access mechanisms.
    - The software shall not establish outbound network connections to any external servers, cloud services, or third-party systems other than the authorized backend system.
    - Any update mechanism, if provided, shall be disabled by default or subject to explicit approval by the procuring public entity.
2. **Resource Utilization & Performance**
    - The client service software shall consume minimal system resources and shall not degrade the performance of the host machine.
    - Under idle conditions, the service shall not exceed:
        - CPU usage beyond nominal background levels,
        - unnecessary memory allocation,
        - disk I/O operations.
    - The service shall activate device operations only upon explicit request from the web application.
    - The software shall not perform background scanning, polling, or data transmission without authorization.
3. **Network & Communication Restrictions**
    - The client service shall listen only on the specified loopback interface port (localhost) and shall not expose any public network ports.

4. **Operating System & Process Security**
   - The client service shall run with the least privileged permissions required for device operation.
   - The service shall not install additional software components without explicit consent.
5. **Stability & Fault Tolerance**
   - The client service shall handle device disconnection, failures, and errors gracefully.
   - In case of failure, the software shall release all device handles and memory resources.
   - The service shall not crash the host system or block other applications.
6. **Third-Party Components & Dependencies**
   - All third-party libraries and SDKs shall be free from known vulnerabilities.
   - The vendor shall disclose all third-party components used in the client service.
   - Deprecated or unsupported components shall not be used.
7. **Security Testing & Compliance**
   - The procuring public entity reserves the right to perform independent security audits, penetration testing, or code review.
   - The vendor shall rectify any identified security or performance issues at no additional cost.
8. **Vendor Accountability**
   - The vendor shall be fully responsible for any security breach, performance degradation, or system instability caused by the client service software.

Section D: Vendor Compliance Letter Format

To,

.....

.....

Subject: Vendor Compliance Declaration for Iris Biometric Client Service Software

Dear Sir/Madam,

We, **[Vendor Company Name]**, having our registered office at **[Company Address]**, hereby submit this Compliance Declaration in relation to the development, supply, and deployment of the **Client Service Software for Iris Device Integration** for the **..... (office name) municipality/rural municipality.**

We hereby confirm and declare that:

1. The client service software developed and supplied by us shall not store, cache, retain, or persist any biometric data (including iris images or templates) on the local machine, either temporarily or permanently.
2. The software shall be free from any backdoor, malicious code, spyware, adware, or unauthorized remote access mechanisms, and shall not contain any hidden or undocumented functionality.
3. The software shall not initiate any unauthorized outbound or inbound network communication, except for secure and explicitly authorized communication with the designated main server.
4. The software shall consume minimal system resources and shall not adversely affect the performance, stability, or security of the host system.
5. We acknowledge and accept that the Department of National ID and Civil Registration, ... (municipality/rural municipality) shall continuously monitor biometric data transactions, and in the event of any detected vulnerability, anomaly, or policy violation, the Department reserves the full right to disable, suspend, or block the concerned client service software without prior notice.
6. We further commit to fully cooperate with the Department, municipality/rural municipality in any security audit, inspection, investigation, or compliance verification, and to promptly rectify any identified issues at no additional cost.
7. We understand that any violation of this declaration may result in legal action, contract termination, and blacklisting, as per prevailing laws and government regulations.
8. The software shall comply with all applicable laws, rules, and policies of Nepal.

We hereby certify that the above statements are true, correct, and binding, and we accept full responsibility for compliance.

Yours faithfully,

For [Vendor Company Name]

Authorized Signatory: _____
Name: _____
Designation: _____
Signature & Seal: _____
Date: _____