Republic of Zambia

Name of the client: Smart Zambia Institute
Clarifications No. 01: Issue Date: 19 January 2026
Bid / Reference No. ZM-SZ-505117-GO-RFP
Name of the Request for Proposal (RFP): "System Integrator for Development, Deployment, Customization, and Integration of Foundational Digital ID, CRVS Core Modules Backend Infrastructure and Enrolment Kits"

Clarifications NO. No 01

Purpose: The purpose of this to provide responses to requests for clarifications that have been received regarding the above-referenced Request for Proposals.

Note to proposers: In providing the clarifications, please take note that in some certain existing provisions in the RFP have changed. Where a clarification only is provided, please note that the provisions of the RFP as issued remain unchanged.

Serial Number	Description of Query	CLARIFICATION/AMENDMENT
1.	SZI to consider broadening the RFP's technology requirements by allowing for "MOSIP or any other foundational ID platform based on open standards *or open source."*	Pursuant to **ITP 8 (Amendment of Request for Proposals Document)**, the Purchaser hereby notifies all Proposers of the following modifications to the procurement schedule and submission requirements: The Purchaser has amended "Section III – Evaluation and Qualification Criteria

		Factor - 1.4 Experience sub factor 1.4.2 "Specific Experience" Currently reading as in the words in italics as follows *"The contracts should include the following specific requirement: (a) MOSIP Certified firm that has successfully delivered at least one biometric-based project in the domain of Functional or Foundational Identity with demonstrable proof that the system is maintained with ongoing operational support."* The words in italics have been replaced with the following words which are in Italics: *"Proposers are free to use any proven foundational Identity Platform based on open standards. Proposers are not limited to MOSIP. However, proposers must be the patent holder or must have the legal right and authorization to use, customize, and deploy the proposed platform."*
2.	**PROPOSAL SUBMISSION TIMELINE** Various proposers have requested an extension of the proposal deadline submission.	Pursuant to **ITP 8 (Amendment of Request for Proposals Document)**, the Purchaser hereby notifies all Proposers of the following modifications to the procurement schedule and submission requirements: **Amendment of Proposal Deadlines and Submission Mode** 1. Section II - Proposal Data Sheet (PDS): ITP 23.1 and ITP 26.1 The deadline for Proposal submission and the scheduled time for the public opening of Proposals are hereby deleted and replaced with: • *"New Submission Deadline: February 5, 2026, at 10:00 hours CAT."* • *"New Proposal Opening Time: February 5, 2026, at 10:00 hours CAT. The location for submission and opening remains unchanged as specified in the original PDS."* 2. Section II - Proposal Data Sheet (PDS): ITP 7.1 The deadline for the submission of requests for clarification is hereby extended to *January 22, 2026.* 3. Clarification on Submission Mode Proposers are explicitly reminded that only physical submissions shall be permitted. Electronic or online submissions are not authorized for this procurement; any proposal received via electronic means will be deemed non-responsive and rejected.

3.	Most commercial fingerprint scanner SDKs support only Windows and Android OS and not IOS. We believe the kits are going to use laptops running on Windows OS, so we can safely assume iOS is not required. Please confirm	Pursuant to **ITP 8 (Amendment of Request for Proposals Document)**, the Purchaser hereby notifies all Proposers of the following modifications to the procurement schedule and submission requirements: The requirement is hereby **amended**. Support for **iOS** and **Linux** is removed from the operating system requirements.
4.	Suggestion: Intel Core 5, 10 cores, up to 5 Ghz. Better price performance ratio, energy efficient and well suited to the registration workloads. Can you confirm if this suggestion is acceptable?	Pursuant to **ITP 8 (Amendment of Request for Proposals Document)**, the Purchaser hereby notifies all Proposers of the following modifications to the procurement schedule and submission requirements: The Purchaser has amended "Section VII – Purchaser's Requirements, Biometric Enrollment Kit Requirement – 800 Qty, and under laptops specification currently reading as the words in italics, as follows. *12th Generation Intel® Core™ i7-1265U, 12 MB Cache, 10 Cores, up to 4.8 GHz, 15 W* The words in italics have been replaced with the following words which are in Italics: *New Minimume requirement is CPU: Ultra 7 155U Gen.14th, 12 MB Cache, up to 4.8 GHz, 12 Cores or higher* - The stated laptop specification is the minimum requirement. Bidders may propose higher-spec that meet or exceed mandatory requirements
5.	Suggestion: The purpose of the secondary screen is to display the demographic and other data to the user so that he can validate and confirm. For this purpose, the screen size of 12 inches and above is also suitable. This size can help make the kit much more compact, ease to carry and use. Can you confirm if this is acceptable?	Pursuant to **ITP 8 (Amendment of Request for Proposals Document)**, the Purchaser hereby notifies all Proposers of the following modifications to the procurement schedule and submission requirements: The Purchaser has amended "Section VII – Purchaser's Requirements, Biometric Enrollment Kit Requirement – 800 Qty, and under laptops- Secondary Display - specification currently reading as the words in italics, as follows *Connected as an accessory to allow the applicant see his/her information 14" FHD Secondary Monitor (Non-touch),* The words in italics have been replaced with the following words which are in Italics: *The requirement is hereby amended. size, a 13.3-inch or higher secondary display is acceptable.*

6.	Suggestion: Instead of ring light, a 6W LED assembly with top and bottom light provides the desired lighting to illuminate the face of the subject as well as offers compact assembly with the camera. We suggest that an integrated 6W LED assembly with top & bottom light should be permitted (& not just ring light form factor), as long as it offers and meets all functional requirements, please confirm	Pursuant to **ITP 8 (Amendment of Request for Proposals Document)**, the Purchaser hereby notifies all Proposers of the following modifications to the procurement schedule and submission requirements: The Purchaser has amended "Section VII – Purchaser's Requirements, One Ring Light - specification currently reading as the words in italics, as follows *Ring light of 6 watts, 1000 Lux at 50cm to 400 Lux at 1 meter (to illuminate the face in case the enrollment room is dark)* *USB* *4.1A / 5V DC drive current / input Voltage* *120 Degrees viewing angle* *a) On/off power and brightness settings* *b) Controllable by software* *c) PWM dimming method* *PWM dimming method* *Fully Integrated with the HD webcam* The words in italics have been replaced with the following words which are in Italics: *Type and capacity"Ring light of 5 watts, 1000 Lux at 50cm to 400 Lux at 1 meter (to illuminate the face in case the enrollment room is dark)* *Power source - USB* *Power input - "5V/1A DC drive current / input Voltage* *Viewing angle 120 Degrees viewing angle* *Adjustable settings "a) On/off power and brightness settings , b) Controllable by Manually or software"* *Integrations- Fully Integrated with the HD webcam*
7.	1. Is it mandatory to be accredited to MOSIP and Technical and Commercial Partner? 2. In case if the bidder is owner of the similar platform built on Open Source technology – will the bidder qualify for this criteria. 3. The Technical Partner – System Integration ensures the organization is qualified and capable of deploying MOSIP Platform.	**See item 1.** Following the Addendum, the solution requirement is amended to allow any proven Open-Standards platform. Bidder must provide Manufacturing Authorization for the proposed solution. If the bidder proposes MOSIP, they must submit valid MOSIP Technical & Commercial Partnership credentials. Other clarifications (e.g., 3-year minimum) are applicable for alternative open-source platforms.

	Hence we kindly request to relax this requirement to allow any of the Technical **OR** Commercial SI Partner MOSIP fairly new and have limited number of partners and most of them accredited recently. However, it doesn't mean these accredited partners are not capable of delivering the MOSIP deployment requirements. Hence we kindly request to relax the minimum 3 years of accreditation requirements.	**Requirement clarified per Addendum.**
8.	Instead of JV arrangements, can the bidder propose a consortium arrangement?	As this is a World Bank-funded project, the Bank specifically requires legally binding Joint Venture (JV) agreements to ensure accountability and joint & several liability of members. Consortium arrangements do not meet this legal and fiduciary requirement. **Requirement remains unchanged.**
9.	As the requirements and qualification/eligibility criteria are too many, Can this requirement be relaxed to allow more number of JV members to meet the eligibility criteria?	Limiting JV members to three ensures clear accountability, effective management, and alignment with World Bank procurement standards. Additional members could complicate contractual obligations and liability. **Requirement remains unchanged.**
10.	Kindly confirm if this requirement of evaluation should meet the contract value of USD 15 Million or more as per the eligibility criteria – Specific experience or can the bidder demonstrate any biometric based project reference which meets the specification as per the evaluation requirements but doesn't meet the USD 15 Million in case of one project/USD 8 Million two projects? Can this requirement be relaxed to allow if any JV member meets this requirement. We feel the requirement is overly stringent and restrictive, which may exclude many capable bidders from qualifying. This is likely to result in limited competition, contrary to the World Bank	The project scope is wide and includes multiple products. To ensure technical and financial capability, the lead bidder must meet the USD 15M criterion. Allowing JV members only without a strong lead could compromise delivery and risk management. **Requirement remains unchanged.**

	Procurement Guidelines that emphasize fair, open, and competitive procurement to achieve value for money. We request to relax this requirement to allow any JV member to meet this requirement instead only the lead bidder. The JV arrangement ensures all the members Jointly and severally liable incase of failure which protects the customer interest.	
11.	The explicit inclusion of electoral biometric systems with 25 Million biometric records as qualifying experience—while other large-scale functional identity systems are excluded—may unintentionally favor a limited set of vendors whose primary experience is in voter registration rather than foundational national identity. This could restrict competition without necessarily improving alignment with the project's national ID objectives. Hence we request to relax this criteria.	The current ABIS requirement is 15 million licenses, and the current population of Zambia is around 22 million, with an expected growth rate of 3+% per year. Considering the above, the lead bidder must demonstrate experience aligning with both current and future requirements. Electoral-specific relaxation is not applicable. This purchaser clarifies that the proposers experience should include large-scale deduplication and identity resolution for national foundational or national functional identity systems. **Requirement remains unchanged.**
12.	This requirement is more than the entire population of Zambia. Restricting the requirements to such a large database might restrict many of the capable bidders from qualifying. Hence we kindly request to relax these requirements.	The proposed solution targets a current population of approximately 22 million, with an expected growth rate of 3+% per year. The lead bidder must demonstrate experience handling databases of comparable scale and with capacity for future growth. This ensures the bidder has the knowledge and capability to support both present and future national ID requirements. The requirement ensures that the bidder has sufficient large-scale national identity experience. **Requirement remains unchanged.**
13.	1. Kindly clarify what exactly meaning of Contract withing last 7 years – Can the bidder provide a reference of the project prior to December 2018 but completed within last 7 years ie completed after December 2018? 2. As the requirements are very restrictive, kindly request to relax this requirements to)	SZI requires bidders with recent and verifiable experience to ensure lessons learned, technical relevance, and successful delivery. Extending the period risks including outdated experience that may not reflect current technology or operational standards. **Requirement remains unchanged.**

	contract within the last 15 Years (15) (December 2010) years	
14.	The eligibility criteria, when considered in totality, appear overly prescriptive and narrowly structured, with specific combinations of geographic scope, scale thresholds, MOSIP-specific requirements, and the explicit inclusion of electoral biometric systems alongside national identity systems. This combination is likely to favor a very limited and specific experience profile, resulting in only one or a few bidders qualifying and thereby restricting effective competition. This may be inconsistent with World Bank procurement principles that emphasize fair, open competition and value for money, and it is therefore suggested that the requirements be reviewed to avoid unintended bidder exclusion.	***Refer to Point 1****: The Addendum now allows any proven Open-Source Identity Platform. The requirements are designed to balance open competition with technical rigor and alignment with World Bank procurement principles. Requirement clarified as per Addendum.*
15.	Please clarify the scope and use case of document image scan using the web camera, considering the fact that there is a separate portable document scanner for scanning documents.	The requirement remains strictly as per the tender document. The Web Cam / Face Camera is intended solely for capturing the applicant's facial image, and document scanning shall be performed only by the dedicated document scanner provided as part of the kit. **Requirement remains unchanged.**
16.	The Foundation Trust Module is a MOSIP requirement for authentication devices. For registration equipment, FTM is not required. The registration devices should support host based security (SBI 1.0). Please confirm. Reference: https://docs.mosip.io/1.2.0/id-lifecycle-management/supporting-components/biometrics/biometric-specification	The device must mandatorily support Foundation Trust Module (FTM)–based hardware security. SBI 1.0–compliant host-based security must also be implemented. FTM establishes a hardware root of trust and enables secure boot. It protects cryptographic keys and prevents unauthorized tampering. Together, these ensure compliance with any open-source applications **Requirement remains unchanged.**
17.	The Foundation Trust Module is a MOSIP requirement for authentication devices. For registration equipment, FTM is not required. The registration devices should support host based security (SBI 1.0).	The device must mandatorily support Foundation Trust Module (FTM)–based hardware security. SBI 1.0–compliant host-based security must also be implemented. FTM establishes a hardware root of trust and enables secure boot. It protects cryptographic keys and prevents unauthorized tampering. Together, these ensure compliance with any open-source applications **Requirement remains unchanged.**

	Please confirm. Reference: https://docs.mosip.io/1.2.0/id-lifecycle-management/supporting-components/biometrics/biometric-specification	
18.	The Foundation Trust Module is a MOSIP requirement for authentication devices. For registration equipment, FTM is not required. The registration devices should support host based security (SBI 1.0). Please confirm. Reference: https://docs.mosip.io/1.2.0/id-lifecycle-management/supporting-components/biometrics/biometric-specification	The device must mandatorily support Foundation Trust Module (FTM)–based hardware security. SBI 1.0–compliant host-based security must also be implemented. FTM establishes a hardware root of trust and enables secure boot. It protects cryptographic keys and prevents unauthorized tampering. Together, these ensure compliance with any open-source applications **Requirement remains unchanged.**
19.	Please clarify the requirement for a display on a fingerprint scanner. There are LED indicators on the fingerprint scanner to guide positioning of fingers. Please confirm if this is what is required or should this requirement be discarded. Please, confirm that LFD acronym corresponds to Live Finger Detection which is a normal requirement for fingerprint readers	The display/screen requirement for the fingerprint scanner includes visual guidance mechanisms such as LED indicators or an equivalent interface to assist users in correct finger placement, and therefore this requirement shall not be discarded. Additionally, the acronym LFD refers to Live Finger Detection, which is a standard and mandatory requirement for fingerprint scanners to prevent spoofing and ensure secure and reliable biometric capture. **Requirement remains unchanged.**
20.	This requirement for tri-color LEDs is proprietary; normally commercial scanners support LED based indicators but not necessarily in 3 colors. Please confirm that using LED indicators for user guidance is enough to meet this requirement or if a specific fingerprint reader is selected, then please confirm the fingerprint reader required that meets this requirement.	The requirement remains unchanged. The intent of the tri-color LED requirement is to ensure clear and effective visual guidance to the user during fingerprint capture (for example, indicating ready, capture in progress, or error conditions). The specification does not mandate a specific fingerprint reader model or brand; any commercial fingerprint scanner that provides equivalent LED-based visual indicators fulfilling this functional intent shall be considered compliant. **Requirement remains unchanged.**
21.	Could you please confirm whether it should say instead: 13.5 cm - 14.5 cm (5.3 inches -5.7 inches)	The specified dimension range of 13.5 cm – 14.5 cm (5.3 inches – 5.7 inches) is correct and should be retained as stated. **Requirement remains unchanged.**

22.	As the kit we intend to supply already has an internal Battery Management System that is connected to mains and on the other side supplies DC current to the USB Hub, the external power adapter would be redundant. Could you please confirm that in this scenario it would not be necessary to include the External Power Adapter?	The requirement for the external power adapter remains unchanged. However, in the scenario described, where the kit already includes an internal Battery Management System (BMS) that connects to mains power and supplies DC current to the USB hub, the external power adapter may not be necessary for operation. The key intent of the requirement is to ensure reliable and uninterrupted power to all kit components; as long as the internal BMS provides equivalent functionality and meets safety and operational standards, it would satisfy the purpose of the external power adapter requirement. **Requirement remains unchanged.**
23.	We will include a reliable USB hub proved among several deployments with thousands of kits. Could that USB Hub be accepted? Please confirm which rating agency the 5-Star rating review is available on, as it is a specialized hub manufactured for these kits.	The requirement for a reliable USB hub remains unchanged. The proposed USB hub can be accepted provided it meets the functional and reliability requirements outlined in the tender, as demonstrated in previous deployments. Regarding the 5-star rating, the specific rating agency or platform is not mandated; the purpose of mentioning a high rating is to ensure proven performance and reliability in real-world usage. **Requirement remains unchanged.**
24.	Could you please confirm that the paper width required for the printer is 57.5 ± 0.5mm?	The requirement remains unchanged. The paper width for the printer is confirmed to be 57.5 ± 0.5 mm as specified. **Requirement remains unchanged.**
25.	Is a speed of 80 mm/s accepted for this printer considering that it is what most commercial printers come with? If not, please confirm exactly which printer you are requesting as the requirement is very specific.	The requirement for a 100 mm/s printer speed is specified to ensure efficient and timely printing during large-scale operations. In enrollment or verification scenarios, high-speed printing reduces wait times for users, supports continuous operation without delays, and ensures that the kit can handle peak workloads effectively. **Requirement remains unchanged.**
26.	Usually, either USB or RS232 interface is available in a thermal printer, while USB is the most common and recommended. Could you please confirm whether USB is enough? It, please confirm exactly which printer you are requesting as this requirement is very specific.	The requirement is accepted with **either** connectivity through USB. While the tender mentions USB, RS232, and Bluetooth, USB is the most common and recommended interface for thermal printers and is sufficient to meet the functional and operational requirements specified. There is no need to mandate RS232 or Bluetooth as long as the USB interface reliably supports all intended printer operations. **Requirement remains unchanged.**
27.	Please confirm if the following paper thickness is acceptable: 0.055-0.12mm . Please confirm if 1500 mAh battery capacity is acceptable. If not, please confirm exactly which printer you are requesting as the requirement is very specific.	The requirement remains unchanged. - "Thermal Printer Paper Thickness: 0.06mm~ 0.015mm Battery: DC7.4V, 1600mA, Rechargeable Li-ion battery" **Requirement remains unchanged.**

28.	Suggestion: Most commercial laptops today do not come with an in-built 4G/5G modem, and the ones that do are very expensive. Moreover, for enterprise data applications, 4G connectivity provides the best coverage as well as price performance. We suggest that Laptop should offer WiFI and BT connectivity. A separate 4G USB modem can be provided that can be connected to the kit securely and ensures ease of SIM provisioning. Can you confirm that this is acceptable?	Considering that the proposed hardware is expected to be used for the next 5 to 7 years, the specification remains as stated to ensure future readiness and long-term usability. The laptop must support an internal broadband modem with 3G, 4G, and 5G network compatibility, along with Wi-Fi and Bluetooth connectivity. This requirement ensures reliable operation across evolving network environments, backward compatibility in areas with limited coverage, and sustained performance over the entire lifecycle of the equipment. **Requirement remains unchanged.**
29.	Minimum optical resolution of 2592*1944 pixels will provide a 5MP camera resolution. However, the image sensor spec mentions 8MP resolution also. Please confirm the minimum resolution that should be considered.	The portable document scanner must have a minimum optical resolution of 2592 × 1944 pixels and a minimum 8 MP CMOS image sensor with integrated LED. The optical resolution defines the effective capture quality, while the 8 MP image sensor requirement ensures sufficient sensor capability for clarity, accuracy, and future-proof performance. Both specifications are mandatory and must be met. **Requirement remains unchanged.**
30.	Please confirm if the maximum document size is upto A4 or legal/A3 size is also required to be scanned?	The Specification is scanner should support up to A4 and Legal size **Requirement remains unchanged.**
31.	1. Swapping out batteries places a technical load on the registration operator as well as leads to reduced efficiency of registration operation, if swapping out is required during the day. We recommend one single power management system with 60Ah battery that can last more than a full day of operation, 8h and can be charged easily from outside the case without needing any operator intervention to connect/disconnect batteries. Please confirm this is acceptable? 2. Charging option: As we suggest a single 60 Ah battery, the charging time to charge a single battery of 60Ah is minimum 6 hours for fully charging the battery from mains, please confirm this is acceptable? 3. We suggest a single battery of 60Ah capacity and therefore the requirement to deploy 2 batteries can be removed. This will reduce the complexity of the	The purchaser clarifies: 1.A single, integrated power management system with a 60 Ah battery capable of supporting at least 8 hours of continuous operation is acceptable, as it improves operational efficiency and avoids the need for battery swapping during the day. External charging without operator intervention to connect or disconnect batteries is also acceptable. 2. Charging option: Battery system should be minimum of 60 Ah, and up to 8 hours of operation a day. 3. The requirement to deploy two separate batteries is removed. A single 60 Ah battery solution is acceptable, provided it meets the stated operational endurance and reliability requirements. 4. Rugged aluminium Design capable of withstanding a 1.5m drop test 5. The USB output is provided via an integrated, battery-powered USB hub; the battery itself does not have dedicated USB ports, similar to an external power bank. 6. The input and output voltage/current specifications as suggested (Input: 12–18V; Laptop Output: 19.5–19.8V DC ≤4A; Printer Output: ≤2A) are accepted and comply with the requirement. 7. The battery dimension requirement is hereby removed. Bidders shall propose battery

	operation and maintenance load as stated in point 1 above, please confirm this is acceptable? 4. As a single battery can be well integrated into the kit, the IP67 case provides protection to all components including battery drops. So, a separate requirement for 1.5m drop for the battery can be removed. 5. The USB output is provided through an integrated hub, which is powered by the battery. There are no dedicated USB ports on the battery itself (unlike an external powerbank) 6. Suggested input & output voltages: Input Source 12~18V, Output Laptop Voltage 19.5 ~ 19.8V DC Output Laptop Current ≤4A Output Printer ≤2A 7. The specific battery dimensions are proprietary and should be removed, otherwise please confirm exactly what battery you are wanting as the requirements are very specific? 8. The display unit could be LCD or LED with main function to show the charging status 9. We suggest 5m cable as that should be sufficient length for most use cases. 10m is too long and would make the kit bulky and the cable difficult to manage.	specifications and dimensions based on their respective solution designs, provided that overall functional, performance, and safety requirements are fully met. 8. charge indication via status LEDs 9. The requirement of a 10-meter power cable shall remain unchanged. This is to ensure that the MEK can be connected to the nearest available power outlet in various deployment environments without operational constraints. The requirement must therefore be maintained as specified in the tender. 10. Surge adapter and charge regulator Maximum support power 180W **Requirement remains unchanged.**
32.	What is the expected number of identities to be managed by the Digital ID system at go-live?	At go-live, the Digital ID system is expected to manage a minimum of 15–20 million identities, as per the requirement, and is designed to scale seamlessly to accommodate future growth. **Requirement remains unchanged.**
33.	Is there a defined target for Digital ID coverage (population size or percentage) within the contract duration?	The target for Digital ID coverage within the contract duration is to cover the complete Zambian population, with the system designed to support full national enrollment and future population growth. **Requirement remains unchanged.**
34.	Are all Digital ID components (CRVS, ABIS, Digital ID Wallet, Authentication, Integrations) expected to go live simultaneously, or can some be phased post-go-live?	All Digital ID components—CRVS, ABIS, Digital ID Wallet, Authentication, and Integrations—are expected to go live simultaneously, with no phased or post–go-live rollout. **Requirement remains unchanged.**

35.	Is there a standard, government-approved state workflow already defined for Digital ID?	The project will be expected to follow the defined standard workflow that has been formally approved by the Government of Zambia or the responsible authority. **Requirement remains unchanged.**
36.	Should Digital ID workflows be uniform nationwide, or configurable by region, office type, or registration channel?	Digital ID workflows shall be uniform nationwide, following a single, government-approved national workflow applicable across all regions, office types, and registration channels, ensuring consistency, standardization, and regulatory compliance at a national level. **Requirement remains unchanged.**
37.	Confirm that Digital ID issuance in this RFP is digital-first, and that physical ID card production is out of scope for the current procurement?	Digital ID issuance under this RFP is digital-first, and physical ID card production is explicitly out of scope for the current procurement. **Requirement remains unchanged.**
38.	Confirm that web-based Digital ID Wallet sufficient for citizen access for the current procurement?	Refer to Section VII. The RFP scope is clearly defined and comprehensively covers all required components and functionalities as specified, with no ambiguity or additional scope beyond what is explicitly stated in the RFP. **Requirement remains unchanged.**
39.	Is there an estimated number of systems/ relying parties expected to integrate with Digital ID during Phase 1?	The vendor clarifies that a minimum of Five (5) systems integrated through an Application Programming Interface (API) during the kick-off phase. **Requirement remains unchanged.**
40.	Is there a predefined list of government agencies, banks, or telecoms expected to integrate during the initial rollout?	There is no predefined list at this stage. During implementation, Smart Zambia Institute (SZI) will share the required information, including the list of government agencies, banks, and telecom operators to be integrated as part of the initial rollout. **Requirement remains unchanged.**
41.	Is a national Government Service Bus/API Gateway already operational, or is the SI expected to provision and configure this capability?	The SI is expected to propose and implement an integration layer (API Gateway and related security controls) required for INRIS (CRVS + NID) and its external integrations. Where an existing national GSB/API Gateway is available and approved for use, the solution should be designed to integrate with it; otherwise, the SI should provision and configure an equivalent capability within the project scope. **Requirement remains unchanged.**
42.	What languages are expected to be supported in the first release?	English **Requirement remains unchanged.**
43.	What is the anticipated number of enrolment centres and mobile units to be implemented at go live and at scale?	The anticipated number of enrolment centres and mobile units to be implemented at go-live and at scale will be provided during the implementation phase, based on the final rollout plan and operational requirements. **Requirement remains unchanged.**

44.	Has an assessment been done on the quality and completeness of legacy identity and CRVS data to be migrated?	At this stage, no formal assessment has been completed on the quality and completeness of legacy identity and CRVS data. The successful bidder will be provided with the complete existing data and will be responsible for conducting a detailed data quality and completeness assessment as part of the project. **Requirement remains unchanged.**
45.	Is the expectation to migrate all historical identity records, or only active/current records?	The expectation is to migrate all historical identity records, not just the active/current records, ensuring continuity, completeness, and integrity of the national Digital ID database. **Requirement remains unchanged.**
46.	How is the administrative structure of Zambia organized from the highest to the lowest level? Could you provide a brief description of each level?	During the project kick-off, the information on the administrative structure of Zambia—from the highest to the lowest level—will be provided **Requirement remains unchanged.**
47.	What roles do local government units play in the administrative process, especially related to civil registration and vital statistics?	During the project kick-off, the information on the roles of local government units in the administrative process, including their responsibilities related to civil registration and vital statistics, will be provided
48.	Could you describe the flow of administrative and statistical data within the current system? How is this data collected, stored, and used at various administrative levels?	During the kick-off, the flow of administrative and statistical data within the current system, including how it is collected, stored, and used at various administrative levels, will be discussed **Requirement remains unchanged.**
49.	What mechanisms are currently in place for communication and coordination between different levels of administration?	During the kick-off, the mechanisms currently in place for communication and coordination between different levels of administration will be discussed
50.	How do CRVS offices manage their records and data? Are there specific systems or databases currently in use?	CRVS offices currently manage records using a mix of administrative processes and record-keeping methods that may vary by location and level (district vs. central). This can include paper-based registries, locally maintained electronic records, and inputs from sector systems (e.g., health facilities) where available. At this stage, the Purchaser is not prescribing a specific legacy CRVS software system or database that must be retained. Bidders should assume a mixed "as-is" environment and propose: ● an inception assessment of current record management practices, ● a data migration and digitization strategy (including scanning/indexing where required), and ● an approach to ensure continuity of operations during transition into the proposed INRIS CRVS solution. **Requirement remains unchanged.**

51.	How accessible are CRVS offices to the public? What services are most frequently requested by the public?	CRVS services are provided through a network of civil registration offices that serve citizens primarily via walk-in/in-person support, with varying levels of accessibility depending on geography and staffing. Public demand most frequently centers around: ● Birth and death registrations (including late registrations) ● Certificate issuance (new copies, duplicates, certified copies/extracts) ● Marriage-related services (registration and certificates) ● Corrections/amendments due to errors or legal updates ● Record search/verification for administrative and service-delivery purposes Bidders should propose an approach that supports efficient service delivery at registry offices, enables case/queue-based processing, and provides optional digital service channels where feasible, while ensuring inclusion for citizens who rely on in-person services. **Requirement remains unchanged.**
52.	How are health facilities distributed across different regions in Zambia ? Are there areas with limited access to these facilities?	Zambia's health facilities are distributed nationwide across urban, peri-urban, and rural areas, typically with higher concentration and service breadth in major towns/cities, and more dispersed primary-level facilities (health posts/centres) in rural settings. As in many countries, access is not uniform: some communities—especially in more remote or sparsely populated areas—face longer travel times and limited transport connectivity, which can affect timely access to facility-based services. Available sector summaries indicate that Zambia has a large national footprint of public and private facilities, with a significant share located in rural areas. However, physical presence of facilities does not always translate to easy access for all households, and distance remains a known barrier in remote settings (e.g., studies on rural access and distance to essential obstetric services). **Requirement remains unchanged.**
53.	Specifically, what roles do these health facilities play in the civil registration and vital statistics system? Are they directly involved in the registration of births and deaths?	Health facilities typically play a frontline "notification and certification" role in the CRVS ecosystem, because a significant share of births and deaths occur in or are first confirmed by health services. In general, health facilities may be involved in CRVS in the following ways: ● Birth notification: Recording the birth event at the facility and issuing a birth notification/attestation that feeds into the CRVS registration process. ● Death notification and medical certification: Confirming the death and producing the medical cause of death (MCCD) documentation, which is an important input for both legal registration and vital statistics. ● Data quality and completeness: Capturing accurate clinical and demographic details at source, which reduces errors and supports timely registration.

		● Statistical reporting: Providing structured data that supports national vital statistics (e.g., facility births/deaths, causes of death), either directly or through integration with a health information system. Whether facilities are directly performing the legal registration (i.e., acting as registration points) can vary by policy and operational model: ● In some models, facilities only notify and the CRVS office completes the legal registration and certificate issuance. ● In other models, facilities can host delegated registrars or be enabled as registration points, with final validation/approval performed by CRVS. **Requirement remains unchanged.**
54.	What procedures are currently in place for collecting and reporting birth and death data at these facilities? How is this data transmitted to CRVS offices?	Procedures for collecting and reporting birth and death information at health facilities generally follow a standard facility workflow (clinical record → notification/certification → reporting), but the exact operational practice can vary by facility type and location. In general terms: ● Births: Facilities record birth details in their maternity/labour registers and issue a birth notification/attestation. Basic demographic details (mother, newborn, place/time of birth) are captured at the point of service. ● Deaths: Facilities record deaths in inpatient/outpatient registers and prepare a medical cause of death certification (where applicable), along with a death notification for legal registration and statistics. Transmission to CRVS offices commonly occurs through one (or a combination) of these methods: 1. Paper-based submission: Periodic delivery of notification forms/medical certificates to the relevant CRVS office (by the family, facility staff, or designated courier). 2. Assisted entry at CRVS: CRVS offices receive paper notifications and enter them into their systems/registers. 3. Digital transmission (where available): Facilities transmit notification data electronically via a health information system or a secure digital channel to CRVS (email/portal/API), depending on facility capability and connectivity. **Requirement remains unchanged.**
55.	What technological resources do health facilities have access to for reporting vital events? Are these systems integrated with the national CRVS system?	Technological resources across health facilities are not uniform and generally vary by level of care (hospital vs. health centre/post), location (urban vs. rural), staffing, and connectivity. In practice, facilities may have access to some combination of: ● Basic ICT equipment: desktops/laptops, printers/scanners, and intermittent internet access (more common in higher-level facilities).

		● Mobile devices/tablets: used in some programmes for service delivery and reporting where available. ● Facility registers and local systems: ranging from paper registers to basic electronic tools, depending on maturity. ● Health information systems (where deployed): which may capture birth/death-related clinical data (including medical certification of cause of death) and can be leveraged as a source for CRVS notification. Regarding integration: existing integration with a national CRVS system is not assumed to be comprehensive or consistent across all facilities. Bidders should therefore assume a mixed landscape and propose: ● an interoperability approach (APIs/adapters, secure data exchange, standards where feasible), ● support for both electronic and paper-assisted notification pathways, and ● an incremental rollout plan that accommodates facilities with limited equipment or connectivity (store-and-forward / offline-first where needed). **Requirement remains unchanged.**
56.	How do health facilities collaborate with other government agencies or international organizations in terms of data sharing and CRVS processes?	Health facilities typically collaborate with other government agencies and (where applicable) international partners through policy-driven and programme-driven reporting and data exchange arrangements. This collaboration can occur at different levels: ● Government agencies (national/sub-national): Facilities routinely share aggregated and case-level information with relevant ministries and agencies (e.g., health authorities, statistics offices, local administration), primarily to support service delivery management, public health surveillance, planning, and reporting. ● Civil registration authorities: Facilities may share birth and death notifications and, where applicable, medical certification of cause of death, to support legal registration and vital statistics. ● National statistics functions: Data relevant to vital statistics may be shared in aggregated form for inclusion in official statistical publications and planning cycles. ● International organizations and donor programmes: Where specific programmes exist (e.g., maternal/child health, mortality surveillance, digital health strengthening), facilities may provide data extracts or reports under agreed governance frameworks, typically via the Ministry of Health or designated national coordinating bodies. **Requirement remains unchanged.**

57.	Who are the key stakeholders involved in the CRVS processes at various administrative levels (national, provincial, district, community)	CRVS delivery typically involves a multi-stakeholder chain across national, provincial, district, and community levels. While exact structures and titles may vary, bidders should assume the following stakeholder categories are involved: National level ● Civil Registration Authority / Central CRVS Department (policy, standards, central registry oversight, approvals for exceptional cases, national reporting) ● Ministry responsible for Home Affairs / Internal Administration (governance, legal oversight, identity linkages where applicable) ● Ministry of Health (birth/death notification policy, medical certification of cause of death, facility workflows) ● National Statistics Office (vital statistics production, statistical standards, analytics/reporting requirements) ● National ICT / eGovernment authority / data centre operator (hosting, cybersecurity, integration standards, infrastructure operations) ● Legal/Judicial authorities (court-ordered amendments, adoption/divorce processes, legal validation where required) Provincial / Regional level ● Provincial CRVS supervisory offices (oversight, performance monitoring, escalations, quality assurance) ● Provincial Health Offices (health facility supervision, compliance with notification/certification practices) ● Regional ICT support units (connectivity, equipment support, user support escalation) District level ● District Civil Registry Offices / District Registrars (primary service delivery, verification, approvals, certificate issuance where delegated) ● District Health Offices & facility management (operational coordination for notifications, data quality) ● Local government administration (community coordination, outreach, referrals, service access support) Community level ● Community health workers / facility outreach teams (notification support, awareness, referral, follow-up) ● Traditional/community leaders (supporting notification in customary contexts; referrals; awareness) ● Gazetted officials / authorized notifiers (e.g., for marriages or specific declarations,

		depending on policy) ● Citizens/informants (parents/guardians, next of kin, witnesses—who initiate or support registration requests) **Requirement remains unchanged.**
58.	What specific roles and responsibilities do these stakeholders have in the management and operation of the CRVS system?	CRVS stakeholders typically have the following core responsibilities: ● Central/National CRVS authority: Sets policy and standards, owns the central registry, oversees quality and national reporting, approves exceptions. ● Provincial/Regional supervisors: Monitor performance and compliance, handle escalations, support training and quality assurance. ● District registrars/offices: Deliver services to the public—receive notifications/applications, verify data/documents, approve cases, issue certificates, manage corrections and customer support. ● Health facilities & health authorities: Capture and notify births/deaths, provide medical certification (especially cause of death), ensure timeliness and data quality. ● Statistics office: Defines vital statistics outputs and uses CRVS data for official statistics and feedback on data quality. ● ICT/data centre authority: Hosts and secures the platform, manages operations (backup/DR, monitoring), and supports integrations. ● Courts/legal actors (where applicable): Support/approve legally driven changes (e.g., adoptions, divorces, court-ordered amendments). **Requirement remains unchanged.**
59.	What levels of access and permissions are required for each stakeholder role within the CRVS system?	Bidders should propose a role-based access control (RBAC) model with least-privilege, full audit logging, and separation of duties. Typical access levels include: ● National CRVS Admin (Central): Configure workflows/forms/templates; manage users/roles; view national dashboards; approve exceptional cases; no direct editing of records without workflow controls. ● Central Approver/Validator: View and validate cases escalated from districts; approve/reject; issue/authorize certificates; run national reports. ● Provincial Supervisor: Read-only access to provincial records + performance dashboards; manage escalations; limited approval if delegated. ● District Registrar/Officer: Create and update cases in assigned jurisdiction; verify documents; approve within delegated limits; issue certificates; initiate corrections. ● Data Entry / Front Desk (District): Capture applications/notifications and scan/upload documents; cannot approve or issue certificates. ● Health Facility Notifier: Submit birth/death notifications and supporting medical

		documents; track status; cannot legally register/approve unless explicitly delegated. ● Statistics User (CSO): Access to aggregated/anonymized datasets and dashboards; restricted access to identifiable records. ● Legal/Court User: Limited access to view relevant cases and upload court orders; approve legal amendments where required. ● Auditor: Read-only access to records, workflows, and immutable audit trails; export audit logs. ● System/IT Operator: Infrastructure monitoring and technical admin; no access to personal data content beyond what's required for operations. Bidders should also include field-level permissions (e.g., who can view/edit sensitive attributes), jurisdiction-based access (district/province), and delegation/temporary access controls. **Requirement remains unchanged.**
60.	What payment methods are currently supported for CRVS-related fees (credit/debit cards, bank transfers, mobile payments)?	CRVS fees are expected to be payable through multiple channels to ensure accessibility, including counter payments, bank-based payments/transfers, mobile payments, and card payments where feasible. The Purchaser prefers solutions that can integrate with Government of Zambia digital payment capabilities (where applicable), and bidders should therefore design the payments component to be gateway-agnostic and pluggable (API-based), supporting configurable providers and full receipting, reconciliation, and audit trails. Detailed integration specifications (APIs, security requirements, settlement/reconciliation formats, onboarding steps) for any preferred government payment gateway/provider will be shared with the successful bidder during implementation / integration planning. **Requirement remains unchanged.**
61.	Are there preferred payment gateway providers? If so, what are their integration specifications?	At this stage, no specific payment gateway provider is prescribed by the Purchaser. Bidders should propose a solution that supports integration with multiple standard payment gateways using secure, API-based interfaces, with the final provider(s) and specifications to be confirmed during implementation. **Requirement remains unchanged.**
62.	What is the fee structure for various CRVS services, including late registration? Are there different rates for different services or penalties?	The fee structure for CRVS services (including any charges for certificates, searches, corrections, and late registration) is governed by applicable laws/regulations and administrative directives, and may vary by service type and case category (e.g., normal vs. late registration). At this stage, bidders should assume: ● Different services may have different fees (and some services may be free depending on

		policy), and ● Late registrations may attract additional requirements and/or penalties as defined by the relevant legal framework. Bidders are expected to propose a system that supports configurable fee schedules (by service type, time thresholds for late registration, exemptions/waivers where applicable), along with receipting, audit trails, and reconciliation. Final fee tables and penalty rules will be confirmed and configured during implementation in consultation with the Purchaser. **Requirement remains unchanged.**
63.	What are the expected application loads (number of users, transactions per second)?	At this stage, the Purchaser has not defined fixed application load metrics such as number of users or transactions per second. Bidders should propose a scalable architecture based on reasonable assumptions, with detailed load profiling and capacity planning to be finalized during the inception and kick-off phases. **Requirement remains unchanged.**
64.	Can we obtain the current blueprint of the infrastructure setup? Ex: Network Design, Server Connectivity –	During the kick-off, the current blueprint of the infrastructure setup, including network design and server connectivity, will be discussed. **Requirement remains unchanged.**
65.	Are there any limitations or challenges in your existing infrastructure setup? Ex: Network Bandwidth, Firewall restriction, Internet connectivity,	During the kick-off, any limitations or challenges in the existing infrastructure, such as network bandwidth, firewall restrictions, and internet connectivity, will be discussed. **Requirement remains unchanged.**
66.	Please provide details on backup procedure?	During the kick-off, details on the backup procedures and processes will be discussed
67.	2.1 General requirements and capabilities Please confirm if the Face camera also need to scan document because there is already a dedicated Document scanner as part of the kit	The requirement remains strictly as per the tender document. The Web Cam / Face Camera is intended solely for capturing the applicant's facial image, and document scanning shall be performed only by the dedicated document scanner provided as part of the kit. **Requirement remains unchanged.**
68.	2.6 Image Quality Confirm 250 pixels at 120cm is acceptable	The requirement remains strictly as per the tender document **Requirement remains unchanged.**
69.	2.10Device flexibility Confirm the adjustability should include Height /Pan and Tilt adjustments	Yes. The adjustability requirement includes height, pan, and tilt adjustments to enable capturing the registrant's image from the required direction, as specified in the tender document. **Requirement remains unchanged.**
70.	2.11 Security What is the purpose of this FTM? usually the registration device don't require FTM in MOSIP	The device must mandatorily support Foundation Trust Module (FTM)–based hardware security. SBI 1.0–compliant host-based security must also be implemented. FTM establishes a hardware root of trust and enables secure boot.

		It protects cryptographic keys and prevents unauthorized tampering. Together, these ensure compliance with any open-source applications **Requirement remains unchanged.**
71.	a. Camera Is DZAP looking for an old-style enrollment kit, which requires all components to be removed from the kit and connected via a power strip and external USB hub? This is not recommended	The requirement remains strictly as per the tender document **Requirement remains unchanged.**
72.	3.8 Security What is the purpose of this FTM? usually the registration device dont require FTM in MOSIP	This is an optional component, to be used only if the camera needs to be mounted outside the MEK for capturing images under specific conditions. The requirement remains strictly as per the tender document. **Requirement remains unchanged.**
73.	3.14 Security What is the purpose of this FTM? usually the registration device dont require FTM in MOSIP	The Foundational Trust Module (FTM) is primarily required for authentication and trust services (e.g., authentication servers, signing/encryption services, and other components that perform sensitive cryptographic operations and key management). For registration kits/devices, the Purchaser will accept solutions that operate with or without an on-device FTM, provided the bidder demonstrates equivalent security controls for device identity, secure key storage, packet encryption/signing, tamper resistance, and certificate lifecycle management (e.g., TPM/secure element/OS keystore + hardening) and maintains end-to-end confidentiality and integrity of registration packets. **Requirement remains unchanged.**
74.	3.21 Construction Can you consider a range from IP54 to IP65?	IP65 is mandatory. A range from IP54 to IP65 cannot be accepted. **Requirement remains unchanged.**
75.	6.8 Construction If the 1.5m dorp test is a must? The battery is in the kit during using	Rugged aluminum design is required. The 1.5 m drop test is not mandatory with the battery installed; during testing, the battery should not be installed. All other requirements remain strictly as per the tender document **Requirement remains unchanged.**
76.	4.4 Interface USB 2.0, USB3.0 USB TYPE C are all required or just need one of them is acceptable?	All three interfaces—USB 2.0, USB 3.0, and USB Type-C—are required. Quoting only one of them is not acceptable **Requirement remains unchanged.**
77.	5.9 Display/ screen Don't understand of this requirement our A900 has a 2.8 inch built in LCD info screen	the acronym LFD refers to Live Finger Detection, which is a standard and mandatory requirement for fingerprint scanners to prevent spoofing and ensure secure and reliable biometric capture. **Requirement remains unchanged.**

78.	5.10 Security What is the purpose of this FTM? usually the registration device dont require FTM in MOSIP	The Foundational Trust Module (FTM) is primarily required for authentication and trust services (e.g., authentication servers, signing/encryption services, and other components that perform sensitive cryptographic operations and key management). For registration kits/devices, the Purchaser will accept solutions that operate with or without an on-device FTM, provided the bidder demonstrates equivalent security controls for device identity, secure key storage, packet encryption/signing, tamper resistance, and certificate lifecycle management (e.g., TPM/secure element/OS keystore + hardening) and maintains end-to-end confidentiality and integrity of registration packets. **Requirement remains unchanged.**
79.	6.3 Charging options The battery is 11.1V /60Ah which is 666Wh, such a big battery may not be fully charged in 2 hours, 4-5 hours is technically reasonable.	Using a 20 A charger, the battery can be fully charged in approximately 2-3 hours **Requirement remains unchanged.**
80.	6.5 Battery deployment Each battery is 60 Ah or each is 30Ah?	The requirement to deploy two separate batteries is removed. A single 60 Ah battery solution is acceptable, provided it meets the stated operational endurance and reliability requirements. **Requirement remains unchanged.**
81.	6.8 Construction Is the 1.5m drop test a must? The battery is in the the kit during usage	Rugged aluminum design is required. The 1.5 m drop test is not mandatory with the battery installed; during testing, the battery should be removed. All other requirements remain strictly as per the tender document **Requirement remains unchanged.**
82.	6.16 Surge adapter and charge regulator Is a Surge adapter and a charge regulator both required?	Yes, both a surge protection adapter and a charge regulator are required to meet the specified requirements, including voltage protection range, surge protection indicator, and status indicators for temperature, battery percentage, operating voltage, and output voltages **Requirement remains unchanged.**
83.	8.1 No of USB Ports Will you consider these 10 ports to be all USB 3.0 as 2.0 is outdated?	The device connected to the USB ports has varying power requirements, which necessitate USB 2.0, USB 3.0, and USB-C interfaces. Therefore, all three types must be maintained as per the requirement; USB 2.0 cannot be omitted even if it is considered outdated. **Requirement remains unchanged.**
84.	8.2 Type of Ports Is a 12V/4A adapter acceptable? Is type B and type c input both required or just one of them is acceptable?	The requirement remains strictly as per the tender document **Requirement remains unchanged.**

85.	11.1 Printer type Please confirm the printer is A6 printer or 2 inch printer? the 57.5 ± 0.5mm paper width is 2 inch printer, not A6 printer	The printer must support A6 paper size (105 × 148 mm) as stated in the requirement. It should also be compatible with common thermal paper widths, including 80 mm and 57 mm (2-inch) rolls. **Requirement remains unchanged.**
86.	11.4 Paper Width The 57.5 ± 0.5mm paper width is 2 inch printer, not A6 printer	This is a commonly used paper **Requirement remains unchanged.**
87.	12.4 Others For item a, in battery section 6.18, the cable is 10 meters, here is 2 meters, which one is correct? item C&F, it seems the customer is looking for an old-style enrollment kit, which requires all components to be removed from the kit and connected via a power strip and external USB hub. In this case, what kinds of components are needed to operate in the case? and why a cooling fan is required since all components are used out of the kit?	For the battery cable, 2 meters is mandatory for all Mobile Enrollment Kits (MEKs), while 10 meters is required for half of the MEKs as specified in section 6.18. Regarding the old-style enrollment kit, the components needed to operate outside the MEK include the camera, laptop, and printer, connected via a power strip and external USB hub. A cooling fan is required in this configuration to ensure proper ventilation and prevent overheating, since all components are operating outside the enclosed MEK **Requirement remains unchanged.**
88.	What is the format and size of the reference images in the existing ABIS?	The format and size of the reference images are defined in the officially approved sign-off documentation of the existing ABIS. Bidders are advised to refer to the finalized system documentation and acceptance records of the current ABIS to obtain accurate and authoritative information. **Requirement remains unchanged.**
89.	What biometric templates are currently stored in the existing ABIS?	The existing ABIS currently stores biometric templates for the following modalities: • Face templates • Fingerprint templates Storage of Iris templates is not confirmed at this stage and is subject to verification with the designated technical authority and review of the existing ABIS configuration. Final confirmation will be made available during the system assessment and migration planning phase **Requirement remains unchanged.**
90.	Which biometric modalities are currently used?	The current registration process supports the capture and enrolment of Face and Fingerprint (FP) biometric modalities.

		Requirement remains unchanged.
91.	How many records are in the database?	The existing ABIS database currently holds approximately 1 million biometric records.
92.	What database technology is used (e.g., PostgreSQL, Oracle)?	The current ABIS deployment uses PostgreSQL as the underlying database technology. **Requirement remains unchanged.**
93.	What is the disk size of the database?	The currently allocated storage capacity for the ABIS database node is 1TB, which includes data storage and operational overhead. **Requirement remains unchanged.**
94.	Can all records be provided as flat files if necessary?	It is preferred that biometric records continue to be stored and managed as biometric templates within the ABIS environment. Providing all records as flat files is not the preferred approach due to data integrity, security, and performance considerations. **Requirement remains unchanged.**
95.	The existing ABIS supplier (if it is proprietary software) will be required to provide support.	Details regarding support obligations from the existing ABIS vendor will depend on the terms and conditions of the current ABIS contract. Bidders are requested to review the existing vendor contract documentation for clarity on support scope and responsibilities. **Requirement remains unchanged.**
96.	During the migration, will this be handled by the issuer of the tender (SZI)	No. The System Integrator (SI) selected under this tender shall be fully responsible for planning, executing, and validating the migration of data and functionality from the existing ABIS to the new ABIS instance, in coordination with Smart Zambia Institute (SZI) and the incumbent vendor, where required. **Requirement remains unchanged.**
97.	2. Use of Subcontractor Credentials Can the technical experience and credentials of named subcontractors be referenced and considered in the proposal, or will only the credentials of consortium (Joint Venture) partners be evaluated for experience and past performance?	Technical experience and credentials of subcontractors shall not be considered for the purpose of proposal evaluation. Only the experience, credentials, and past performance of the Joint Venture (JV) partners shall be evaluated in accordance with the tender requirements and World Bank procurement guidelines. **Requirement remains unchanged.**
98.	3. Geographic Scope of HSM Experience Is it acceptable to demonstrate global Hardware Security Module (HSM) deployment experience, or is experience specifically within Sub-Saharan Africa mandatory for compliance with the security and trust requirements? Can HSM implementations from other geographies be considered.	Experience in Sub-Saharan Africa is mandatory for compliance with the security and trust requirements. HSM deployment experience from other geographies shall not be considered for meeting this specific experience requirement. **Requirement remains unchanged.**

99.	4. OEM Partner Experience for Biometric Enrolment Kits (Questions 9 & 10) For the requirements relating to biometric enrolment kits, is it acceptable to provide project experience and references from Original Equipment Manufacturer (OEM) partners as evidence, where such OEMs are responsible for the design, supply, and deployment of the enrolment hardware?	For the biometric enrolment kit requirements, only the experience and project references of the bidder and/or Joint Venture (JV) partners shall be considered. Experience, credentials, or references of OEM partners shall not be accepted as evidence for compliance with these requirements. **Requirement remains unchanged.**
100.	5. Timeline for Integrated System Demonstration (Post-Award) In the event of contract award, would it be acceptable to allow a demonstration period exceeding seven (7) days in order to showcase a fully integrated National ID system, including Digital ID, HSM, and ABIS components? This demonstration would be undertaken jointly by the Prime Contractor and consortium partners.	Due to the strict project timelines, the allocated period for the SAN box demonstration shall remain seven (7) days and any extension beyond this period will not be considered. The Prime Contractor shall be fully prepared within this timeframe to showcase a fully integrated National ID system. This demonstration is mandatory and is intended to enable stakeholders to assess the technical competence, readiness, and implementation capability of the System Integrator (SDI) in adapting and deploying the proposed Open-Source Identity Platform under stringent delivery timelines. The SDI shall demonstrate the solution using a similar biometric enrollment kit, with a customized deployment of MOSIP core modules or any equivalent proven Open-Source Identity Platform, covering at a minimum: pre-registration, registration (citizen enrollment using three biometric modalities—fingerprint (ISO/IEC 19794-2 / 442), facial portrait, and iris), digital ID issuance, and authentication (online/eKYC). **Requirement remains unchanged.**

101.	. Demonstration Environment – Hosting Model (Question 19) For the purposes of demonstrating the solution, would the following options be acceptable: a) Demonstration of the integrated solution using a secure cloud-based sandbox environment, presented as functionally equivalent to an on-premises deployment; or	As the proposed solution is strictly an on-premises implementation and the Purchaser is operating under stringent timelines, the selected bidder is expected to demonstrate the capability to implement and deploy the solution on-premises within the prescribed timelines. Accordingly, the Purchaser expects the bidder to be fully prepared to meet this requirement, and confidence in delivery will be placed on the capability and readiness of the selected bidder. **Requirement remains unchanged.**
102.	. Demonstration Environment – Hosting Model (Question 19) For the purposes of demonstrating the solution, would the following options be acceptable: b) Deployment of a sandbox environment hosted with the local partner, configured remotely by consortium partners using secure VPN access, and demonstrated as a fully integrated environment (including biometric enrolment kit integration) to the relevant authorities?	The Systems Integrator (SI) shall demonstrate that their sandbox implementation is hosted on-premises and that they can share specific information with the evaluation committee for assessment. To do this, the SI may need to provide access to certain resources and portals such as:- Information sharing: The SDI should share specific information with the evaluation committee. The information to be shared includes VPN (Virtual Private Network) access to on-prem infrastructure, hardware management, and software management portals. User Rights: The SDI should provide the necessary user rights to the evaluation committee to access the mentioned resources and portals. This ensures that the committee can evaluate the implementation effectively." **Requirement remains unchanged.**
103.	Here we're considering the different cloud deployment models, private cloud, public and hybrid cloud agreements.	For this project, the target deployment is strictly on-premises, and bidders are required to demonstrate their capability to implement, configure, and operate the solution in an on-premises environment within the prescribed timelines. **Requirement remains unchanged.**
104.	(RFP VII: Sections 1.2, 7.1, 7.2, 7.4 — Requirements of the Information System) 2.1 Section VII provides narrative descriptions of CRVS and National ID business processes (pages 158–180), including step-by-step workflows and operational requirements. However, the RFP does not	Section VII of the RFP intentionally provides business process narratives and operational workflows for CRVS and National ID to define the Purchaser's functional intent and outcomes. Detailed system-level functional specifications—including data models, field-level definitions, validation and exception rules, workflow diagrams, user role matrices, reports, APIs, and integration message formats—are not provided at this stage.

	provide the corresponding system-level functional specifications required for accurate solution costing — such as detailed data models, field-level definitions, validation rules, exception handling rules, workflow diagrams, user role matrices, reporting requirements, API specifications, and integration message formats. To ensure alignment with Purchaser expectations, please provide the full system-level functional specification for each CRVS and National ID module, or confirm whether the Bidder is expected to derive these specifications independently during the analysis phase.	Bidders are therefore expected to derive and propose the detailed system-level functional specifications based on the requirements set out in the RFP, applicable standards, and their proposed solution architecture. The successful bidder shall, during the analysis and design phase, develop comprehensive functional and technical specifications for each CRVS and National ID module, which will be reviewed, validated, and formally approved by the Purchaser prior to configuration, customization, and deployment. **Requirement remains unchanged.**
105.	2.2 Please confirm whether the CRVS system must include a Vital Statistics production subsystem, including automated statistical tables, dashboards, SDMX exports, and integration with the national statistics system, or whether vital statistics generation will be handled by a separate platform.	The CRVS system is required to support the production of vital statistics as part of the overall solution. This includes the capability to generate automated statistical tables and dashboards and to enable data exchange and integration with the national statistics system, including support for standard data formats such as SDMX, where applicable. Where certain advanced analytics or publication functions are handled by external platforms, the CRVS system shall provide the necessary interfaces and data outputs to support seamless integration. **Requirement remains unchanged.**
106.	2.3 Please clarify whether the Bidder is expected to integrate with any existing CRVS legacy systems, and if so, provide details on current platforms, data structures, APIs, and migration volumes.	The Bidder is expected to assess and plan for integration with any existing CRVS legacy systems, where applicable. However, detailed information on current platforms, data structures, APIs, and migration volumes is not fully defined at this stage. The successful bidder shall be responsible, during the analysis and design phase, for conducting a detailed assessment of existing CRVS systems in coordination with the Purchaser, defining the required integration interfaces, data mappings, and migration scope, and proposing an appropriate integration and migration approach for review and approval by the Purchaser. **Requirement remains unchanged.**

107.	(RFP VII: Sections 7.4, 7.4.4; ITP 16.3) 3.1 The RFP requires REST APIs covering all required functionalities but does not specify the interoperability standards (e.g., OpenHIE, MOSIP, HL7 FHIR, ISO 5218, W3C Verifiable Credentials). Please provide the mandatory interoperability standards and data exchange formats to be supported.	The RFP mandates the use of RESTful APIs to cover all required functionalities; however, no single interoperability standard is prescribed as mandatory at this stage. Bidders are expected to propose and implement appropriate, widely adopted interoperability standards and data exchange formats relevant to CRVS and National ID systems, such as OpenHIE, MOSIP specifications (where applicable), HL7 FHIR, ISO standards, and W3C Verifiable Credentials, as appropriate to their proposed solution. The selected bidder shall, during the analysis and design phase, finalize the interoperability standards, API specifications, and data exchange formats in consultation with the Purchaser, ensuring compliance with functional requirements, national policies, and international best practices. **Requirement remains unchanged.**
108.	3.2 Please confirm whether the CRVS system must support real-time, bidirectional integration with the Foundational Digital ID platform for event notifications, identity updates, and lifecycle management, or whether integration is limited to one-way data exchange.	The CRVS system is required to support real-time, bidirectional integration with the Foundational Digital ID platform. This includes event notifications, identity updates, and lifecycle management to ensure data consistency and timely synchronization between systems. The exact integration workflows, triggers, and data exchange mechanisms shall be detailed and finalized during the analysis and design phase, in coordination with the Purchaser. **Requirement remains unchanged.**
109.	(RFP VII: Data Migration Requirements) 4.1 The RFP references data migration but does not specify the source systems, data volumes, data quality levels, or cleansing expectations. Please provide detailed information on: (a) number of records per event type; (b) data formats;	The RFP defines data migration as a required scope but does not prescribe detailed source-system specifications at this stage. Information related to source systems, record volumes by event type, data formats, data quality levels, completeness and accuracy, transformation rules, and deduplication requirements will be determined during the analysis and design phase.

	(c) completeness/accuracy levels; (d) expected transformation rules; (e) whether deduplication is required.	The successful bidder shall be responsible for conducting a comprehensive data assessment, including profiling of source data, identification of data quality issues, definition of cleansing and transformation rules, and determination of deduplication requirements, in close coordination with the Purchaser. A detailed data migration strategy and plan shall be prepared and submitted for Purchaser review and approval prior to execution. **Requirement remains unchanged.**
110.	4.2 Please clarify whether the Bidder is responsible for digitization of paper records, or whether migration applies only to existing electronic datasets.	Data migration under this RFP applies only to existing electronic datasets. Digitization of paper-based records is not included in the Bidder's scope under this procurement, unless explicitly stated otherwise in the tender documents. **Requirement remains unchanged.**
111.	(RFP VII: Backend Infrastructure; PDS ITP 17.5–17.6) 5.1 The RFP requires supply and configuration of backend infrastructure but does not specify the target hosting model (on-premises, hybrid, private cloud, government cloud). Please confirm the mandated hosting environment and provide the required technical specifications.	The mandated hosting environment for the backend infrastructure is strictly on-premises. Bidders are required to supply, configure, and deploy all backend infrastructure within the Purchaser's premises, in full compliance with the technical, functional, security, and performance requirements specified in the RFP. **Requirement remains unchanged.**
112.	5.2 Please clarify whether the Bidder is expected to provide disaster recovery infrastructure, including secondary sites, replication technologies, and RPO/RTO requirements.	Yes, the Bidder is expected to provide a comprehensive disaster recovery (DR) solution as part of the backend infrastructure scope. This includes: Secondary/backup site(s) capable of supporting failover in case of primary site outage. Replication technologies to synchronize data between primary and DR sites, ensuring minimal data loss. Defined Recovery Point Objective (RPO) and Recovery Time Objective (RTO) requirements in line with the system's criticality and operational needs. The successful bidder shall design, implement, and validate the DR infrastructure, including failover and failback procedures, in coordination with the Purchaser to ensure business continuity, high availability, and compliance with national standards. **Requirement remains unchanged.**
113.	(RFP VII: Enrollment Kits) 6.1 The RFP requires supply of enrollment kits but	The quantities and detailed technical specifications for each component of the Mobile Enrollment Kits (MEKs) are already provided in the RFP. Bidders should refer to Section

	does not provide technical specifications, quantities, biometric modalities, or certification requirements. Please provide detailed specifications for each component (e.g., fingerprint scanners, cameras, signature pads, printers, UPS, tablets).	VII – Purchaser's Requirements: Biometric Enrollment Kit Requirement for full details, including specifications for fingerprint scanners, cameras, signature pads, printers, UPS/batteries, and laptops. Bidders are expected to fully comply with these specifications when preparing their proposals. **Requirement remains unchanged.**
114.	6.2 Please confirm whether enrollment kits must support offline enrollment, local caching, and secure synchronization, and whether any specific encryption or tamper-proofing standards apply.	Yes, the enrollment kits (MEKs) must support offline enrollment, including local caching of captured data when connectivity is unavailable. The kits must also support secure synchronization of data with the central system once connectivity is restored. All stored and transmitted data must comply with industry-standard encryption protocols (e.g., AES-256 for data at rest, TLS 1.2 or higher for data in transit) and include tamper-proofing measures to ensure integrity, confidentiality, and authenticity of biometric and demographic data captured during enrollment. **Requirement remains unchanged.**
115.	(ITP 11.2(j)(b); Section VII: Support Requirements) 7.1 The RFP requires compliance with SLAs but does not provide the baseline SLA framework (uptime, response times, resolution times, penalties). Please provide the mandatory SLA parameters to be costed and committed to in the proposal.	The RFP requires compliance with Service Level Agreements (SLAs) for all system components, but does not prescribe a fixed SLA framework. Bidders are expected to propose SLAs in line with the criticality, operational requirements, and best practices for national-scale digital ID systems, including: System uptime/availability (e.g., percentage availability of key modules, including ABIS, CRVS, and enrollment kits) Response times for incident acknowledgement and support requests Resolution times for different severity levels of incidents (critical, high, medium, low) Penalties or service credits associated with non-compliance to SLA targets The proposed SLA parameters will be evaluated for reasonableness, alignment with industry standards, and feasibility. The successful bidder shall formalize and commit to the SLAs as part of the contract, ensuring that support, maintenance, and operational readiness meet the requirements of the Purchaser.

		Requirement remains unchanged. If you want, I can also draft a table of recommended baseline SLA metrics that bidders can cost and commit to in their proposals.
116.	7.2 Please clarify whether the Bidder is expected to provide 24/7 national support, regional support presence, or embedded support teams within Smart Zambia Institute.	The Bidder is expected to provide comprehensive support coverage to ensure continuous operation of the National ID system. This includes: 24/7 national support for critical system components, including ABIS, CRVS, and enrollment kits. Regional support presence as necessary to respond promptly to on-site incidents and maintenance needs. Embedded support teams within Smart Zambia Institute (SZI) are not mandatory, but the Bidder must ensure sufficient coordination and availability of skilled personnel to meet SLA commitments and operational requirements. The exact deployment of support resources shall be proposed by the Bidder in alignment with the operational requirements, SLA targets, and project timelines. **Requirement remains unchanged.**
117.	(ITP 11.2(j)(c); ITP 16.2(a)) 8.1 The RFP requires a comprehensive training program but does not specify target user groups, training volumes, competency levels, or certification requirements. Please provide the expected number of trainees per category (registrars, administrators, ICT staff, statisticians, health workers).	The RFP requires the Bidder to provide a comprehensive training program covering all relevant user groups for the National ID and CRVS systems. The target trainee categories include, but are not limited to: Registrars – responsible for citizen enrollment and verification. System administrators – responsible for configuration, user management, and system monitoring. ICT support staff – responsible for operational support, maintenance, and troubleshooting. Statisticians and data analysts – responsible for reporting, data analysis, and vital statistics production. Health workers and other sectoral staff – where integration with sectoral services is

		required. The expected number of trainees, competency levels, and certification requirements will be finalized during the analysis and design phase in consultation with the Purchaser. Bidders are expected to propose a training plan that includes curriculum, delivery methods, hands-on exercises, assessment mechanisms, and post-training support to ensure all user groups achieve the required competencies. **Requirement remains unchanged.**
118.	8.2 Please confirm whether the Bidder is responsible for developing national training curricula, training-of-trainers (ToT) programs, and long-term capacity-building frameworks.	Yes, the Bidder is responsible for developing and delivering national training curricula, including Training-of-Trainers (ToT) programs, and establishing long-term capacity-building frameworks. This includes: Designing training content and materials aligned with the system functionality, workflows, and operational procedures. Conducting ToT sessions to enable sustainable knowledge transfer to SZI personnel and other designated trainers. Developing a capacity-building plan to ensure ongoing skill development, refresher training, and knowledge retention for all relevant user groups. The training and capacity-building program shall be designed to support sustainable system operation, maintenance, and future scaling in line with the Purchaser's strategic objectives. **Requirement remains unchanged.**
119.	(ITP 16.2(a)(v); Section VII: Testing Requirements) 9.1 Please provide the detailed acceptance testing framework, including required test types (UAT, SIT, performance testing, security testing), acceptance thresholds, and documentation templates.	The RFP requires the Bidder to implement a comprehensive testing, quality assurance, and acceptance process, but does not prescribe a fixed framework. The successful Bidder shall develop and execute a detailed acceptance testing plan, covering the following aspects: Test types: System Integration Testing (SIT): To validate end-to-end functionality across all modules (CRVS, National ID, ABIS, HSM, enrollment kits). User Acceptance Testing (UAT): To confirm that the system meets operational and functional requirements for end-users.

		Performance and Load Testing: To verify system scalability, response times, and throughput under expected peak loads. Security Testing: To ensure compliance with data protection, encryption, access control, and vulnerability management standards. Acceptance thresholds: The Bidder shall define measurable criteria (e.g., uptime, error rates, response times, processing accuracy) in consultation with the Purchaser. Documentation templates: The Bidder shall provide test plans, test cases, execution logs, defect reports, and final acceptance certificates. The final acceptance testing framework will be reviewed and approved by the Purchaser before execution, ensuring alignment with project requirements, operational expectations, and contractual obligations. **Requirement remains unchanged.**
120.	9.2 Please clarify whether independent verification and validation (IV&V) will be conducted by the Purchaser or whether the Bidder must include IV&V services in the proposal.	Independent Verification and Validation (IV&V) will be conducted by the Purchaser or its designated third-party. The Bidder is not required to provide IV&V services as part of their proposal. However, the Bidder must fully cooperate with the IV&V process, providing access to system documentation, test results, source code, and other relevant materials as requested, and address any findings or recommendations arising from the IV&V assessments. **Requirement remains unchanged.**
121.	(ITP 11.2(j)(e)) 10.1 The RFP requires cybersecurity risk management plans but does not specify the mandatory security standards (e.g., ISO 27001, NIST CSF, OWASP, GDPR-equivalent). Please provide the required compliance frameworks and certification expectations.	The RFP requires the Bidder to implement a comprehensive cybersecurity risk management plan covering all system components, data flows, and user interactions. While the RFP does not prescribe a single mandatory standard, the solution and proposed practices must comply with internationally recognized cybersecurity frameworks and best practices, including, but not limited to: ISO/IEC 27001 , NIST Cybersecurity Framework (CSF) – for risk identification, protection, detection, response, and recovery, OWASP Top 10 – for secure application development , Data protection and privacy compliance The selected bidder must demonstrate adherence to these standards through system design, implementation, and operational procedures, including secure coding, encryption, access

		control, auditing, monitoring, and incident response mechanisms. Certification or formal compliance evidence may be requested during evaluation or post-award verification. **Requirement remains unchanged.**
122.	10.2 Please confirm whether the Bidder must implement Security Operations Center (SOC) integration, SIEM tools, continuous monitoring, and incident response capabilities as part of the contract.	No, the Bidder is not required to implement a Security Operations Center (SOC), SIEM tools, or continuous monitoring and incident response capabilities as part of this contract. However, the Bidder must ensure that the solution is designed, configured, and deployed securely, following industry-standard cybersecurity practices, including encryption, access controls, auditing, and secure data handling, to protect the integrity and confidentiality of all system components. **Requirement remains unchanged.**
123.	(ITP 16.2(a)(i); PDS Sections on Project Organization) 11.1 Please provide the detailed project governance structure, including roles and responsibilities of Smart Zambia Institute, Ministry of Home Affairs, Ministry of Health, CSO, and other stakeholders to ensure accurate planning of coordination, approvals, and dependencies.	The detailed project governance structure, including roles and responsibilities of all stakeholders, shall be provided during implementation. The System Integrator (SI) will coordinate with the Purchaser and relevant government entities to define responsibilities, reporting lines, approvals, and dependencies to ensure effective project execution, alignment with timelines, and compliance with operational requirements. **Requirement remains unchanged.**
124.	11.2 Please clarify whether the Bidder is expected to provide a full-time onsite project management office (PMO) or whether a hybrid onsite/offsite model is acceptable.	The Bidder is not required to provide a full-time onsite Project Management Office (PMO). A hybrid onsite/offsite project management model is acceptable, provided that the Bidder demonstrates the capability to effectively coordinate all project activities, maintain communication with the Purchaser and stakeholders, and meet project timelines and SLA commitments. The PMO must ensure adequate coverage for critical activities, reporting, and decision-making throughout the project lifecycle. **Requirement remains unchanged.**
125.	(RFP VII: Section 1.2(d)) Section 1.2(d) requires integration of "MOSIP-compliant" technologies, but the RFP does not specify whether formal MOSIP certification is mandatory. 12.1 Please confirm whether the Purchaser requires the Bidder to hold any formal MOSIP certification (e.g., MOSIP Partner Certification, MOSIP Compliance Validation) as part of this procurement.	Following the Addendum, the Purchaser does not mandate formal MOSIP certification for all proposed solutions. Bidders proposing MOSIP as the platform must provide valid MOSIP Technical and Commercial Partnership credentials. For alternative proven Open-Source Identity Platforms, MOSIP certification is not required, but bidders must provide Manufacturing Authorization and demonstrate that the solution meets the functional, technical, and interoperability requirements specified in the RFP. **Requirement remains unchanged.**

126.	12.2 If formal MOSIP certification is not mandatory, please confirm what forms of acceptable evidence of MOSIP compatibility the Purchaser will accept (e.g., prior MOSIP-based deployments, API-level compatibility, architectural alignment, or other documentation).	N/A **Requirement remains unchanged.**
127.	12.3 If formal MOSIP certification is required, please specify which certification pathway applies and whether certification must be obtained prior to contract award or may be completed during implementation.	if a bidder proposes MOSIP as the solution, they must provide valid MOSIP Technical and Commercial Partnership credentials as evidence of capability and compatibility. **Requirement remains unchanged.**
128.	Target Architecture Definition. RFP Observation: Deployment of Open-Source Identity Platform (MOSIP or equivalent) Please confirm whether a target architecture (centralized, federated, or hybrid) is prescribed, or whether bidders are permitted to propose an optimized architecture that meets the functional and performance requirements.	The RFP does not prescribe a fixed target architecture (centralized, federated, or hybrid) for the Open-Source Identity Platform. Bidders are permitted to propose an optimized architecture that meets all functional, technical, security, scalability, and performance requirements specified in the tender. The proposed architecture must be robust, future-ready, and capable of supporting national-scale operations, with clear justification and alignment to World Bank procurement principles and operational requirements. **Requirement remains unchanged.**
129.	Existing Identity Systems Baseline. RFP Observation: No existing national identitysystem or partial Digital ID implementation stated Please confirm whether there is any existing Digital ID or identity management system in operation, and if so, provide its current-state architecture and functional scope.	There is no existing live Digital ID or identity management system currently in operation. Accordingly, there is no current-state architecture or functional scope to be provided at this time. **Requirement remains unchanged.**
130.	MOSIP vs Equivalent Platform Acceptance. RFP Observation: Alternates between "MOSIP" and "MOSIP or equivalent" Please confirm whether MOSIP is mandatory, or whether functionally equivalent open-source identity platforms are acceptable, and if so, specify the equivalence criteria.	Following the Addendum, MOSIP is not mandatory. Bidders may propose functionally equivalent open-source identity platforms, provided that the proposed solution meets all functional, technical, security, and interoperability requirements specified in the RFP. To demonstrate equivalence, bidders must provide evidence such as: • Proven deployments of the proposed platform at national or large-scale identity projects. • Technical documentation showing feature parity with MOSIP core modules.

		• Interoperability and API compatibility with MOSIP or standard identity management protocols. • Manufacturing Authorization or partnership credentials validating the bidder's authority to deploy the solution. Equivalence will be evaluated based on the platform's ability to deliver the same outcomes, scalability, and compliance standards as MOSIP. **Requirement remains unchanged.**
131.	Data Migration Scope. RFP Observation: Data migration volumes, rules, and legacy data scope not defined Please confirm whether data migration from any existing identity or civil registry systems is in scope, and if so, provide data volumes, formats, and migration expectations.	Data migration from existing identity or civil registry systems is within scope of the project; however, the RFP does not provide detailed information on source systems, record volumes, data formats, or specific migration rules. The successful bidder shall, during the analysis and design phase, be responsible for: • Conducting a comprehensive assessment of legacy systems and data quality. • Defining data mapping, transformation, and cleansing rules. • Planning and executing data migration, including deduplication and validation. • Providing a detailed migration strategy for review and approval by the Purchaser prior to execution. • Exact data volumes, formats, and migration expectations will be determined collaboratively with the Purchaser as part of the project planning process. **Requirement remains unchanged.**
132.	Biometric Scope & ABISRFP Observation: Biometric enrolment and identity verification implied; ABIS unclear Please clarify whether ABIS (Automated Biometric Identification System) is:a) Already existing,b) To be supplied by the bidder, orC) Out of scope of this RFP.	ABIS is within scope of this RFP and shall be supplied by the bidder. The proposed Automated Biometric Identification System (ABIS) must support 15 million licenses and handle three biometric modalities—fingerprint, facial image, and iris—in accordance with the functional, performance, and scalability requirements specified in the RFP. **Requirement remains unchanged.**
133.	Identity Record Volumes. RFP Observation: Experience with ≥30 million identity records referenced Please confirm the expected number of identity records for initial rollout and at full national scale.	For the initial rollout, the system is expected to manage approximately 15–20 million identity records. At full national scale, the solution must be capable of supporting the entire population, estimated at approximately 22 million, with sufficient scalability to accommodate future population growth (3%+ per annum). **Requirement remains unchanged.**

134.	Integration Targets. RFP Observation: Integration with government systems required; specific systems not enumerated Please provide a list of systems and platforms with which the Digital ID system must integrate, including authentication, service access, and data exchange use cases.	The RFP requires the Digital ID system to support integration with multiple government systems and platforms; however, a fixed and exhaustive list of integration targets is not prescribed at this stage.The successful bidder shall, during the analysis and design phase, work with the Purchaser to identify, prioritize, and define detailed integration use cases, interfaces, data exchange mechanisms, and security controls, ensuring compliance with national policies and applicable standards. **Requirement remains unchanged.**
135.	Integration Targets. RFP Observation: Integration with government systems required; specific systems not enumerated Could you provide detailed information on the legacy systems currently in place that need to be integrated with the new Integrated National Registration Information System (INRIS)?	The RFP indicates that integration with existing government systems is required; however, detailed information on specific legacy systems (including platforms, technologies, interfaces, and data structures) is not enumerated at this stage. The successful bidder shall, during the analysis and design phase, work closely with the Purchaser to identify and assess the relevant legacy systems that require integration with the Integrated National Registration Information System (INRIS). This will include defining integration scope, data exchange requirements, interfaces, security controls, and migration or synchronization approaches, which will be documented and approved prior to implementation. **Requirement remains unchanged.**
136.	Integration Targets. RFP Observation: Integration with government systems required; specific systems not enumerated We understand that the Digital ID and CRVS systems are required to be integrated with the SMARTCARE PRO health system. Please clarify whether any additional systems are expected to be integrated under the scope of this project, and if so, kindly provide an indicative list of such systems, their main technologies, and whether they are developed in-house.	Integration with the SMARTCARE PRO health system is within the scope of this project. Apart from SMARTCARE PRO, the RFP does not define a fixed or exhaustive list of additional systems to be integrated at this stage. Any further integrations with other government or sectoral systems (e.g., social protection, education, statistics, service delivery platforms) will be identified and finalized during the project kick-off and analysis phase, in coordination with the Purchaser. At that stage, an indicative list of systems, their primary technologies, integration mechanisms, and whether they are developed in-house or by third parties will be documented, agreed upon, and approved prior to implementation. **Requirement remains unchanged.**
137.	API & Interoperability Standards. RFP Observation: No API standards or protocols specified	The RFP does not prescribe specific mandatory interoperability standards or API protocols at this stage. Bidders are expected to propose open, secure, and widely adopted standards suitable for national-scale Digital ID and CRVS integrations. The final set of interoperability standards, API specifications, and security mechanisms will be defined and

	Please confirm the preferred interoperability standards, API protocols, and security mechanisms expected for third-party system integration.	approved during the analysis and design phase in consultation with the Purchaser, ensuring compliance with national policies and international best practices. **Requirement remains unchanged.**
138.	Sandbox Demonstration Scope. RFP Observation: Bidders must deliver a working sandbox within 7 working days. Please clarify the functional scope, dataset expectations, and evaluation criteria for the sandbox demonstration.	The purchaser clarifies that the sandbox demonstration is intended to validate the technical capability, readiness, and integration competence of the bidder within the stipulated seven (7) working days. The expected scope and evaluation criteria are as follows: Functional scope: The sandbox must demonstrate a fully integrated National ID solution using an Open-Source Identity Platform (MOSIP or equivalent), including at a minimum: • Pre-registration and registration workflows • Citizen enrollment using three biometric modalities (fingerprint, facial image, and iris) • ABIS integration and biometric matching • Digital ID issuance • Authentication services (online / eKYC) Dataset expectations: The sandbox may use synthetic or test data only. No production or live citizen data is required. The dataset should be sufficient to demonstrate end-to-end workflows, biometric processing, and system performance at a representative scale. Evaluation criteria: The sandbox will be evaluated on: • Completeness of functional coverage • Level of integration between components (enrollment kits, ABIS, Digital ID, authentication) • Security controls and access management • Stability, responsiveness, and overall technical readiness • Ability to deploy and configure the solution on-premises within the defined timeline The demonstration is a mandatory evaluation step and forms a key basis for assessing the bidder's capability to deliver the solution within the project's stringent timelines. **Requirement remains unchanged.**

139.	Consequence of Sandbox Non-Delivery. RFP Observation: Sandbox failure consequences unclear Please confirm whether failure to deliver the sandbox within the stipulated timeframe results in technical disqualification or scoring impact only.	Failure to deliver the sandbox demonstration within the stipulated timeframe of seven (7) working days shall result in technical non-compliance and may lead to technical disqualification of the bidder. The sandbox demonstration is a mandatory requirement and a critical component of the technical evaluation, intended to validate the bidder's readiness, integration capability, and ability to meet the project's stringent timelines. Accordingly, non-delivery or incomplete delivery of the sandbox within the defined period will not be treated as a scoring impact only, but as a material deviation from the RFP requirements. **Requirement remains unchanged.**
140.	Acceptance Testing Framework. RFP Observation: No acceptance criteria, benchmarks, or sign-off authority defined Please provide the acceptance testing framework, including performance benchmarks, security testing requirements, and acceptance authority.	The RFP requires the Bidder to implement a structured acceptance testing framework, although detailed benchmarks and criteria are not predefined at this stage. The acceptance testing framework shall be defined and executed as follows: Testing scope: The Bidder shall conduct System Integration Testing (SIT), User Acceptance Testing (UAT), performance and load testing, and security testing covering all components, including CRVS, National ID, ABIS, HSM, backend infrastructure, and enrollment kits. Performance benchmarks: Benchmarks such as system availability, transaction response times, enrollment throughput, biometric matching accuracy, and scalability thresholds shall be proposed by the Bidder in line with national-scale operational requirements and international best practices, and shall be reviewed and approved by the Purchaser prior to testing. Security testing requirements: Security testing shall include vulnerability assessments, penetration testing, access control validation, encryption verification, audit logging, and compliance with applicable cybersecurity standards and national policies. Acceptance authority: Final system acceptance and sign-off shall rest with the Purchaser, based on successful completion of agreed test cases, achievement of approved benchmarks, and resolution of all critical defects.

		The detailed acceptance testing plan, benchmarks, and documentation templates shall be finalized during the analysis and design phase and formally approved before execution. **Requirement remains unchanged.**
141.	Decision-Making & Escalation. RFP Observation: Governance structures implied but not detailed Please confirm the decision-making, escalation, and approval structure applicable during implementation.	The RFP establishes a structured but flexible governance approach for decision-making, escalation, and approvals during implementation, while allowing details to be finalized post-award.The detailed decision rights, escalation paths, and approval timelines will be formalized during the project initiation phase and documented in the Project Governance and Management Plan. **Requirement remains unchanged.**
142.	Managed Services Duration. RFP Observation: Duration and scope not explicitly defined Please confirm the expected duration and scope of managed services, including whether they form part of the main contract or a separate phase.	Managed services are included as part of the main contract and are expected to commence post go-live of the system. The exact duration and detailed scope of managed services (including operations, maintenance, monitoring, and support activities) are not explicitly defined in the RFP and shall be finalized during contract negotiations and the implementation planning phase. Bidders are expected to propose a reasonable managed services approach aligned with the operational needs of a national-scale Digital ID and CRVS system, which will be reviewed and agreed upon by the Purchaser prior to commencement. **Requirement remains unchanged.**
143.	Bid Security Amount. RFP Observation: Amount not stated	Bid security is not required for this procurement. **Requirement remains unchanged.**
144.	Performance Security. RFP Observation: Amount and form not clearly stated	The performance security shall be valid for eighteen (18) months. The amount and acceptable form shall be as specified in the Bidding Data Sheet (BDS) and Contract Conditions of the RFP and must be submitted by the successful bidder upon contract award. **Requirement remains unchanged.**
145.	Aggregation of Experience Thresholds. RFP Observation: Experience thresholds unclear if per project or cumulative Please confirm whether experience thresholds must be met per single project or may be aggregated across multiple projects.	Experience thresholds must be met per single project. Aggregation of experience across multiple projects is not acceptable for meeting the specified experience requirements. **Requirement remains unchanged.**

146.	Mixed Scoring Scales. RFP Observation: Different scoring scales used across categories Please confirm that the use of different scoring scales across technical categories is intentional, with no additional normalisation.	Yes, the use of different scoring scales across technical evaluation categories is intentional. No additional normalization will be applied beyond what is already defined in the RFP. **Requirement remains unchanged.**
147.	Governance, scope Please indicate how Civil Registration (CRVS) data are currently managed (e.g. paper based records, Excel files, or other formats) and provide an estimate of the volume of historical CRVS data.	Detailed information on how Civil Registration (CRVS) data are currently managed, including data formats and the estimated volume of historical records, will be provided during the project kick-off meeting. **Requirement remains unchanged.**
148.	Architecture and technical requirements Please clarify the types of hosting environments envisaged (on-premises, private cloud, public cloud, hybrid cloud, etc.) for both the Digital ID and CRVS systems, for the primary site as well as the secondary (disaster recovery) site.	For both the Digital ID and CRVS systems, the mandated hosting environment is strictly on-premises for the primary site as well as the secondary (disaster recovery) site.
149.	Architecture and technical requirements Please specify the two sites planned for the production environment and the disaster recovery environment and confirm whether these sites are already interconnected. Please also clarify which party is responsible for providing and managing this interconnection.	The specific locations of the production site and the disaster recovery (DR) site will be confirmed and communicated during the project kick-off and implementation planning phase. The interconnection between the production and DR sites, including bandwidth, latency, and security requirements, will also be detailed at that stage. Responsibility for providing and managing the inter-site connectivity will be clarified during implementation, based on the agreed architecture and operational model, and documented as part of the approved infrastructure and deployment plan. **Requirement remains unchanged.**
150.	Support and guarantee We note that the post-delivery support period is stated as 36 months on page 250, whereas the "Implementation Schedule Table" on page 254	The post-delivery support period shall be thirty-six (36) months. **Requirement remains unchanged.**

	indicates “Commencement of Support for 24 months”. Please clarify which duration applies.	
151.	Support and guarantee Please clarify the exact duration of the warranty period, as well as the duration and scope of the post-warranty period.	The warranty period shall apply for the duration specified in the RFP and Contract Conditions and shall cover all supplied hardware, software, and integrated components against defects and non-performance. Following the warranty period, a post-warranty support period shall apply as part of the managed services scope, covering system maintenance, support, and operational assistance. **Requirement remains unchanged.**
152.	Pg 146 Sec 1.2 Development and Integration of Card Personalization software, Card Production Management, Warehouse and Dispatch and supporting card stock management, dispatch, issuance and destruction There is a mention of card personalization system in the scope of work, however the details of the card are not available. 1. Please specify the card material of the proposed card (PVC, PET/PVC, PC etc) 2. Please specify the card physical format and structure detailing what needes to be printed on each side of the card (including color scheme, logos, photo, demographic data (such as name, gender, etc), QR code, contents of the QR code and so on) 3. Please specify the card printing method (laser engraving, direct to card printing etc) that must be used to print the photo and demographic data on the card for personalisation 4. Please specify the security features that are required in the card (like guilloche, microtext, hologram, CLI, Laminat etc) 5. Please specify the volume of cards to be produced and the corresponding timeframe and locations to	The activities related to card personalization, card production management, warehouse, dispatch, issuance, and destruction are not part of the delivery scope under this procurement. The requirement is limited to ensuring that the Integrated National Registration Information System (INRIS) is technically capable of integrating with external card personalization and card production management systems, through open, secure, and standards-based interfaces (APIs). Details such as card material, physical card design, printing and personalization methods, security features, production volumes, production models, sites, and associated ICT infrastructure are out of scope for this tender and will be handled separately by the Purchaser or a designated third party. **Requirement remains unchanged.**

	calculate the card production capacity and requirement for printers. The type of card material and printing method has a huge impact on the type of equipment to be chosen and the corresponding bill of materials. 6. Please specify whether centralized production is preferred or a mixed central and decentralised model shall be used for card production and distribution? 7. Please specify how many card personalization sites should be offered. 8. Please specify how many card issuance sites should be planned. 9. Please specify if all the ICT infrastructure for card production and personalisation is to be supplied by the bidder	
153.	Pg 146 Section 1.2 Migration of data from the existing system to the new Integrated National Registration Information System Please specify the type and format of legacy data that is available for migration. Type: fingerprint/face/demographic(textual) data etc Format: raw data/jpeg files/templates Volume of each type of data to be migrated	The detailed information on the type, format, and volume of legacy data available for migration—including biometric data (fingerprint, facial images) and demographic (textual) data, as well as whether such data is available as raw data, image files (e.g., JPEG), or biometric templates—is not specified at this stage. These details will be assessed and confirmed during the project kick-off and analysis phase, in coordination with the Purchaser and relevant system owners. The successful bidder shall be responsible for evaluating the available legacy data, defining the appropriate migration approach, and proposing data mapping, transformation, and validation mechanisms for approval prior to execution. **Requirement remains unchanged.**
154.	Page 211 DATA MIGRATION FROM EXISTING SYSTEM TO MOSIP Legacy Data Access Method In order to accurately assess migration feasibility and effort, can the Purchaser confirm whether data provided from legacy systems (including demographic and biometric data) will be made available in a readable, non-encrypted format, or whether decryption keys and procedures will be	At this stage, the data access method for legacy systems, including whether demographic and biometric data will be available in readable, non-encrypted format or in encrypted form, is not fully defined. Where legacy data is stored in encrypted form, the availability of decryption keys, access procedures, and related security protocols will be determined and agreed upon during the project kick-off and analysis phase, in coordination with the Purchaser and the incumbent system owners. The System Integrator (SDI) will be expected to follow all applicable

	provided to the SDI where data is stored in encrypted form?	security, confidentiality, and data protection requirements during data access and migration activities. **Requirement remains unchanged.**
155.	Page 211 DATA MIGRATION FROM EXISTING SYSTEM TO MOSIP Digitization of Paper Records The RFP requires migration of legacy data into the new system. Can the Purchaser confirm whether this scope includes the digitization (scanning and indexing) of paper- based records that are not currently available in electronic form, or whether the SDI's responsibility is limited to migration of existing digital data only?	The scope of data migration under this RFP is limited to existing electronic (digital) data only. The digitization, scanning, or indexing of paper-based records is not included in the SDI's responsibilities under this procurement, unless explicitly stated otherwise in the RFP or subsequent contractual amendments. **Requirement remains unchanged.**
156.	Page 146 FUNCTIONAL, ARCHITECTURAL AND PERFORMANCE REQUIREMENTS Scope of Legacy System Integrations The RFP refers to integration with existing legacy systems. Can the Purchaser clarify how many legacy systems are currently in scope for data integration, and provide a high- level description of each system's function?	The RFP identifies the need for integration with existing legacy systems; however, the exact number and detailed descriptions of such systems are not defined at this stage. A high-level identification and description of the legacy systems in scope for integration—including their primary functions—will be provided during the project kick-off and analysis phase. The successful bidder shall work with the Purchaser to assess these systems and define the detailed integration scope, interfaces, and data exchange mechanisms for approval prior to implementation. **Requirement remains unchanged.**
157.	Page 147 FUNCTIONAL, ARCHITECTURAL AND PERFORMANCE REQUIREMENTS Scope of Third-Party Integrations The RFP references integration with multiple third-party systems. Can the Purchaser confirm whether the SDI's scope under this tender is limited to designing INRIS with open APIs and integration capability, or whether the SDI is also required to implement and deliver actual integrations with specific third-party systems? If integrations are required, can the Purchaser identify which systems are in scope?	The SDI's scope under this tender includes designing and implementing the Integrated National Registration Information System (INRIS) with open, secure APIs and full integration capability. In addition, the SDI is required to implement and deliver actual integrations with identified third-party systems that are confirmed by the Purchaser. However, the specific third-party systems in scope are not exhaustively defined at this stage. The list of third-party systems, along with the integration use cases and technical details, will be identified and finalized during the project kick-off and analysis phase in coordination with the Purchaser, and will be documented and approved prior to implementation. **Requirement remains unchanged.**

158.	Page 303-309 DELIVERABLES System Environments Can the Purchaser clarify the number and types of system environments expected to be implemented and maintained under this contract (e.g. development, integration, testing, staging/pre-production, production, disaster recovery), and indicate which of these environments are within the scope of the SDI's responsibility to design, deploy, and operate?	Under this contract, the SDI is expected to design, deploy, and support multiple system environments to ensure effective development, testing, deployment, and operations. While the RFP does not prescribe an exhaustive environment list with fixed sizing at this stage. The SDI is responsible for the design, deployment, and configuration of all required environments, including Production and DR, in line with the approved architecture and on-premises hosting requirements. The operation and support responsibilities for each environment (e.g., duration, level of support) will be finalized during implementation planning and documented in the agreed delivery and support model. **Requirement remains unchanged.**

Percy Chinyama
National Coordinator
SAMRT ZAMBIA INSTITUTE, E-GOVERNMENT DIVISION

STATUS AND EFFECT OF THIS ADDENDUM

3.1 This Addendum forms an **integral part of the RFP documents** and shall be read in conjunction with the original RFP.

3.2 Proposers are required to:

- Review this Addendum carefully.
- Take its contents fully into account when preparing their Proposals
- Acknowledge receipt of this Addendum in their Proposal submission in accordance with the RFP instructions

3.3 Failure to comply with the requirements introduced under this Addendum may result in the Proposal being deemed **non-responsive** during evaluation.

ANNEX A

AMENDED TECHNICAL AND FUNCTIONAL REQUIREMENTS

INTEGRATED NATIONAL ID REGISTRY AND CRVS PLATFORM

(Issued pursuant to Addendum No. 01 to the Request for Proposals)

1. Platform Governance and Openness

1.1 Open-Source Requirement

The proposed National Identification Registry (NIR) and Civil Registration and Vital Statistics (CRVS) solution ***shall be based on open-source software*** *released under an* ***OSI-approved license****.*

The source code shall be:

- *Publicly accessible in a recognized source-code repository*
- *Freely auditable by the Government.*
- *Modifiable and deployable by the Government without dependency on a single vendor*

*The solution **shall not impose proprietary licensing fees** for core platform components.*

1.2 Vendor Neutrality

*The solution shall be **vendor-agnostic** and designed to:*

- *Enable multiple system integrators to deploy, operate, and enhance the system*
- *Allow replacement of individual components without system redesign*
- *Ensure long-term technological sovereignty for the Government*

2. Architecture and Design Principles

2.1 Modular and Microservices-Based Architecture

*The solution shall adopt a **modular, microservices-based architecture**, characterized by:*

- *Loosely coupled and independently deployable services*
- *Clear functional separation between system components*
- *Horizontal scalability and high availability*

At a minimum, the architecture shall include distinct modules for:

- *Identity registration and lifecycle management*
- *Biometric processing and deduplication*
- *Identity repository management*
- *Credential issuance and management*
- *Civil registration and vital events management*
- *Integration and interoperability services*

2.2 API-First and Standards-Based Design

*All system components shall expose functionality through **secure, well-documented RESTful APIs**.*

APIs shall:

- *Conform to OpenAPI (formerly known as the Swagger Specification) specifications*
- *Support versioning and backward compatibility.*
- *Enable integration with external government and private systems without proprietary middleware*

2.3 Cloud-Native and Containerized Deployment

*The solution **shall be designed to operate on a cloud-native architecture**, supporting deployment on:*

- *Public cloud*
- *Private cloud*
- *Government cloud*
- *On-premise infrastructure*

The platform shall:

- *Support containerization technologies*
- *Support container orchestration*
- *Enable independent scaling, upgrade, and maintenance of system components*

This design shall ensure:

- *Improved system maintainability*
- *Operational resilience*
- *Ease of future upgrades and enhancements*

3. Biometric and Identity Capabilities

3.1 Platform with Pluggable Biometric Framework

*The solution shall support a **pluggable biometric architecture** that enables integration with biometric SDKs and supports 3 modalities (Fingerprint, Face, and Iris).*

The biometric framework shall:

- *Not be hard-wired to a single biometric vendor*
- *Allow certified SDKs to be added or replaced without core system changes*
- *Support national and international biometric standards*

3.2 Pluggable Multi-Vendor Biometric Devices

*The solution shall support **biometric capture devices from multiple manufacturers**, ensuring that:*

- *Biometric devices are **not restricted to a single vendor***
- *Devices can be onboarded through **standardized device interfaces and protocols***
- *New biometric device vendors can be added without modification to the core system logic*

This requirement applies to biometric capture for Fingerprint, Face, and Iris

3.3 Large-Scale Biometric Deduplication

*The solution shall support **1:N biometric deduplication** at a national scale, including:*

- *Configurable deduplication policies by modality*
- *Auditable deduplication decision processes*
- *Capability to scale to populations of several million records or more*

4. Automated Biometric Identification System (ABIS)

4.1 ABIS Vendor Eligibility

The proposed solution shall include an ***Automated Biometric Identification System (ABIS)*** *provided by a qualified biometric service provider.*

The ABIS solution ***shall support, at a minimum****, the following biometric modalities: Fingerprint, Facial image, and Iris*

The ABIS solution shall be capable of:

- *Storing and processing biometric data for* ***a minimum population size of fifteen million (15,000,000) unique identity records***
- *Performing biometric identification and verification at a national scale with acceptable performance benchmarks*

4.2 Proven Large-Scale Deployment Experience

The proposed ABIS provider shall demonstrate:

- ***Proven experience*** *in delivering biometric identification systems for* ***large-scale national or multi-million population deployments***
- *Successful operational deployments with populations* ***equal to or exceeding 15 million records***
- *References or case studies from sovereign or government clients, where applicable*

4.3 Data Migration and Onboarding Support

The ABIS provider shall support ***biometric data migration and onboarding****, including:*

- *Ingestion of existing biometric templates and associated metadata*
- *Validation and quality assessment of migrated data*
- *Support for phased or parallel migration strategies to minimize operational risk*

The ABIS solution shall be capable of coexisting with legacy systems during transition, where required.

4.4 Biometric Services and SDK Availability

*In addition to core ABIS functionality, the biometric service provider **shall provide software development kits (SDKs)** or equivalent APIs to support the following biometric services:*

- ***Biometric quality assessment**, including quality scoring and compliance with applicable standards*
- ***1:1 biometric matching (verification)** for authentication use cases*
- ***Biometric templatization**, including secure extraction and storage of biometric templates*

These services shall:

- *Be callable independently via APIs or SDKs*
- *Support integration into enrollment, authentication, and verification workflows*
- *Not be restricted to proprietary hardware or device vendors*

4.5 Standards Compliance and Interoperability

The ABIS solution and associated biometric SDKs shall:

- *Comply with relevant **ISO/IEC biometric standards***
- *Support interoperability with the National Identification System and the CRVS platform through open APIs*
- *Allow configuration or replacement without requiring changes to the core platform architecture*

4.6 Deployment and Scalability

The ABIS solution shall:

- *Support horizontal and vertical scalability*
- *Be deployable in on-premise, private cloud, public cloud, or hybrid environments*
- *Align with the overall cloud-native and containerized architecture of the proposed solution*

5. Civil Registration and Vital Statistics (CRVS)

5.1 Event-Based Civil Registration

*The CRVS system shall be **event-driven** and support registration and management of the following life events:*

- *Birth*
- *Death*
- *Marriage*
- *Divorce*
- *Adoption and other legally defined events*

*The system shall support both **online and offline** event registration with subsequent synchronization.*

5.2 Integration Between CRVS and National ID

The CRVS system shall integrate seamlessly with the National ID Registry such that:

- *Birth registration can trigger the creation of a unique identity record*
- *Subsequent life events update the identity record, where applicable*
- *Data exchange occurs through secure, real-time, or near-real-time APIs*

6. Offline Capability and Field Operations

6.1 Offline-First Registration

*The solution shall support **offline-first operations** for both identity enrolment and civil registration, particularly in low/no connectivity environments.*

Offline capabilities shall include:

- *Secure local data storage*
- *Cryptographic protection of stored data*
- *Automated synchronization upon network availability*

6.2 Offline Registration Kits

*The solution shall support **offline registration kits** for use in remote or no-connectivity environments.*

Offline registration kits shall:

- *Capture demographic and biometric data without network connectivity*
- *Store data securely using encryption*
- *Support controlled synchronization once connectivity is restored*

Offline kits shall be suitable for use by:

- *Civil registration officers*
- *Mobile registration teams*
- *Outreach and mass enrolment programs*

6.3 Registration Kit Form Factors

*The solution shall support **multiple registration kit form factors**, including:*

- ***Tablet-based registration kits***
- ***Laptop-based registration kits***

Both form factors shall support:

- *Biometric device integration*
- *Offline data capture*
- *Secure data storage and synchronization*
- *Uniform workflows and user experience*

6.4 Global Registration Kit Vendor Ecosystem

*The solution shall be compatible with a **globally interchangeable registration kit ecosystem**, meeting the following minimum requirements:*

- *Support for **a minimum of ten (10) biometric device and registration kit vendors globally***
- *Ability to procure registration kits from multiple international or regional suppliers*
- *No contractual or technical dependency on a single hardware vendor*

This requirement is intended to:

- *Ensure supply-chain resilience*
- *Avoid hardware vendor lock-in*
- *Enable competitive procurement over the system lifecycle*

7. Security, Privacy, and Data Protection

7.1 Privacy-by-Design

*The solution shall implement **privacy-by-design and privacy-by-default** principles, including:*

- *Data minimization*
- *Purpose limitation*
- *Controlled access to sensitive data*
- *Separation of biometric and demographic data*

7.2 Security and Standards Compliance

The solution shall comply with:

- *ISO/IEC biometric and information security standards*
- *OWASP security best practices*
- *Applicable national data protection and cybersecurity regulations*

The system shall support:

- *Hardware Security Modules (HSMs) or equivalent secure key management*
- *Encryption of data at rest and in transit*
- *Comprehensive audit logging*

8. Interoperability and Ecosystem Readiness

8.1 Interoperability with Government Systems

The solution shall be designed to integrate with:

- *Existing population registers*
- *Immigration and border management systems*
- *Social protection, health, education, and other sectoral systems*

Integration shall be achieved using open standards and documented APIs.

8.2 Alignment with Digital Public Infrastructure (DPI) Principles

The solution shall align with globally recognized ***Digital Public Infrastructure (DPI)*** *principles, including:*

- *Interoperability*
- *Openness*
- *Reusability*
- *Scalability across sectors*

9. Capacity Building and Knowledge Transfer

9.1 Government Capacity Building

*The bidder shall provide a comprehensive **capacity-building and knowledge-transfer program** to ensure that:*

- *Government technical teams can operate and maintain the system*
- *Local teams can implement future enhancements independently.*

Documentation, training materials, and access to source code shall be provided as part of the engagement.

10. Evaluation Considerations (Informative)

In evaluating proposals, the Authority may consider, inter alia:

- *Maturity and production readiness of the proposed open-source platform*
- *Number of sovereign or government deployments*
- *Availability of **multiple biometric device and registration kit vendors** supported by the solution*
- *Availability of multiple certified or experienced implementation partners*
- *Proven integration between national identity and civil registration systems*
- *Demonstrated ability to operate in **offline and low-connectivity environments***
- *For ABIS, the Authority may consider the provider's demonstrated experience with large-scale deployments, modality coverage, scalability, availability of biometric SDKs, and ability to support data migration*