FEDERAL REPUBLIC OF NIGERIA

NIGERIA DIGITAL IDENTIFICATION FOR DEVELOPMENT PROJECT

TERMS OF REFERENCE

SECURITY ARCHITECT

1. BACKGROUND

Of the 187 million living in Africa's most populous country, only about 30% have had their births registered - this figure drops to 19% in rural areas and to 7% within the poorest quintile of the population. Less than 50% of residents have any form of ID card, whilst only 9% of individuals have a national ID number (NIN). Based on the Global Findex Survey[1] results of 2018, 33% of those who do not have ID cite that it is too difficult to obtain, whilst approximately 20% cite a lack of supporting documentation.

Nigeria hosts a fragmented ID landscape which incurs significant costs on the Federal Government (FGN). Over 13 government agencies (National Identity Management Commission, National Population Commission, Central Bank of Nigeria, Independent National Electoral Commission, Nigerian Communications Commission and others) and at least 3 state agencies offer ID services in Nigeria. Many of these agencies, capture biometrics and issue ID cards independently without data links with other systems, resulting in duplication and sub-optimal utilization of scarce resources.

The FGN has indicated a strong desire to harmonize the existing identification ecosystem towards developing a foundational identification platform which can be leveraged to improve service delivery. Based on completion of an initial identification ecosystem diagnostic in July 2016, the Vice President convened a workshop of all identification stakeholders in December 2016 which confirmed the need to develop a Strategic Roadmap[2] charting the way forward. The Strategic Roadmap was then prepared with the support of the World Bank Group, and highlighted the need for a minimalist, foundational, and eco-system-based approach to identification in the country. The Roadmap was endorsed by the Harmonization Committee at a second Vice Presidential Level Workshop attended by over 200+ identification stakeholders on January 31, 2018; the group moved to submit the Roadmap to the Federal Executive Council for final government endorsement.

Consequently, the FGN applied for a credit from the World Bank and intends to apply part of the proceeds of the credit to increase the number of persons in Nigeria who have government-recognized proof of unique identity that enables them to access services. The Project will be implemented by the National Identity Management Commission (NIMC) based in Abuja, Nigeria. NIMC, through the Federal Ministry of Finance, has obtained a Project Preparation Advance (PPA) to enable it finance preparatory activities for the Project. Some activities shall be retroactively financed by NIMC prior to approval of the PPA.

[1] World Bank Global Financial Inclusion (Global Findex) Database

[2] A Strategic Roadmap for Developing Digital Identification in Nigeria: Draft Report for Review, June 2017

2. OBJECTIVES OF THE ASSIGNMENT

- Defines the security architecture requirements of the enterprise
- Defines the integrity and confidentiality of information within the enterprise
- Ensures compliance of security technology suppliers
- Assures compliance of enrolment partners

3. SCOPE OF SERVICES

The Security Architect shall:

1. Plan and design the security architectures of the ID4D project, following intense research and adaptation of global-best practices to Nigeria's security laws and regulations;
2. Develop and implement coherent detailed security policies and regulations for the ID4D project;
3. Be responsible for the approval of ID4D network-related technologies (firewall, software, hardware, servers);
4. Monitor and ensure compliance of the ID4D project efforts with Nigeria and Donors' security policies;
5. Anticipate security risks of the ID4D project and provide substantial input towards managing those risks;
6. Work with ecosystem partners to institutionalise security consciousness with regards to biometric data, as required by all relevant regulations and laws;
7. Organise regular vulnerability testing and security assessments, documenting lessons learnt from such sessions;
8. Provide instant solutions to security-related incidents, while also documenting detailed analysis of incidents and lessons learnt;
9. Provide input during budget planning, to ensure maximum data security during project implementation;
10. Regularly organise security-sensitization sessions for ecosystem partners;
11. Constantly recommended cost-effective IT solutions that guarantee a secure ID4D network;
12. Ensure all ID4D documents, ranging from bidding documents to contracts, inculcate the importance of security;
13. Ensure ID4D staff and contractors' effectively handle security issues, providing solutions where needed;
14. Carry out any other relevant periodic duties assigned by the Technical Lead.

4. REPORTING, LOCATION AND TIME SCHEDULES

The Security Architect will report to the Technical Lead Project Coordinator in NIMC Headquarters Abuja.

The commencement of the services shall come into force and effect on the date (the "Effective Date") of the Client's notice the Security Architect to begin carrying out the services.

5. QUALIFICATION OF THE SECURITY ARCHITECT

The Security Architect shall have the following minimum educational qualifications and experience:

- MSc in Information Security or a related discipline, and one or more security certifications such as; Certified Information Systems Security Professional (CISSP), Certified Information Security Manager (CISM), Certified Information Systems Auditor (CISA) Certified in Risk and Information Systems Control (CRISC)
- 5 years' experience as an Information Security or Cyber Security Technical Lead or Architect
- Experience advising on and creating information security policies in accordance with Information security frameworks and regulations (e.g. ISO 27001, data protection legislation)
- Hands-on experience across multiple areas of information security e.g. vulnerability management, penetration testing mechanisms, identity access management, Data Loss Protection, SIEM resources, Risk Management, endpoint detection, Ethical Hacking Techniques and the ability to rapidly analyze security vulnerability reports.
- Demonstrable experience of technical risk analysis assessment and remediation
- Strong understanding of current trends and developments in information security
- Experience in working for any international donor-funded program will be considered an asset
- Ability to understand interoperability standards, risk models, privacy and liability policies, requirement and accountability mechanism for an identity ecosystem.
- Experience in projects involving multiple partner institutions will be considered an asset
- Fluency in written and spoken English. Local languages are an asset

6. DETAILED SKILLS AND EXPERIENCE

Area	Description
Communication between technical and non-technical	Understands security concepts deeply enough to engage with security technologists and communicate in a language that is appropriate to the audience. Able to respond to challenges.

Design secure systems	Able to design secure system architectures through the application of patterns and principles, to meet user needs whilst managing risks. Able to identify security issues in system architectures. Ability to analyze existing security systems and report possible threats and software issues, research system weakness and proffer remediable solutions.
Enabling and informing risk based decisions	Ability to implement a risk management process by performing risk assessment and evaluation; establishing the level of risk the Commission is willing to take and develop an effective risk budget and insurance. Create and implement a business continuity plan, implement compliance audit and build risk awareness amongst employees and Contractors. Capable of making and guiding effective decisions on risk, explaining clearly how the decision has been reached. Able to make decisions proportionate to the level of technical complexity and risk.
Specific security technology and understanding	Knowledge of system architectures. Able to understand the risk impact of vulnerabilities on existing and future designs and systems and identify how easy or difficult it will be to exploit these vulnerabilities. Hands on experience in security systems including intrusion detection system, anti-virus software, authentication systems, log management and auditing and network monitoring. Thorough understanding of the latest security principles, techniques and protocols.
Analysis	Able to visualise, articulate and solve complex problems and concepts by interrogating and using data or intelligence to formulate and influence plans. Able to interpret complex business and technical issues. Can identify and recognise a viable solution or control. Understands and links complex and diverse sets of information to inform the response and approach, for example identifying vulnerabilities and their impact.
Managing user privileges	Ability to establish effective management processes and regulate the use of privilege roles and accounts. Limit user privileges and monitor user activity. Control access to activity and audit logs.
Incident Management	Proven capability to establish an incident response and disaster recovery system. Ability to test incident management plans, resolve and report criminal incidents and provide incident management training to staff.

Monitoring	Ability to establish a monitoring strategy and produce supporting policies. To continuously monitor all systems and networks, analyse logs for unusual activities that could indicate an attack.
Remote and mobile working	Develop a remote or mobile working policy for all users. Apply all security baseline for all devices while protecting data both in transit and at rest.

7. FACILITIES AND INFORMATION TO BE PROVIDED

Adequate office space, with furniture and internet facilities, shall be assigned to the Security Architect.

8. ESTIMATED EFFORT LEVEL AND DURATION OF THE ASSIGNMENT

The duration of the assignment is initially for 12 months but will renewed subsequently on an annual basis subject to satisfactory performance. The contract type is Time Based.