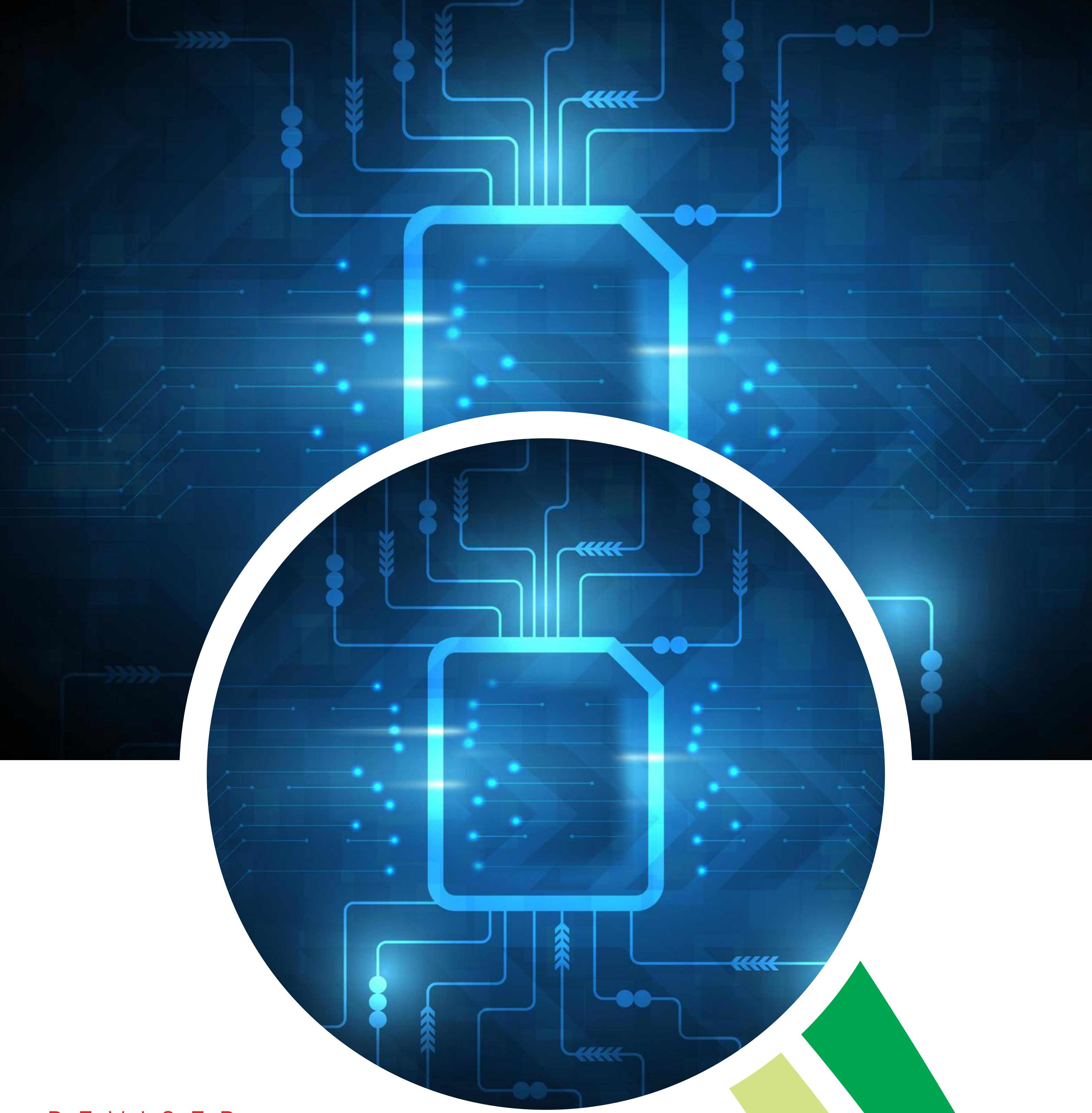


REVISED

NATIONAL IDENTITY POLICY FOR SIM CARD REGISTRATION

FEDERAL MINISTRY OF
COMMUNICATIONS AND
DIGITAL ECONOMY
Leveraging Digital Technology for
National Economic Development

REVISED
NATIONAL IDENTITY POLICY FOR SIM CARD REGISTRATION

First Edition: February 2020
Second Edition: May 2021

CONTENT

President's Mandate

The National Identity Number (NIN) is the foundational digital ID for the country; both Nigerian citizens and legal residents are expected to obtain the NIN. The Federal Government has taken steps to ensure that the NIN is used as the primary digital identity across the various sectors of the economy.

The approval of the National Digital Economy Policy and Strategy (NDEPS) showed our commitment towards the development of our Nation's Digital Economy. A digital identity system is the foundation for the development of a digital economy and the Federal Government is supporting the digital economy by actively promoting the use of NIN. To this end, we took a decision to transfer the supervision of the National Identity Management Commission (NIMC) to the Federal Ministry of Communications and Digital Economy.

The Subscriber Identification Module (SIM) has become a necessary component for citizens to access various services provided through telecommunications systems. This administration places a premium on the safety and security of Nigerians and linking the SIM to NIN will significantly enhance security. It is in line with this commitment that we have initiated a process that will require every SIM to be linked to the National Identity Number (NIN), which is the primary identity database for the country.

The NIN is a robust biometrics database that will enhance access to government services, support the private sector in providing customized services to citizens and support our efforts to secure our nation. The Revised National Digital Identity Policy for SIM Card Registration will ensure a linkage between the NIN and SIM for the development of our digital economy and the enhancement of our National security.

I have directed the Honourable Minister of Communications and Digital Economy (HMCDE) to ensure that no SIM card is allowed to access our telecommunications network unless it has a NIN attached to it. We are committed to ensuring that technology provides a platform for improving service delivery in the country and does not become a tool to perpetrate crime.

I commend the HMCDE, Dr Isa Ali Ibrahim (Pantami), for his commitment in carrying out his responsibility of developing the digital economy sector, including championing the NIN-SIM registration process.

I hereby direct the Honourable Minister of Communications and Digital Economy to coordinate the implementation of the Policy. I also urge all stakeholders to ensure compliance.

M Buhari

Muhammadu Buhari

08-03-21.

FOREWORD

The issue of unregistered and improperly registered subscriber identity module (SIM) cards had lingered, compromising national security and negatively affecting the efficiency of Nigerian security agencies. Upon my assumption of office as the Honorable Minister of Communications and Digital Economy, and as part of the agenda of President Muhammadu Buhari, GCFR, in promoting security, I directed the Nigerian Communications Commission (NCC) to conduct an audit exercise on SIM card registration in the country.

Furthermore, I directed NCC to carry out an audit exercise to discover the unregistered and improperly registered SIMs, It was discovered that there were 9.4 million improperly registered SIM cards. Considering the implication of such unregistered and improperly registered SIM cards on national security, I issued a directive for the updating of the registration of those SIM cards by 11:59pm of the 25th September 2019. Subsequently, NCC resolved the lingering issues and ensured that only those properly registered were eventually reactivated.

Mobile devices interestingly play an important role in the development of any digital economy and a digital economy is a catalyst for the growth of every sector of the economy. For example, Information and Communications Technology (ICT), which is a component of the digital economy, contributed an unprecedented 17.83% to the Nigerian GDP in the second quarter of 2020 (Q2 2020). In order to ensure the growth of the mobile ecosystem, the need for a secure and safe environment on our mobile network cannot be overemphasized. The ability to determine the real identity of a mobile user is a prerequisite for having a secure mobile network. The identity of the mobile users can be determined when the registered credentials of the SIM card user are verified against the National Identity database (NIDB), and this involves the use of the National Identity Number (NIN) issued by the National Identity Management Commission (NIMC).

Furthermore, mandating the use of NIN for SIM card registration will accelerate the growth of the national identity database as the SIM card registration database is one of the largest databases holding the digital identity of Nigerians, including biometrics and other essential information on citizens. This will enable Nigeria to take giant strides towards improving national planning, overcoming security challenges and boosting our GDP.

National digital identity will accelerate economic planning and development. It will also promote digital inclusion, digital financial services and other value-added services across the nation. It will also help Nigerian security agencies to improve their effectiveness in dealing with cybercrime, particularly in the area of digital forensics, crime tracking and identification. This Policy lays a foundation using the NIN to support the development and security of the mobile ecosystem of Nigeria. I call on all stakeholders to support in its implementation.

To achieve the set goals and mandates as mentioned above, I will be coordinating the exercise of the mandatory NIN-SIM linkage exercise as directed by His Excellency, President Muhammadu Buhari, GCFR, through his signed mandate to me.

Isa Ali Ibrahim (Pantami), PhD, FNCS, FBCS, FIIM
Minister, Federal Ministry of Communications and Digital Economy of the
Federal Republic of Nigeria

EXECUTIVE SUMMARY

The Subscriber Identity Module (SIM) registration is a mandatory requirement for all mobile phone subscribers. Subscribers must register their SIM cards with their respective Mobile Network operators (MNOs) to have access to both voice and data network services. Considering the vulnerability and security risk posed by unidentified network users, Nigeria aligned with the global best practice by mandating the collection of identity information in a Capture and Validate (C&V) Mobile SIM registration and Know Your Customer (KYC) process. The exercise entails the capturing of the identity details of the individuals associated with SIM cards, verifying such captured data and linking the NIN to the SIM.

The captured data from mobile network users normally requires a means of verification and validation, and in most countries, such verification and validation are done against a national identity database. In the absence of such validation, it is often difficult to know whether the information provided by individuals is authentic or falsified. However, the availability of a national identity document and an authentication mechanism are essential for such validation and verification. Such validation can be carried out at the point of sale or at point of activation. Regardless of the point of validation, such verification and authentication helps in limiting identity fraud and other network-related crimes.

Unfortunately, Nigeria's current SIM card registration process does not require a verifiable national identification. However, the growth of the Nigerian national identity database hosted and managed by the National Identity Management Commission (NIMC) presents a great opportunity for such verification and validation exercise at the point of SIM card registration. The current size of the NIMC database is only a fraction of the current size of the SIM registration database. A policy which requires each SIM registration to be mapped to NINs can significantly accelerate the growth of the NIMC database as the mobile phone network user database keeps growing.

Mandating the use of NIN for SIM card registration has several benefits, including improving and enhancing national security, as well as accelerating economic planning and development. It will also boost the digital economy by promoting digital inclusion and accelerating the growth of the national identity database through increased enrolment by the growing mobile phone network subscribers.

1.1 Background

The mobile network system today forms the backbone of the Nigerian communication infrastructure, delivering both voice and data services to millions of Nigerians, and also linking the nation to international telecommunication networks and the Internet. To a large extent, the global digital economy relies on the Internet and this reliance has its benefits and drawbacks. Such benefits include access to knowledge, increased collaboration and ease of online payments, amongst others. The drawbacks include cyber threats that users get exposed to and privacy concerns that they have to deal with.

The penetration of mobile networks and the increasing number of subscribers in Nigeria has also witnessed a rise in the number of malicious actors who use the mobile network to perpetrate various crimes, ranging from online fraud to terrorism. The wireless nature of these communication networks makes it possible to commit such crimes many miles away from the perpetrator, thereby making it difficult or even impossible to track, arrest and prosecute. This threat was accentuated at a time when subscribers could obtain mobile network access without providing any personal details.

The National Digital Economy Policy & Strategy (NDEPS) is anchored on 8 Pillars of the Digital Nigeria Roadmap of the country. Pillar #6 (the soft infrastructure pillar) focuses on strengthening public confidence in the use of digital technologies and participation in the digital economy. According to the NDEPS document, the Soft Infrastructure pillar will address the importance of cybersecurity and other standards, frameworks and guidelines that encourage citizens to go digital. The need for digital identity lies at the root of citizenship and service delivery in a digital economy. With identity being digitized and tied to biometrics, the National Identity Number (NIN), Biometric Verification Number (BVN), Voter IDs and SIM card registration details can provide channels for identifying citizens in order to facilitate credible transactions. One of the key Policy Objectives of Pillar #6 is support for the accelerated implementation of a Digital Identity Programme. A key implementation strategy is to Identify the barriers militating against the implementation of digital identity scheme and data harmonization in order to accelerate full scale digital identification.

1.2 SIM Card Registration

Several countries mandate the registration of pre-paid SIM cards in order to get mobile network service. This registration exercise usually requires network subscribers to provide proof of identification, personal data and in some cases, biometric information, for their mobile SIM card to be activated to enable them obtain network services, such as voice and data services. Essentially, governments adopt such registration policies as part of efforts to mitigate security concerns and address malicious activities like online-fraud and identity theft. Governments are focused on enhancing security and they have realized that SIM card registration can potentially enable new experiences for consumers by enabling access to value-added mobile and digital services that would otherwise be unavailable to them as unregistered users. Network operators also understand the loyalty they can elicit from their registered customers through Know Your Customer (KYC) initiatives.

1.3 Beyond SIM Card Registration

The rapid growth of the digital economy makes it increasingly important for citizens to have a secure digital identity, which is very pivotal in promoting the participation of the citizens in the digital economy. However, the citizens' identity based on SIM card registration alone cannot provide such digital identity, though it provides a stop-gap in the process of achieving such secured robust digital identity.

Verification against a national identity database provides the most comprehensive SIM registration solution, which gives the government, security agencies and mobile network operators a high degree of confidence that the details provided by the subscriber are true and accurate.

Currently, the national identity database managed by NIMC and the SIM card registration database managed by NCC are managed in silos. The SIM card registration process does not mandate the presentation of the National Identification Number (NIN) for inclusion in the SIM card registration database. Verification and validation of subscriber information are largely absent, constituting a loophole in the exercise, thereby posing security challenges which the exercise was intended to address in the first place.

In order to promote and strengthen a national digital identity, both the NIN and the mobile network identity of citizens must be matched and securely linked through a Capture and Validate (C&V) SIM card Registration process, which requires the mobile network operators to validate their customers' credentials against a central government database, which in the case of Nigeria is the National Identity database (NIDB). The verification confirms the subscriber identity through the NIN and makes available the personal details of the subscriber, through an authorized channel, in a secured manner.

1.4 Digital Identity and Digital Economy

Various stakeholders agree that in order to create a safe and resilient digital economy, we must achieve a traceable digital identification system that would mitigate challenges that contribute to the issues associated with digital services. The Federal Ministry of Communications and Digital Economy is therefore committed to ensuring that all the necessary policies and communications infrastructure are put in place to support the digital economy and enhance the security of Nigerians.

The ability to determine and confirm one's digital identity is important in securing rights and access to a number of life-enhancing services including healthcare, voting, education, financial services, employment and social protections. As progress is made in the digital age, digital identification becomes more critical to having access to mobile connectivity and a range of mobile services especially across more than 140 countries where the mandatory SIM card registration policies are in place. According to the GSMA reports, the World Bank GSMA Report: Mandatory registration of prepaid SIM cards - Addressing challenges through best practice, April 2016 estimates that 1.1 billion people worldwide lack any legal identification, predominantly in Africa and South Asia . Furthermore, World leaders at the World Economic Forum 2018 have made effort in strengthening multi-stakeholder cooperation and collective action to pursue the opportunities that come with digital identities and ensure the protection of rights in a sustainable and responsible manner.

It is important to note that the United Nations had also recognized the significance of addressing the identity gap through its Sustainable Development Goal (SDG) to provide legal identity for all, including birth registration by 2030. The mobile industry was the first to publicly commit to addressing all 17 SDGs. With a global subscriber base that surpassed 5 billion in 2017, the mobile ecosystem has created a global digital platform that is increasingly connecting everyone and everything.

1.5 The Journey So Far

The NCC officially announced that the registration of old SIM Cards concluded on the 30th of June, 2013. However, there were cases of millions of unregistered and improperly registered SIM cards still accessing mobile network services. The situation created loopholes that could be exploited by criminals to compromise national security.

Following the timely directives of the Honourable Minister of Communications and Digital Economy, Dr Isa Ali Ibrahim (Pantami) FBCS, FNCS, FIIM, the issue was resolved and those millions of unregistered or improperly registered SIM card were either properly registered and reactivated or disconnected altogether. This bold step significantly improved security across the nation by helping the security agencies to track and trace crimes committed using mobile phones and other mobile communication devices.

To sustain the gains of such an effort, the Honourable Minister urged key stakeholders like the Minister of Defense, Minister of Interior, National Security Adviser, Director General, Department of State Services, Inspector-General of the Nigerian Police Force, the Controller-General of the Nigerian Customs Service to collaborate with the Federal Ministry of Communications and Digital Economy by contacting the Ministry in the event of a crime abetted by the use of SIM cards and other mobile devices. This is to enable the ministry to use information from its databases and other audit trails in order to furnish the security agencies with relevant information for further investigation. These steps will enhance the security of the mobile networks in the country and will encourage citizens to feel at ease when using services provided on the networks.

POLICY ROADMAP

2.1 Vision

To develop a telecommunications sector where digital identity unlocks access to mobile-enabled services and provides security for all.

2.2 Mission

We develop a telecommunications sector with effective digital identity-based SIM card registration process that creates value and prosperity for all.

2.3 Authority

This Policy has been developed under the authority of the Honourable Minister of Communications and Digital Economy in line with the following sections of the Nigerian Communications Act 2003 (NCA 2003):

> ***i. Subsection 23(a): The Minister shall have the following responsibilities and functions pursuant to this Act— the formulation, determination and monitoring, of the general policy for the communications sector in Nigeria with a view to ensuring, amongst others, the utilisation of the sector as a platform for the economic and social development of Nigeria; and***
>
> ***ii. Subsection 25(1): The Minister shall, in writing, from time to time notify the Commission or and express his views on the general policy direction of the Federal Government in respect of the communications sector.***

This Policy can be cited as "Revised National Digital Identity Policy for SIM Card Registration." and shall come into effect the date of the signature.

2.4 Policy Objectives

The objectives of the National Digital Identity Policy for SIM Card Registration are as follows:

i. to mitigate identity fraud and other online crimes ;

ii. to curtail compliance abuse by mobile network operators and subscribers;

iii. to establish customer identity that will be useful for offering value-added services like the Know Your Customers (KYC) initiatives;

iv. to validate SIM card registration records and allow it to be used as a digital identity to authenticate subscribers for e-government and other value-added services;

v. to enhance the validity of the SIM card registration data and make it effective for use by security agencies for crime mitigation;

vi. to serve as a catalyst for the rapid growth of the national identity data base managed by NIMC;

vii. to facilitate efficient and secure SIM-NIN linkage processes and ensure adequate consultations and engagements are carried out for successful and efficient implementation of the processes involved;

viii. to promote collaboration among all relevant stakeholders in achieving the mandatory SIM-NIN linkage exercise;

ix. to develop robust, and reliable guidelines and secure processes for new SIM registrations, SIM replacements/swaps, Corporate Activations and Machine-to-Machine (M2M) activations in away that prevents and mitigates incidences of fraudulently registered SIM cards and associated SIM related crimes;

x. to develop guidelines for engagement/accreditation of dealers and agents that will conduct the transactions mentioned in (vii) above in a way that prevents fraudulent registration;

xi. to ensure that processes put in place for the Mandatory SIM-NIN linkage are secure and reliable;

xii. to ensure compliance with NDPR in handling citizens data warehoused in all the institutions involved in achieving the Mandatory SIM-NIN linkage; and

xiii. to implement a robust SIM Identity Management Solution for effective implementation of the Federal Government directive on mandatory use of National Identification Number (NIN) and to reduce incidence of fraudulently registered SIMs (pre-registered SIMs) to the barest minimum.

2.5 The Guiding Principles

To provide direction for the effective implementation of the National Digital Identity Policy for SIM Card Registration, the following guiding principles shall be adhered to:

i. the policy shall take into consideration the importance of citizens' personal information and privacy;

ii. the policy shall adopt tokenization and other proactive measures, in line with international best practice to protect the privacy of citizens and residents when their personal data is accessed by mobile network operators for the purpose of SIM card registration data verification and validation;

iii. adherence to Nigeria Data Protection Regulation;

iv. the policy shall promote measures to make access to NIMC's national identity database secure and seamless;

v. the Improved NIN slips (standard and premium), as well as the MobileID, collectively called Digital Identity Tokens, shall be deemed valid means of Identification, subject to the tokens being verified each and every occasion they are presented;

v. the policy shall ensure the sensitization of the citizenry on the values and benefits of a national digital identity.

POLICY FOCUS AREAS

To successfully strengthen the registration process of new mobile phone subscribers and to also ensure that the data captured for existing subscribers are all tied to the National Identification Number (NIN) domiciled in NIMC, there is the need to focus on key areas that are more relevant and impactful. The following are such areas:

i. collaboration with stakeholders;

ii. development of customized application software and database;

iii. data management; and

vi. template for individual New Sim Activations, SIM Swap/Replacement, Corporate Activations and Machine-to-Machine Activations.

3.1 Collaboration with Stakeholders

The implementation of a capture and validate (C&V) SIM card registration process requires collaboration with many stakeholders, cutting across several government institutions and network operators. Such institutions include NCC, NIMC, security agencies and the mobile network operators. Due to several ramifications like legal and technical issues, along with financial requirements, strong backing and support from the government is required.

SIM Registration can be a demanding process for the mobile network operators and consumers as well, as such, it is necessary to mitigate the challenges in both new registration and re-registration for consumers. The government can help with logistical support and consumer awareness campaigns, as well as help to cushion the financial burden on consumers and the network operators. Government support can facilitate the success of the exercise.

SIM card registration programs are usually expensive to implement as they involve the development of software systems, logistics and other costly aspects. They also require hardware provisioning –computing devices, biometric capture hardware and so on. However, to reduce the cost overhead, the policy implementation will leverage the existing assets used for the old SIM card registration process.

The security agencies are key stakeholders in the implementation of this policy, hence it is important to engage them in order to ensure that their recommendations are taken into consideration and their concerns are adequately addressed. Also, mobile network operators must be fully engaged and supported to ensure a seamless implementation. Timely consultation with the mobile network operators will help to streamline the entire implementation process and avoid unnecessary disruption. Furthermore, NCC and NIMC must intensify their collaboration to ensure smooth enrollment of new subscribers and updating of existing customer data with the NIN. Similarly, contributions must be sought from all other stakeholders involved for a solution that would be practical and acceptable to all concerned.

The objectives of adequate collaboration with stakeholders include:

i. to ensure that the developed solutions minimize disruption of the SIM registration process;

ii. to give the assurance of an encompassing identity process for all registered users, without exclusion;

iii. to ensure judicious use of funds from government and other donor agencies to support the national digital identity registration exercise;

iv. to ensure that mobile network operators do not pass on any increased costs to their subscribers;

v. to ensure that capital investment budgets of the mobile network operators are allocated to network investment and not SIM card registration requirements;

vi. to minimize financial costs to consumers and mobile network operators involved in the registration process, as well as mitigate the risks that consumers face;

vii. to ensure that recommendations from all security agencies are duly not-ed and considered for implementation, where appropriate;

viii. to consult all stakeholders before, during and after the exercise;

ix. to consider issues of logistics and legal implications for the SIM registration exercise with NIN;

x. to consider the practical implications of any registration requirements; and

xi. to provide adequate information to the stakeholders on how the new SIM registration guidelines will help the security agencies.

3.2 Development of Customized Application Software and Database

To facilitate the implementation of the national digital identity system, an automated solution must be provided during SIM card registration to help in securely accessing NIN data from NIMC database for the verification and validation of personal data provided by subscribers at the point of registration.

With over 53 million registered NIN in the NIMC database, there is the need for the software solution to have robust and secure features. This is necessary to synchronize the NIN database with the NCC SIM card registration database and provide relevant information required for new registrations and the update of already registered subscribers. Overall, the software solution will automate the registration of SIM cards by collecting, verifying, and sending the subscriber credentials including bio-data, document copies, and other relevant information to the databases of NCC and mobile network operators.

Nigerian citizens and legal residents will require NIN to access relevant personal data from the NIMC register, while foreign citizens who are in Nigeria for less than 2 years will require their resident permit (for legal residents), visas (for short term visitors/tourists) and their international passport. If additional data is required in the case of foreign citizens, this can be drawn from the Nigerian Immigration Service (NIS) database. The NIS database can provide visa information and residence permit data.

The objectives of the development of a customized application software and database include:

i. to develop a robust and scalable solution that works across all platforms;

ii. to test and validate the solution comprehensively before implementation to avoid subscriber disenfranchisement;

iii. to set a realistic timeline for the implementation, taking into consideration the size of the project;

iv. to support the process by running nationwide sensitization and awareness campaigns designed to encourage people to update their SIM card registration;

v. to promote an inclusive solution that encourages subscribers to take part in the exercise and not exclude vulnerable citizens;

vi. to ensure that subscribers use the required documents in order to minimize disruption and deactivations;

vii. to develop and implement a solution that promotes local content utilization in both hardware and software; and

viii. to provide features that simplify the registration of customers.

3.3 Data Management

Digital identity data comprising both national identity data from NIMC and NCC SIM card registration constitute a very important asset with great relevance to the digital economy. The digital identity data has potential for fast growth, with its sensitivity as it holds privacy information, a robust and secure data management and protection policy must be ensured. Particularly, a strong data loss prevention and recovery plan must be instituted so that in the event of data loss, data can be recovered and restored with minimal downtime and disruption to digital services. Data management is important during the registration process as it will prevent conflicts over data quality that can arise in subscribers' effort to revalidate their registration details.

NIMC, as the government regulator, will continue to be responsible for the data management process, which shall include adherence to data protection policies, data backup and restoration plans, etc.

The objectives of the data management process include the following:

i. to specify data access requirements and access protocols that will ensure secure access to the digital identity data;

ii. to develop fast and reliable access processes for the registration and verification exercise;

iii. to provide subscribers access to their own data, and provide an avenue for making corrections and updates where necessary;

iv. to create guidelines for data acquisition, processing and storage in line with Nigeria Data Protection Regulation (NDPR) and other relevant regulatory instruments;

v. to protect the national digital identity data from fraudulent and exploitative usage by any entity involved in the capturing and storage of such data; and

vi. to develop and promote the use of digital identity data for digital services across all sectors of the digital economy.

3.4 Template for New Activations

Further to the directive to suspend the sale and activation of new SIM Cards issued to Mobile Network Operators (MNOs) on 7th December, 2020, it became necessary to develop a new template to provide a secure process for new Registrations and SIM replacements/swaps. The new SIM Activation Process in adherence to the directive of Government on the mandatory linkage of National Identification Numbers (NIN) with the subscribers SIM Registration Record will facilitate the following:

i. harmonize the SIM Registration (SIMREG) and NIN details to improve the integrity and consistency of the SIM Registration Records;

ii. enhance the security of lives and property;

iii. eliminate the practice of obtaining pre-registered/fraudulently registered SIMs;

iv. provide an effective mechanism to potentially institute an industry-wide subscription;

v. to establish a template for the new guidelines that provides the steps to be implemented by the regulatory institutions; and

vi. strengthen the SIM Replacement process to avoid fraudulent SIM Swaps.

Accordingly, below are the proposed guidelines and processes for new Registrations, SIM replacements/swaps, Corporate SIM registrations and Machine-to-Machine (M2M) activations as well as guidelines for engagement/accreditation of dealers and agents that will conduct the aforementioned transactions. This will ensure a secure process and mitigate incidences of fraudulently registered SIMs and associated SIM related crimes. It is important to note that seamless verification of subscribers NIN is essential to the successful implementation of the mandatory use of NIN policy in the Telecommunications Industry. It is therefore imperative that NIMC capacity is strengthened to ensure availability of seamless NIN verification services going forward.

3.5 Device Management System (DMS)

With the aim to curtail the counterfeit mobile phone market, discourage mobile phone theft, enhance National Security, protect consumer interest, increase revenue generation for the government, reduce rate of kidnapping, mitigate the use of stolen phones for crime, and facilitate blocking or tracing of stolen mobile phones and other smart devices, one of the means to achieve this is through the deployment of Device Management System (DMS).

The implementation of a Centralized Equipment Identity Register (CEIR) otherwise known as Device Management System (DMS) will serve as a repository for keeping records of all registered mobile phones' International Mobile Equipment Identity (IMEI) and owners of such devices. IMEIs that have been reported as either stolen or illegal will be shared through the DMS to all the operators and service providers. The purpose is to ensure that such devices do not work even if different SIM Cards are inserted in those devices.

DMS will also provide access to all operators to cross-check the IMEIs and their status before allowing a device to become active on their network. Furthermore, registered mobile phone technicians will also be provided with an interface to check IMEIs and ensure it has not been reported as stolen or illegal before they render their technical services.

To achieve this, the Nigerian Communications Commission (NCC) would be responsible for the implementation and management of the DMS to achieve the policy objectives.

Accordingly, His Excellency, President Muhammadu Buhari, GCFR has directed that the Device Management System should be implemented within three months.

The objectives of implementing the DMS include the following:

i. to register and capture the IMEIs of all mobile phones and other smart devices on the DMS which will serve as a repository for sharing data of stolen devices across all networks;

ii. to ensure all un-registered devices do not work in any of the Networks in Nigeria;

iii. to ensure every reported IMEIs for stolen and illegal mobile phones and other smart devices are blacklisted and shared with all operators across all networks;

iv. to mitigate Mobile Phone theft and protect Nigerians from been attacked to snatch their mobile phones and other smart devices;

v. to blacklist and render all stolen Mobile Phones and other Smart Devices valueless in the Nigerian Mobile Phones Market;

vi. to ease the use of mobile phones and other smart devices in all public places without fear of been attacked by mobile phone snatchers;

vii. to facilitate the use of digital technology solutions to address key issues bothering Nigerians in the Tele communication Sector; and

viii. to facilitate the implementation of Device Management System in Nigeria in accordance with best global practice.

3.6 SIM Identity Management Solution

A robust SIM Identity Management Solution should be deployed for effective implementation of the Federal Government Directive on Mandatory Use of National Identification Number (NIN) and to reduce incidence of fraudulently registered SIMs (pre-registered SIMs) to the barest minimum. Some of the key features of the proposed Solution are as follows:

i. real time monitoring and authorization of SIM Registration and SIM Replacement transactions in accordance with the NIN policy;

ii. collation and linkage of registered SIMs on all networks to users NIN;

iii. uniform Software Application (Software Development Kit (SDK) with device location tracking capabilities to be deployed on all SIM Reg Terminals; and

iv. monitoring and Management of data capture devices (including identities of SIM Registration Agents) with capabilities to disable and blacklist devices as well as Dealers/Agents found to be carrying out spurious SIM Registration and SIM Swap transactions.

POLICY IMPLEMENTATION AND REVIEW

The National Digital Identity Policy for SIM Card Registration will be implemented in coordination with all relevant stakeholders, and its impact on both the digital economy and national security will be carefully monitored. A review mechanism shall also be put in place to continuously assess the performance and impact of the policy, and where necessary adjustment shall be made to enhance the effectiveness of the policy.

4.1 Implementation Strategies

The Nigerian Communications Commission (NCC), under the supervision of the Honourable Minister of Communications and Digital Economy, shall oversee the implementation and management of the National SIM Registration Database. As such, NCC will be charged with the responsibility of implementing this policy and have oversight of its strategies, standards, guidelines and frameworks in order to improve the identity and security management of mobile phone subscribers in Nigeria.

In addition to the implementation of the policy and its management, NCC will do the following:

i. support the implementation of guidelines of the policy for making NIN a pre-requisite for SIM card registration;

ii. design the necessary framework for the policy deployment throughout the country;

iii. develop and implement flexible standards that can accommodate changes in identity and security management technology for the registration of mobile phone subscribers;

iv. ensure that the developed registration solution takes a long-term perspective and mitigates the risk of excluding vulnerable subscribers from mobile and digital services;

v. collaborate with mobile network operators and other stakeholders before, during and after the implementation exercise, while balancing national security demands against the protection of citizens' rights;

vi. ensure that the developed registration solution creates maximum utility for citizens and legal residents;

vii. develop the legal contracts, applications, fees and licenses to facilitate the efficient implementation of the policy in the telecommunications sector;

viii. Support the drive for the acceleration of NIN enrolment throughout the country;

ix. provide the public with clear and accurate information on procedures, requirements, and opportunities available due to the policy;

x. provide clear guidelines on procedures for coordination with mobile network operators and other stakeholders; and

xi. develop systems to maximize the usefulness and accessibility of information for all data subjects in the SIM database, including ensuring that such information is secured and available online.

4.2 Monitoring and Evaluation

The following key performance indicators (KPIs) shall be carefully monitored, particularly within the first year of the implementation of the policy:

i. successful launching of the customized application and database;

ii. successful integration of the customized application with the various applications run by NCC, mobile network operators and NIMC;

iii. level of enhancement of the enrolment processes and methodology, taking into consideration the speed and number of enrolments per month;

iv. level of assignment of NIN to already registered SIM cards; and

v. the identification and deactivation of registered SIM cards with no NIN on the SIM database.

GUIDELINES

5.1 Guidelines for New Sim Acquisition and Activation

The objective is to harmonize SIM Reg.KYC with NIMC/NIN details (demographics and biometrics). Furthermore, use of NIN is mandatory for SIM Sales/Acquisition and SIM Replacement. Consequently, NIMC/NIN is the reference /foundational database.

A) Scenarios

New SIM Acquisition / Sales are grouped into scenarios such as:

i. new Customers with NIN requesting New SIM;

ii. existing Customers with NIN requesting additional SIMs;

iii. MNP customers with NIN requesting Mobile number porting;

iv. customers (new & existing) requesting New SIM or Porting without NIN;

v. recycling of Mobile Station International Subscriber Directory Number (MSISDNs) with NIN in adherence to the Quality of Service Regulations 2013;

vi. new SIM purchase by registered corporate organisations; and

vii. guidelines for Diplomatic Missions.

B) General Guidelines for New Sim Acquisition and Activation

The guidelines for New SIM acquisition and activations are as follows:

i. a Service Level Agreement (SLA) will be required. In the event that NIMC consistently falls below the SLA, the MNOs are allowed to activate new SIMs based on basic NIN verification, Facial Image returned from NIMC will be matched against customer Live Image (matching will initially be by eyeballing;

ii. MNOs will capture Customer Live Image & Fingerprint to complete SIMReg KYC (Minimum 4 fingerprints (FP) for onward transfer to the National SIM Database; and

iii. Facial Image Verification may also be utilized as a means of biometric verification.

C) New SIM Acquisition/SIM Sales Guidelines

The new SIM acquisition/SIM sales guidelines are as follows:

i. mandatory use of NIN for verification of Customer Identity;

ii. use of other forms of IDs shall not be mandatory except for customers exempted from NIN (foreigners);

iii. use of other forms of IDs such as Residence/Work Permits, Visitors entry Visas and foreign Customer travel documentsf or foreign customers exempted from NIN;

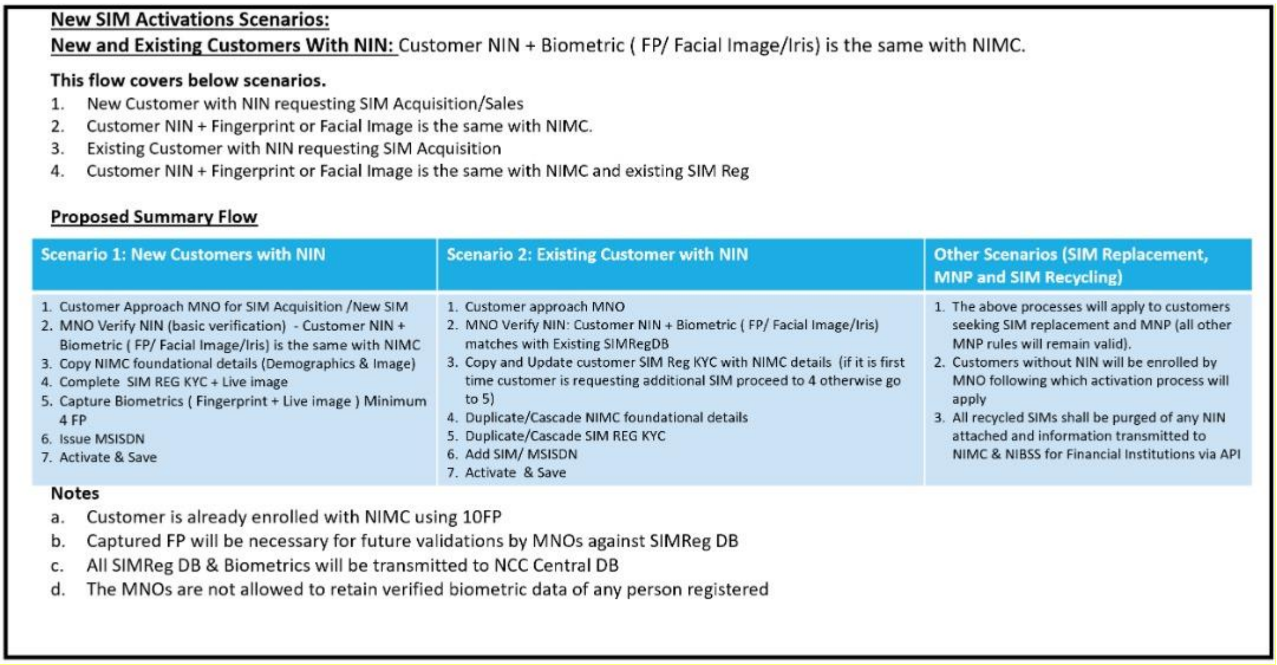
iv. for foreigners exempted from NIN, SIM activations should be tied to their Visa permits –Activation window should be in line with duration of stay on visa. Additional measures being discussed by the technical team to further strengthen this process as may be required;

v. the process provides the opportunity to harmonize customer SIM Reg KYC with NIMC and adopt NIMC foundational demographics data;

vi. NIN becomes customer's unique ID across all Mobile Network Operators (MNOs) ; and

vii. the approach will make it easier to identify the number of SIMs allocated to a customer per MNO and across the industry;

Summary Flow



New SIM Activations Scenarios:

New and Existing Customers With NIN: Customer NIN + Biometric (FP/ Facial Image/Iris) is the same with NIMC.

This flow covers below scenarios.

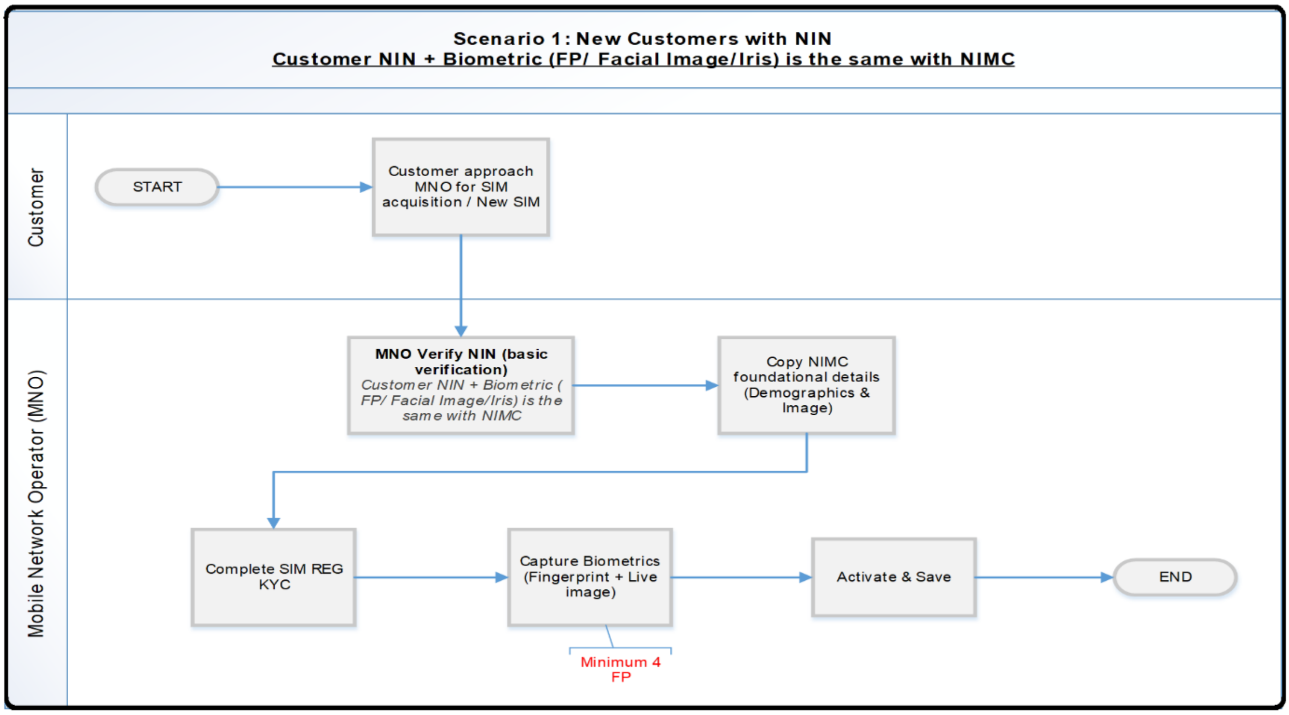
1. New Customer with NIN requesting SIM Acquisition/Sales
2. Customer NIN + Fingerprint or Facial Image is the same with NIMC.
3. Existing Customer with NIN requesting SIM Acquisition
4. Customer NIN + Fingerprint or Facial Image is the same with NIMC and existing SIM Reg

Proposed Summary Flow

Scenario 1: New Customers with NIN	Scenario 2: Existing Customer with NIN	Other Scenarios (SIM Replacement, MNP and SIM Recycling)
1. Customer Approach MNO for SIM Acquisition /New SIM 2. MNO Verify NIN (basic verification) - Customer NIN + Biometric (FP/ Facial Image/Iris) is the same with NIMC 3. Copy NIMC foundational details (Demographics & Image) 4. Complete SIM REG KYC + Live image 5. Capture Biometrics (Fingerprint + Live image) Minimum 4 FP 6. Issue MSISDN 7. Activate & Save	1. Customer approach MNO 2. MNO Verify NIN: Customer NIN + Biometric (FP/ Facial Image/Iris) matches with Existing SIMRegDB 3. Copy and Update customer SIM Reg KYC with NIMC details (if it is first time customer is requesting additional SIM proceed to 4 otherwise go to 5) 4. Duplicate/Cascade NIMC foundational details 5. Duplicate/Cascade SIM REG KYC 6. Add SIM/ MSISDN 7. Activate & Save	1. The above processes will apply to customers seeking SIM replacement and MNP (all other MNP rules will remain valid). 2. Customers without NIN will be enrolled by MNO following which activation process will apply 3. All recycled SIMs shall be purged of any NIN attached and information transmitted to NIMC & NIBSS for Financial Institutions via API

Notes

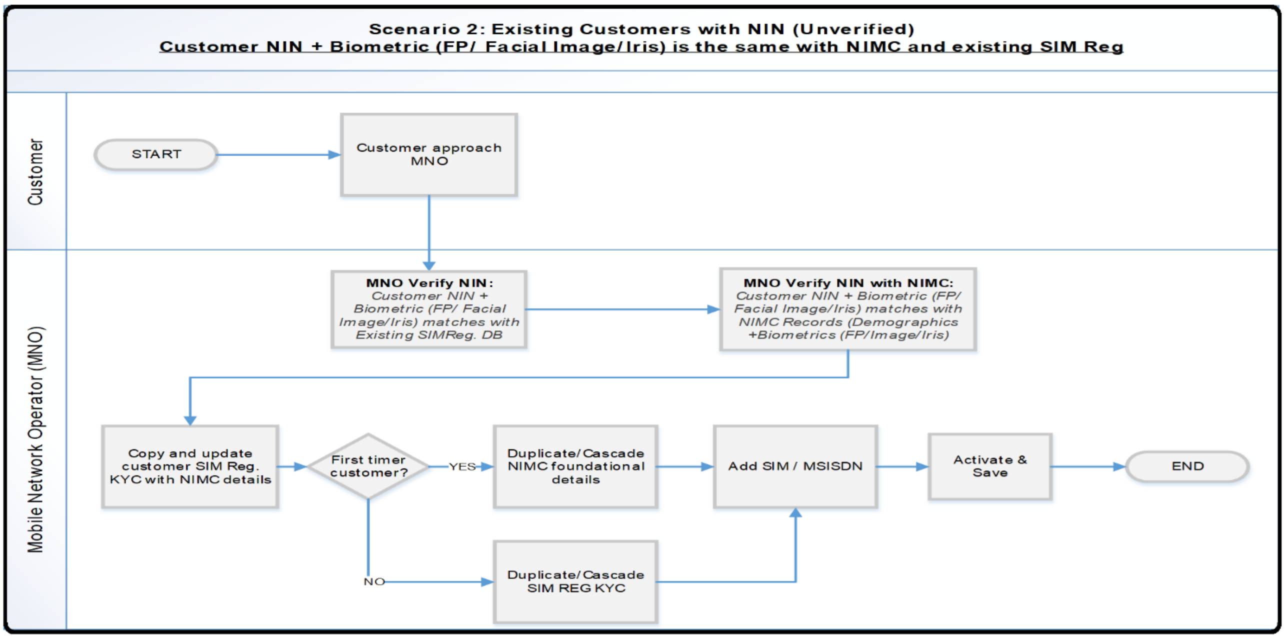
a. Customer is already enrolled with NIMC using 10FP
b. Captured FP will be necessary for future validations by MNOs against SIMReg DB
c. All SIMReg DB & Biometrics will be transmitted to NCC Central DB
d. The MNOs are not allowed to retain verified biometric data of any person registered



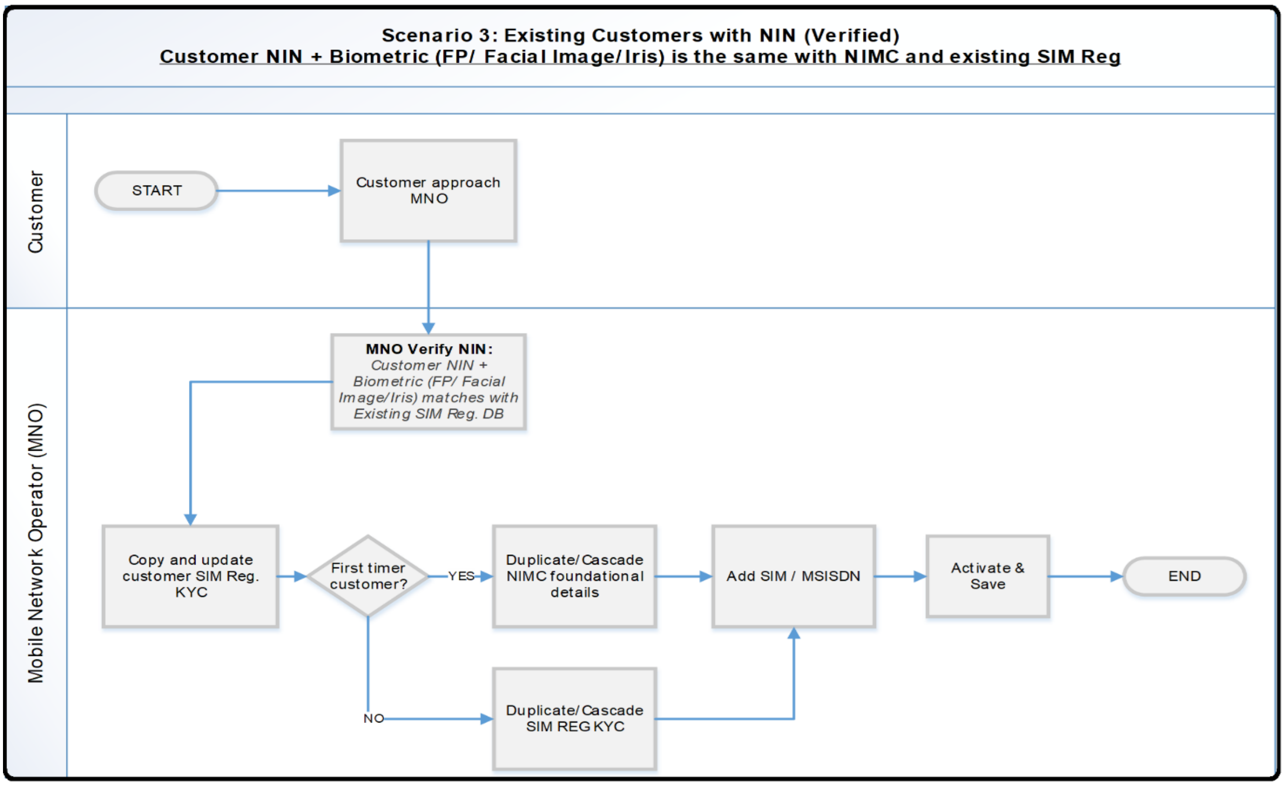
Scenario 1: New Customers with NIN

Customer NIN + Biometric (FP/ Facial Image/Iris) is the same with NIMC

Customer
Mobile Network Operator (MNO)
START
Customer approach MNO for SIM acquisition / New SIM
MNO Verify NIN (basic verification)
Customer NIN + Biometric (FP/ Facial Image/Iris) is the same with NIMC
Copy NIMC foundational details (Demographics & Image)
Complete SIM REG KYC
Capture Biometrics (Fingerprint + Live image)
Minimum 4 FP
Activate & Save
END


Scenario 2: Existing Customers with NIN (Unverified)
Customer NIN + Biometric (FP/ Facial Image/Iris) is the same with NIMC and existing SIM Reg

Customer
Mobile Network Operator (MNO)
START
Customer approach MNO
MNO Verify NIN: Customer NIN + Biometric (FP/ Facial Image/Iris) matches with Existing SIMReg. DB
MNO Verify NIN with NIMC: Customer NIN + Biometric (FP/ Facial Image/Iris) matches with NIMC Records (Demographics +Biometrics (FP/Image/Iris)
Copy and update customer SIM Reg. KYC with NIMC details
First timer customer?
YES
NO
Duplicate/Cascade NIMC foundational details
Duplicate/Cascade SIM REG KYC
Add SIM / MSISDN
Activate & Save
END


Scenario 3: Existing Customers with NIN (Verified)
Customer NIN + Biometric (FP/ Facial Image/Iris) is the same with NIMC and existing SIM Reg

Customer
Mobile Network Operator (MNO)
START
Customer approach MNO
MNO Verify NIN: Customer NIN + Biometric (FP/ Facial Image/Iris) matches with Existing SIM Reg. DB
Copy and update customer SIM Reg. KYC
First timer customer?
YES
NO
Duplicate/Cascade NIMC foundational details
Duplicate/Cascade SIM REG KYC
Add SIM / MSISDN
Activate & Save
END

5.2 Guidelines for SIM Replacement

A) SIM Replacement Process Guidelines

The SIM replacement process guidelines are as follows:

1. use of NIN for SIM Replacement is Mandatory;

2. NIMC/NIN is the Reference Identity DB ;

3. MNOs seek to harmonize SIM Reg. KYC with NIMC/NIN details (demographics and biometrics) ;

4. SIM replacement process captures seven (7) Scenarios as follows: -

i. lost SIM Replacement- Customer Fingerprint is the same with SIM Reg and NIMC;

ii. lost SIM Replacement -Customer Fingerprint is different from SIM Reg and NIMC;

iii. SIM Upgrade: (Existing SIM should be in possession and Active)- Customer Fingerprint is the same with SIMReg & NIMC;

iv. SIM Upgrade: (Existing SIM should be in possession and Active)- Customer Fingerprint different from SIMReg;

v. SIM Replacement Proxy;

vi. lost SIM Replacement (Amputees)-Customer facial image is the same with SIM Reg and NIMC (Amputee Flag is required from NIMC);

vii. lost SIM Replacement Exception Handling: - (Amputees)- Customer facial image is different with SIMReg (Amputee Flag is required from NIMC);

5. NIN provides valid means of Identity for customers, other means of Identity shall no longer be required for persons eligible to obtain NIN;

6. where Customer Fingerprint or Image match NIMC and SIM Registration Records, other forms of validations should not be mandatory –i.e. Fixed Dialing Number (FDN), Last Recharge details etc.;

7. where Customer Fingerprint or Image does not match SIM Reg , Usage details should be validated , if successfully validated , provide service,

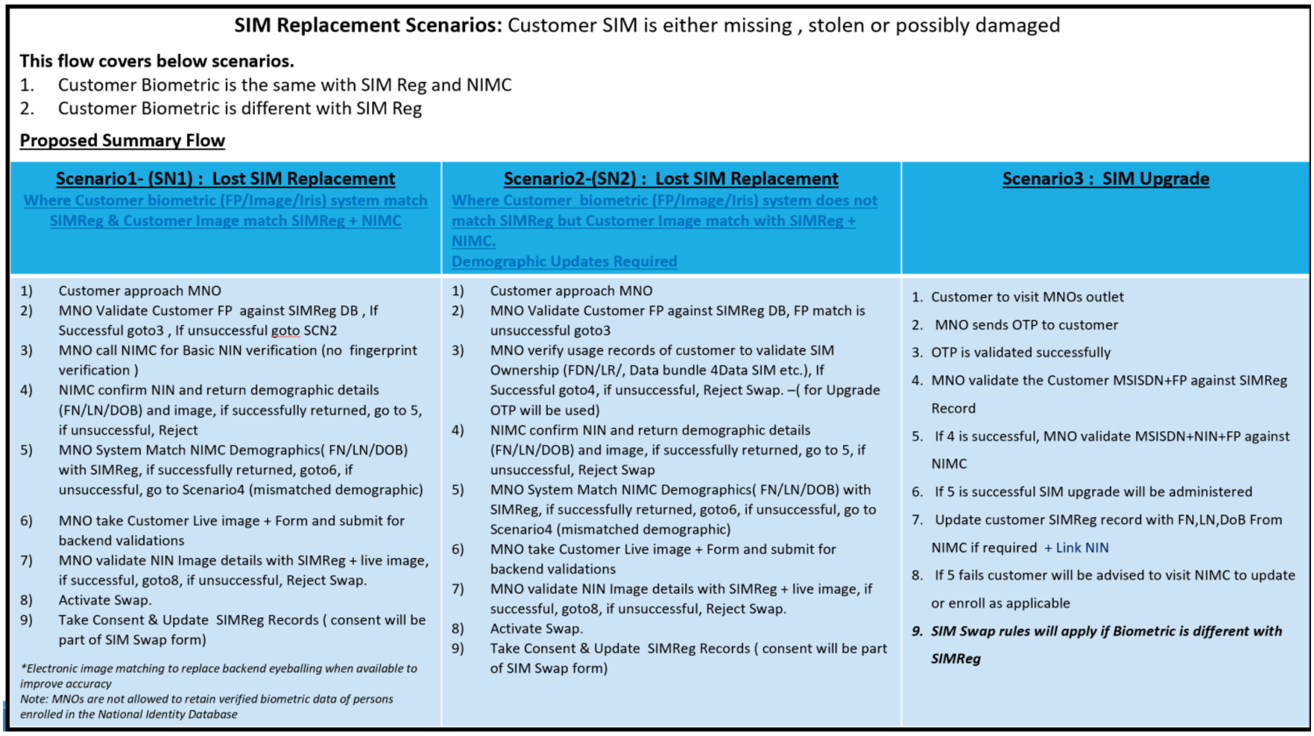
get consent and update customer SIM Reg records with NIMC records (Swap Forms can be updated with consent);

8. capturing of live image remains necessary;

9. use of NIN provides opportunity to harmonize SIM Reg KYC of Walk-in Customers with NIMC; and

10. service Availability SLA should be defined and agreed with NIMC.

Summary Flow



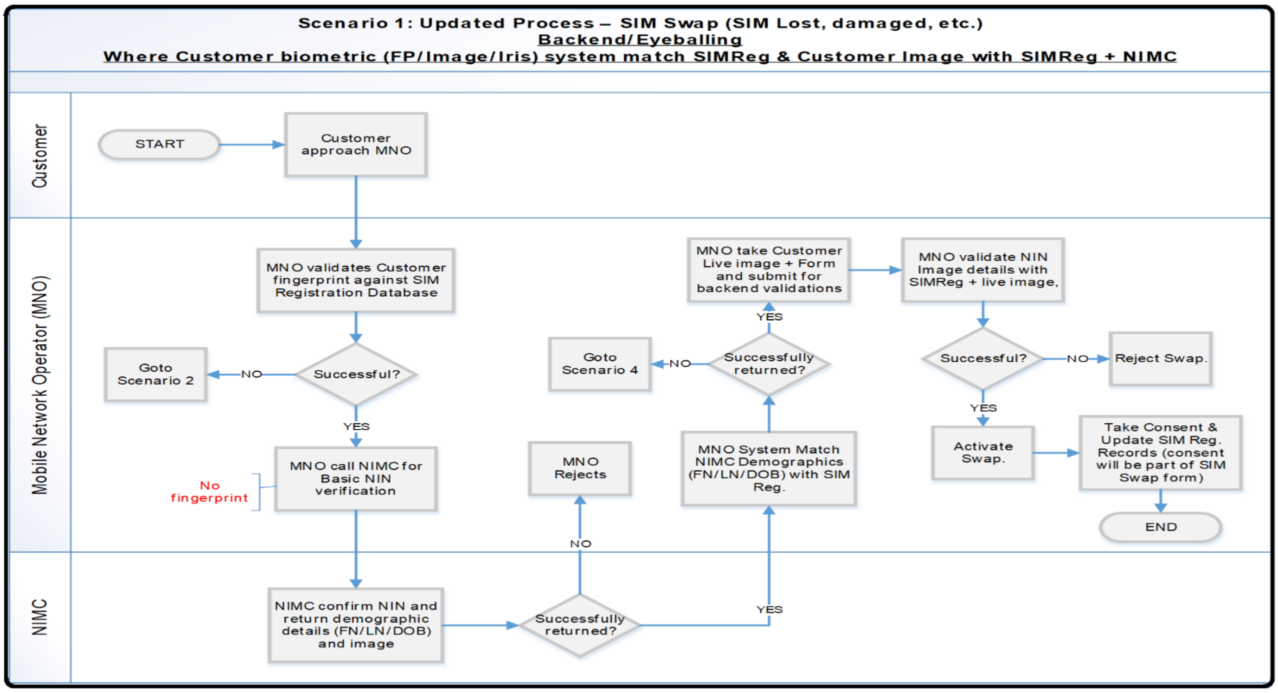
SIM Replacement Scenarios: Customer SIM is either missing , stolen or possibly damaged

This flow covers below scenarios.

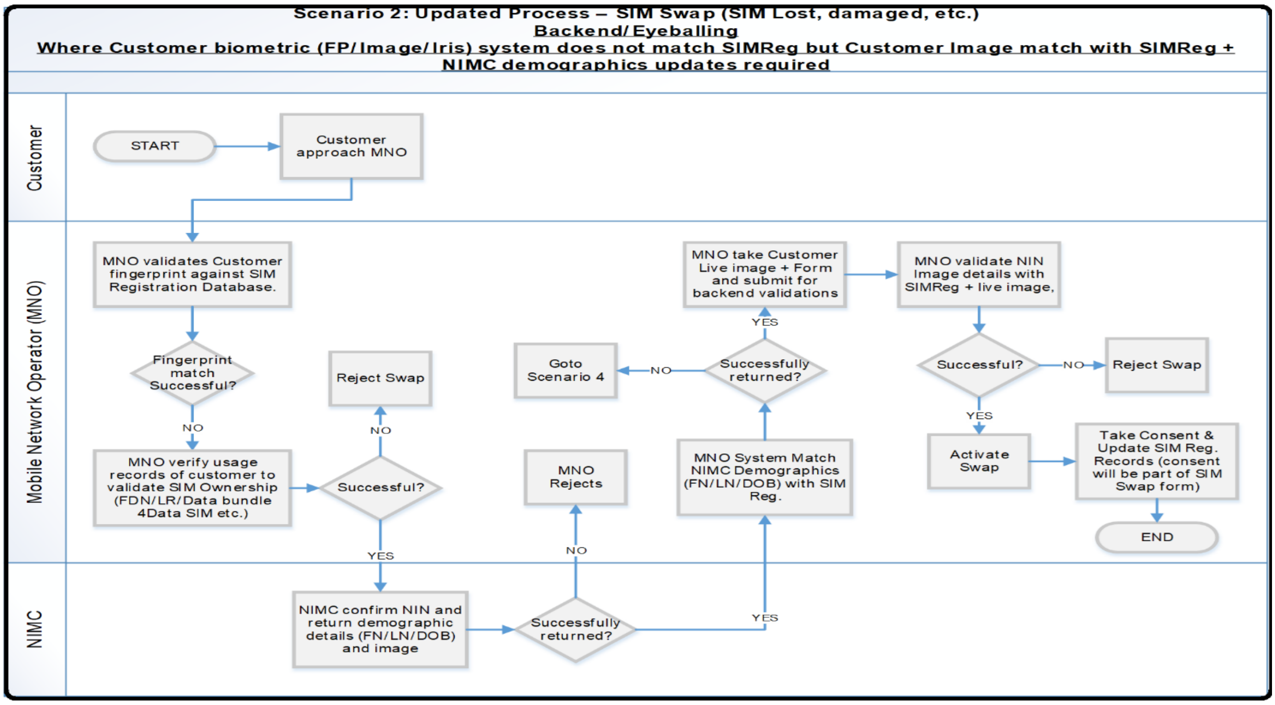
1. Customer Biometric is the same with SIM Reg and NIMC
2. Customer Biometric is different with SIM Reg

Proposed Summary Flow

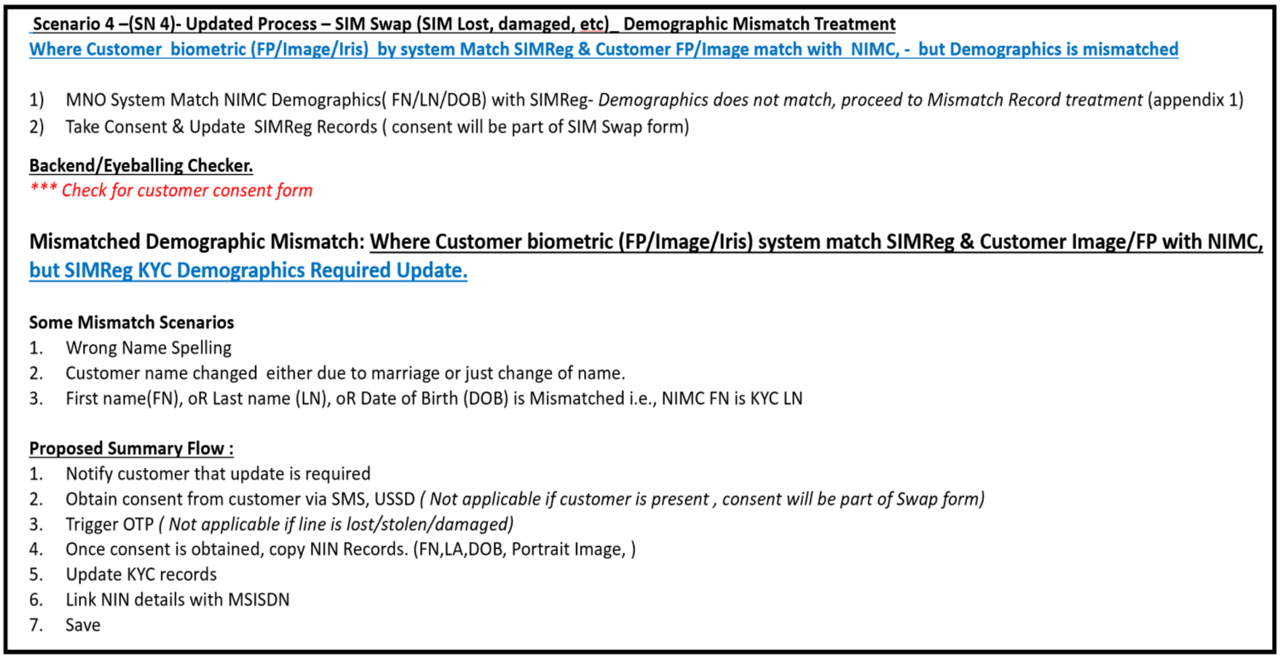
Scenario1- (SN1) : Lost SIM Replacement Where Customer biometric (FP/Image/Iris) system match SIMReg & Customer Image match SIMReg + NIMC	**Scenario2-(SN2) : Lost SIM Replacement** Where Customer biometric (FP/Image/Iris) system does not match SIMReg but Customer Image match with SIMReg + NIMC. Demographic Updates Required	**Scenario3 : SIM Upgrade**
1) Customer approach MNO 2) MNO Validate Customer FP against SIMReg DB , If Successful goto3 , If unsuccessful goto SCN2 3) MNO call NIMC for Basic NIN verification (no fingerprint verification) 4) NIMC confirm NIN and return demographic details (FN/LN/DOB) and image, if successfully returned, go to 5, if unsuccessful, Reject 5) MNO System Match NIMC Demographics(FN/LN/DOB) with SIMReg, if successfully returned, goto6, if unsuccessful, go to Scenario4 (mismatched demographic) 6) MNO take Customer Live image + Form and submit for backend validations 7) MNO validate NIN Image details with SIMReg + live image, if successful, goto8, if unsuccessful, Reject Swap. 8) Activate Swap. 9) Take Consent & Update SIMReg Records (consent will be part of SIM Swap form) **Electronic image matching to replace backend eyeballing when available to improve accuracy* *Note: MNOs are not allowed to retain verified biometric data of persons enrolled in the National Identity Database*	1) Customer approach MNO 2) MNO Validate Customer FP against SIMReg DB, FP match is unsuccessful goto3 3) MNO verify usage records of customer to validate SIM Ownership (FDN/LR/, Data bundle 4Data SIM etc.), If Successful goto4, if unsuccessful, Reject Swap. –(for Upgrade OTP will be used) 4) NIMC confirm NIN and return demographic details (FN/LN/DOB) and image, if successfully returned, go to 5, if unsuccessful, Reject Swap 5) MNO System Match NIMC Demographics(FN/LN/DOB) with SIMReg, if successfully returned, goto6, if unsuccessful, go to Scenario4 (mismatched demographic) 6) MNO take Customer Live image + Form and submit for backend validations 7) MNO validate NIN Image details with SIMReg + live image, if successful, goto8, if unsuccessful, Reject Swap. 8) Activate Swap. 9) Take Consent & Update SIMReg Records (consent will be part of SIM Swap form)	1. Customer to visit MNOs outlet 2. MNO sends OTP to customer 3. OTP is validated successfully 4. MNO validate the Customer MSISDN+FP against SIMReg Record 5. If 4 is successful, MNO validate MSISDN+NIN+FP against NIMC 6. If 5 is successful SIM upgrade will be administered 7. Update customer SIMReg record with FN,LN,DoB From NIMC if required + Link NIN 8. If 5 fails customer will be advised to visit NIMC to update or enroll as applicable ***9. SIM Swap rules will apply if Biometric is different with SIMReg***


Scenario 1: Updated Process – SIM Swap (SIM Lost, damaged, etc.)
Backend/Eyeballing
Where Customer biometric (FP/Image/Iris) system match SIMReg & Customer Image with SIMReg + NIMC

Customer
Mobile Network Operator (MNO)
NIMC
START
Customer approach MNO
MNO validates Customer fingerprint against SIM Registration Database
Successful?
NO
Goto Scenario 2
YES
No fingerprint
MNO call NIMC for Basic NIN verification
NIMC confirm NIN and return demographic details (FN/LN/DOB) and image
Successfully returned?
NO
MNO Rejects
YES
MNO System Match NIMC Demographics (FN/LN/DOB) with SIM Reg.
Successfully returned?
NO
Goto Scenario 4
YES
MNO take Customer Live image + Form and submit for backend validations
MNO validate NIN Image details with SIMReg + live image,
Successful?
NO
Reject Swap.
YES
Activate Swap.
Take Consent & Update SIM Reg. Records (consent will be part of SIM Swap form)
END


Scenario 2: Updated Process – SIM Swap (SIM Lost, damaged, etc.)
Backend/Eyeballing
Where Customer biometric (FP/Image/Iris) system does not match SIMReg but Customer Image match with SIMReg + NIMC demographics updates required

Customer
Mobile Network Operator (MNO)
NIMC
START
Customer approach MNO
MNO validates Customer fingerprint against SIM Registration Database.
Fingerprint match Successful?
NO
MNO verify usage records of customer to validate SIM Ownership (FDN/LR/Data bundle 4Data SIM etc.)
Successful?
NO
Reject Swap
YES
NIMC confirm NIN and return demographic details (FN/LN/DOB) and image
Successfully returned?
NO
MNO Rejects
YES
MNO System Match NIMC Demographics (FN/LN/DOB) with SIM Reg.
Successfully returned?
NO
Goto Scenario 4
YES
MNO take Customer Live image + Form and submit for backend validations
MNO validate NIN Image details with SIMReg + live image,
Successful?
NO
Reject Swap
YES
Activate Swap
Take Consent & Update SIM Reg. Records (consent will be part of SIM Swap form)
END



Scenario 4 –(SN 4)- Updated Process – SIM Swap (SIM Lost, damaged, etc)_ Demographic Mismatch Treatment
Where Customer biometric (FP/Image/Iris) by system Match SIMReg & Customer FP/Image match with NIMC, - but Demographics is mismatched

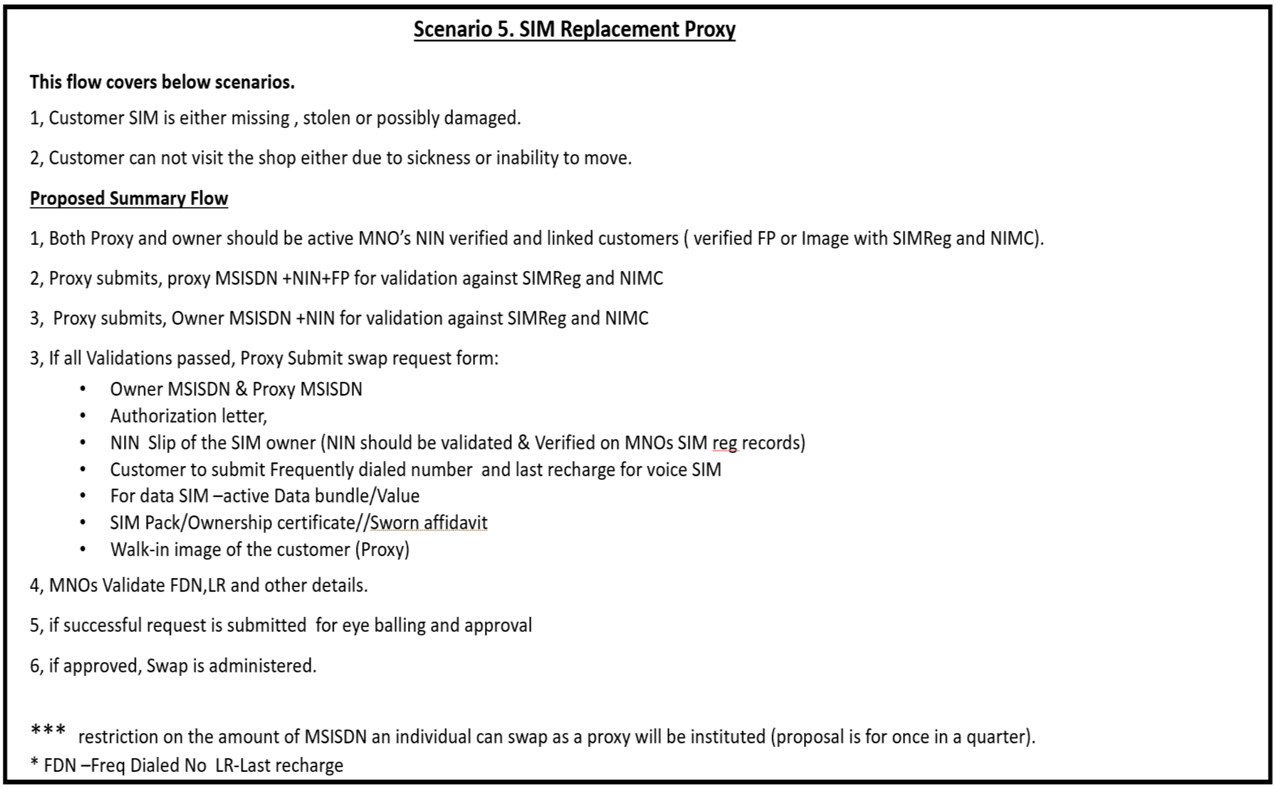
1) MNO System Match NIMC Demographics(FN/LN/DOB) with SIMReg- *Demographics does not match, proceed to Mismatch Record treatment* (appendix 1)
2) Take Consent & Update SIMReg Records (consent will be part of SIM Swap form)

Backend/Eyeballing Checker.
******* *Check for customer consent form*

Mismatched Demographic Mismatch: Where Customer biometric (FP/Image/Iris) system match SIMReg & Customer Image/FP with NIMC, but SIMReg KYC Demographics Required Update.

Some Mismatch Scenarios
1. Wrong Name Spelling
2. Customer name changed either due to marriage or just change of name.
3. First name(FN), oR Last name (LN), oR Date of Birth (DOB) is Mismatched i.e., NIMC FN is KYC LN

Proposed Summary Flow :
1. Notify customer that update is required
2. Obtain consent from customer via SMS, USSD *(Not applicable if customer is present , consent will be part of Swap form)*
3. Trigger OTP *(Not applicable if line is lost/stolen/damaged)*
4. Once consent is obtained, copy NIN Records. (FN,LA,DOB, Portrait Image,)
5. Update KYC records
6. Link NIN details with MSISDN
7. Save



Scenario 5. SIM Replacement Proxy

This flow covers below scenarios.

1, Customer SIM is either missing , stolen or possibly damaged.

2, Customer can not visit the shop either due to sickness or inability to move.

Proposed Summary Flow

1, Both Proxy and owner should be active MNO's NIN verified and linked customers (verified FP or Image with SIMReg and NIMC).

2, Proxy submits, proxy MSISDN +NIN+FP for validation against SIMReg and NIMC

3, Proxy submits, Owner MSISDN +NIN for validation against SIMReg and NIMC

3, If all Validations passed, Proxy Submit swap request form:

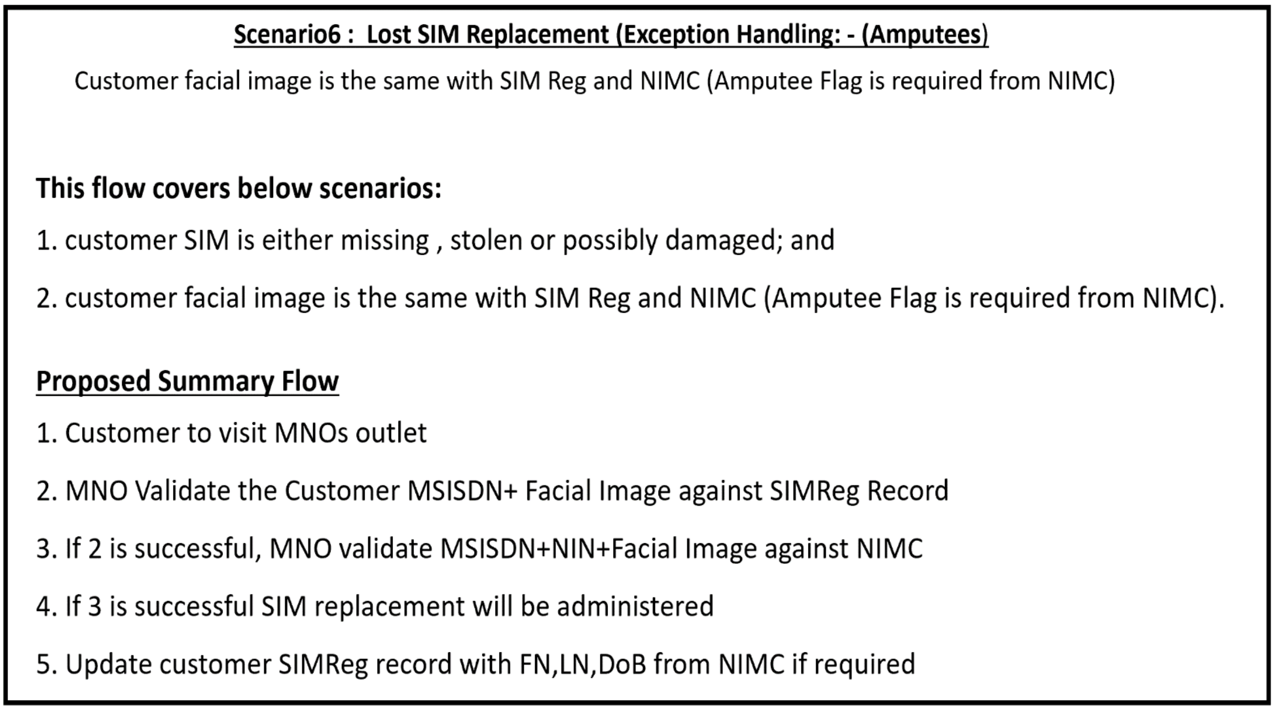
- Owner MSISDN & Proxy MSISDN
- Authorization letter,
- NIN Slip of the SIM owner (NIN should be validated & Verified on MNOs SIM reg records)
- Customer to submit Frequently dialed number and last recharge for voice SIM
- For data SIM –active Data bundle/Value
- SIM Pack/Ownership certificate//Sworn affidavit
- Walk-in image of the customer (Proxy)

4, MNOs Validate FDN,LR and other details.

5, if successful request is submitted for eye balling and approval

6, if approved, Swap is administered.

*** restriction on the amount of MSISDN an individual can swap as a proxy will be instituted (proposal is for once in a quarter).
* FDN –Freq Dialed No LR-Last recharge



Scenario6 : Lost SIM Replacement (Exception Handling: - (Amputees)

Customer facial image is the same with SIM Reg and NIMC (Amputee Flag is required from NIMC)

This flow covers below scenarios:

1. customer SIM is either missing , stolen or possibly damaged; and
2. customer facial image is the same with SIM Reg and NIMC (Amputee Flag is required from NIMC).

Proposed Summary Flow

1. Customer to visit MNOs outlet
2. MNO Validate the Customer MSISDN+ Facial Image against SIMReg Record
3. If 2 is successful, MNO validate MSISDN+NIN+Facial Image against NIMC
4. If 3 is successful SIM replacement will be administered
5. Update customer SIMReg record with FN,LN,DoB from NIMC if required

5.3 Guidelines for New SIM Acquisition/Activation (Corporate & IOT/M2M)

A) Guidelines for New SIM Acquisition/Activation (Corporate & IOT/M2M)

The guidelines for the SIM acquisition/activation (Corporate& IOT/M2M) are as follows:

i. use of NIN is Mandatory for SIM Sales/Acquisition;

ii. NIMC/NIN is the Reference/Foundational DB;

iii. MNOs seek to harmonize SIM Reg. KYC with NIMC/NIN details (demographics and biometrics);

iv. new SIM Acquisition /Sales grouped into 5 Scenarios:

a. new Customers with NIN requesting New SIM

b. existing Customers with NIN requesting additional SIMs

c. MNP customers with NIN requesting Mobile number porting

d. customers (new & existing) requesting New SIM or Porting without NIN

e. recycling of MSISDNs with NIN

v. service Availability SLA should be defined and agreed with NIMC;

vi. where NIMC availability SLA consistently falls below the defined and agreed SLA, Basic NIN Verification (verification without fingerprint) should be allowed for existing MNO Pry TMs requesting i.e. SIM Swaps or additional SIMs; because their NIN is verified (basic verification, no FP) & NIN detail returned will be matched against SIMReg DB, Swaps or additional SIM sales will be rejected if matching fails;

vii. all MNO Pry TM SIM Reg KYC verified demographics and biometrics shall be transmitted to NCC SIM Registration DB;

viii. all validated Secondary NIN and demographics (Names) of associated lines to a Corporate account will be transmitted to NCC central DB for storage (n/a to IOT/M2M);

ix. facial Image verification should be included as biometric verification for Pry TMs only;

x. for diplomats, the Head of Mission will serve as the Telecom Master and will not require NIN for registration of the official lines; and

xi. That the MNOs are not allowed to retain verified biometric data of persons enrolled in the National Identity Database.

B) Guidelines for New SIM Acquisition/Activation (Corporate)
The NIN rules for Corporate Activations are as follows:

1. corporate/Bulk registrations would involve and utilize both a Primary NIN and Secondary NIN (individual NIN per line user) The Corporate nominates a member of staff as its representative to serve as a Telecoms Master (minimum Executive Management level) and to provide the operational Primary NIN representation;

2. the Corporate generates an authorization letter for this nomination with the following:
i. on official letterhead
ii. stamped with company stamp
iii. signed off by 2 company representatives either; C-Level Director, CEO or Board Member. The NIN of one of the Directors is to be provided.

3. telecoms Master performs Primary NIN linkage using his/her NIN through the Primary number of the account either through online or USSD portal;

4. telecoms Master would upload the authorization letter as a part of the NIN linkage process;

5. the NIN data for the Primary number is linked to all other numbers within same account;

6. telecoms Master is also required to ensure the individual user provides his / her individual NIN to serve as Secondary NIN on the line, before the line is activated;

7. the corporate entity is required to present certified true copy of Certificate of Incorporation/CAC registration duly verified by the Corporate Affairs Commission and Tax Clearance Certificate/Tax Identification Number (TIN). Companies listed on the Nigerian Stock Exchange are exempt from this rule.; and

8. public/Government Organizations are to present a legal instrument showing evidence of establishment and must comply with items a-g above.

C) Guidelines for New SIM (IOT/M2M) Activations

The guidelines for new SIM(IOT/M2M) activations are as follows:

a. the Corporate nominates a member of staff as its representative to serves as a Telecoms Master (minimum Executive Management level) and to provide operational Primary NIN representation.

b. the Corporate generates an authorization letter for this nomination with the following:

i. on official letterhead;
ii. stamped with company stamp; and
iii. signed off by 2 company representatives either; C-Level Director, CEO or Board Member. The NIN of one of the Directors is to be provided.

c. telecoms Master performs Primary NIN linkage using his/her NIN and the Primary number of the account either through online or USSD portal;

d. the Telecoms Master would upload the authorization letter as a part of the NIN linkage process;

e. NIN data for the Primary number is linked to all other numbers within same account;

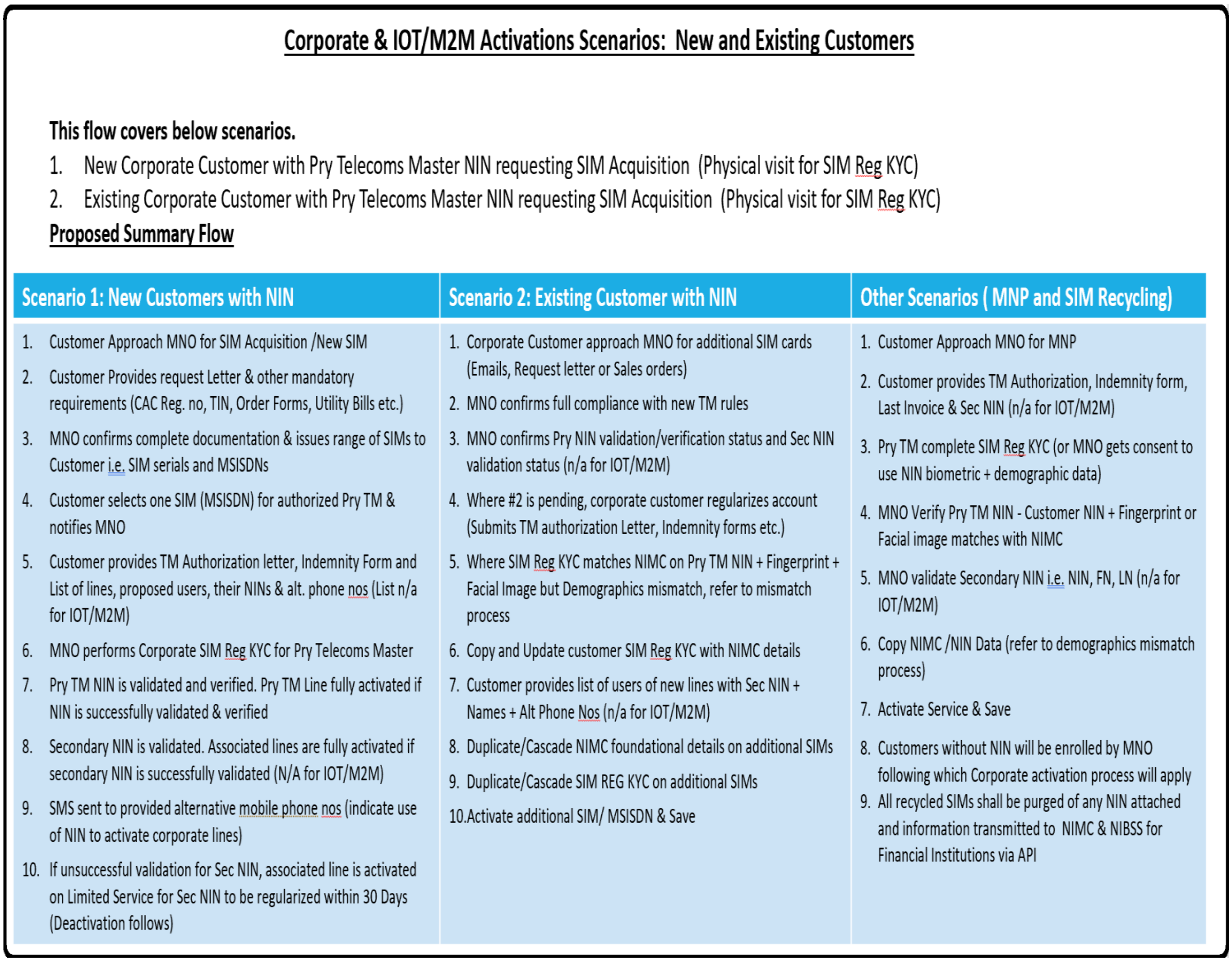
f. SIM Security Protocols would be implemented on the SIM profile to ensure that the SIMs can only be used for point to point Data services – specific to the URL they are working with. All other services will be barred;

g. this process only refers to Bulk Machine to Machine SIM Solutions (data only) in corporate facilities;

h. where a data only service is particular to individual use e.g. Home car tracking, WIFI, MIFI services, et al, the standard NIN registration process will apply;

i. the corporate entity is required to present Certificate of Incorporation/ CAC registration duly verified by the Corporate Affairs Commission and Tax Clearance Certificate/Tax Identification Number (TIN). Companies listed on the stock exchange are exempt from this rule; and

j. Public/Government Organizations are to present a legal instrument showing evidence of establishment Corporate & IOT/M2M Activations Scenarios: New and Existing Customers.



Corporate & IOT/M2M Activations Scenarios: New and Existing Customers

This flow covers below scenarios.

1. New Corporate Customer with Pry Telecoms Master NIN requesting SIM Acquisition (Physical visit for SIM Reg KYC)
2. Existing Corporate Customer with Pry Telecoms Master NIN requesting SIM Acquisition (Physical visit for SIM Reg KYC)

Proposed Summary Flow

Scenario 1: New Customers with NIN	Scenario 2: Existing Customer with NIN	Other Scenarios (MNP and SIM Recycling)
1. Customer Approach MNO for SIM Acquisition /New SIM 2. Customer Provides request Letter & other mandatory requirements (CAC Reg. no, TIN, Order Forms, Utility Bills etc.) 3. MNO confirms complete documentation & issues range of SIMs to Customer i.e. SIM serials and MSISDNs 4. Customer selects one SIM (MSISDN) for authorized Pry TM & notifies MNO 5. Customer provides TM Authorization letter, Indemnity Form and List of lines, proposed users, their NINs & alt. phone nos (List n/a for IOT/M2M) 6. MNO performs Corporate SIM Reg KYC for Pry Telecoms Master 7. Pry TM NIN is validated and verified. Pry TM Line fully activated if NIN is successfully validated & verified 8. Secondary NIN is validated. Associated lines are fully activated if secondary NIN is successfully validated (N/A for IOT/M2M) 9. SMS sent to provided alternative mobile phone nos (indicate use of NIN to activate corporate lines) 10. If unsuccessful validation for Sec NIN, associated line is activated on Limited Service for Sec NIN to be regularized within 30 Days (Deactivation follows)	1. Corporate Customer approach MNO for additional SIM cards (Emails, Request letter or Sales orders) 2. MNO confirms full compliance with new TM rules 3. MNO confirms Pry NIN validation/verification status and Sec NIN validation status (n/a for IOT/M2M) 4. Where #2 is pending, corporate customer regularizes account (Submits TM authorization Letter, Indemnity forms etc.) 5. Where SIM Reg KYC matches NIMC on Pry TM NIN + Fingerprint + Facial Image but Demographics mismatch, refer to mismatch process 6. Copy and Update customer SIM Reg KYC with NIMC details 7. Customer provides list of users of new lines with Sec NIN + Names + Alt Phone Nos (n/a for IOT/M2M) 8. Duplicate/Cascade NIMC foundational details on additional SIMs 9. Duplicate/Cascade SIM REG KYC on additional SIMs 10.Activate additional SIM/ MSISDN & Save	1. Customer Approach MNO for MNP 2. Customer provides TM Authorization, Indemnity form, Last Invoice & Sec NIN (n/a for IOT/M2M) 3. Pry TM complete SIM Reg KYC (or MNO gets consent to use NIN biometric + demographic data) 4. MNO Verify Pry TM NIN - Customer NIN + Fingerprint or Facial image matches with NIMC 5. MNO validate Secondary NIN i.e. NIN, FN, LN (n/a for IOT/M2M) 6. Copy NIMC /NIN Data (refer to demographics mismatch process) 7. Activate Service & Save 8. Customers without NIN will be enrolled by MNO following which Corporate activation process will apply 9. All recycled SIMs shall be purged of any NIN attached and information transmitted to NIMC & NIBSS for Financial Institutions via API

5.4 Guidelines for Foreigner Activations

International passport capture requirement has been the prerequisite for the activation of phone lines for customers. However, with the introduction of mandatory use of NIN for telecommunications services, the process for foreigners (new/existing) needs to be reviewed.

The new process is as follows:

1. foreigners who are lawfully residing in Nigeria for a period of two years or more fall under the category of Registrable persons and will require a NIN to register their SIM;

2. foreigners validly transiting through Nigeria or are employed in or reside in Nigeria for less than 24 months are exempted from the mandatory use of NIN requirement. Persons in this category need to provide justification that they will be residing in Nigeria for less than 2 years;

3. NIN is mandatory for foreigners with Legal Residency status or those living in Nigeria for 2 years and above. For those who do not already have a NIN, operators will capture the Resident for NIN as part of the enrollment process, upon presentation of residents permit;

4. foreigners with Visitor's visas (with visa less than 2 years) do not require a NIN. Operators will capture the following on their records;
   - International passport bio-data page; and
   - Visa page.

5. foreigners with Diplomatic visas (including family diplomatic visas) will also require a NIN for their personal telephone lines if they are staying in Nigeria for 2 or more years. Those staying less than 2 years will require the following for registration of their personal telephone lines:
   - International passport bio-data page; and
   - Letter from embassy indicating that their stay is for less than 2 years.

6. for Embassies and Diplomatic Missions:

i. the data page containing the Passport Number of the Diplomatic passport of the Head of Mission/Embassy along with a Letter of Request signed by the Ambassador or its equivalent for registration of the official telephone lines of the Embassy / Mission in Nigeria shall be submitted to the Ministry of Foreign Affairs for verification and confirmation and registration of the SIMs.

ii. SIM cards of the diplomatic missions are to be linked with a Corporate Diplomatic Identification Number (CDIN), which will be unique to each

Diplomatic Mission. Each Mission will also be responsible for the managing the lines and allocating them internally. Furthermore, the Head of Mission is to serve as the Telecom Master or Point of Contact for the Mission.

iii. any Foreign member of a Diplomatic Mission requiring SIMs for personal use shall go through the processes under item '4' above.

5.5 Guidelines for Engagement/Accreditation of Dealers and Agents

The following are the guidelines for the accreditation of dealers/agents by MNOs to ensure a more secure SIM activation process and reduce incidence of fraudulently registered SIMs:

1. all Dealers engaged by Network Operators for NIN enrolment are to be accredited and their details forwarded to the Commission;

2. details of all enrolment devices and SIMs assigned to each Dealer are to be forwarded to the Commission;

3. the Commission will liaise with security agents to undertake security checks on all dealers and agents. Any agent/dealer with adverse security report will not be engaged and blacklisted as the case may be;

4. MNO's are to accredit Enrolment Agents engaged by their Dealers and forward details of all engaged Agents to the Commission;

5. enrolment Agents must possess a NIN and BVN, details of which are to be forwarded to the Commission;

6. enrolment Agents must have minimum educational qualification of Secondary School Certificate (SSCE/WAEC);

7. MNO's shall not make cash payments to Enrolment Agents as commission or incentive. All payments are to be made through Agent's bank accounts;

8. MNOs should be able to identify the dealers/agents responsible for fraudulently registered SIM cards;

9. MNOs to provide details of Dealers/Agents that registered SIM cards that have been identified as fraudulently registered;

10. MNOs to have a mechanism for flagging off suspected infractions in SIM registration and the SIMs involved in such infractions should be deactivated or blocked from the network;

11. any Dealer/Agent blacklisted by a network for fraudulent SIM registration or SIM swap transactions will be barred from all networks;

12. the Commission will liaise with security agencies like EFCC an ONSA to block the accounts of any agent involved in fraudulently registered SIMs and NIN to serve as deterrent to others;

13. the Commission will liaise with security agents to prosecute dealers/ agents involved in fraudulently registered SIMs and NIN; and

14. any operator that contravenes these guidelines will be sanctioned with relevant sanctions as stipulated by the Commission.

CONCLUSION

A secured digital identity is necessary for the success of any digital economy. However, any digital identity must be robust enough to digitally identify individuals in cyberspace and other online platforms. As the National Identification Number (NIN) provides a legal national digital identity, he SIM card registration information must be validated against the NIN. Verifying SIM card registration on the national citizen identity database hosted and managed by NIMC will provide the required assurance and robustness for a national digital identity capable of promoting and driving more participation in the digital economy for all citizens. The national digital identity policy for SIM card registration is a step in that direction. It will leverage the strength of both databases – NIMC and NCC/mobile network operators, to offer a strong, versatile and robust digital identity, which will promote secured digital inclusion for all Nigerians.

APPENDIX

Key Stakeholders

The following are key stakeholders that will ensure the successful implementation of the policy:

1. Federal Ministry of Communications and Digital Economy
2. Nigerian Communications Commission
3. Ministry of Defense
4. Ministry of Police Affairs
5. Ministry of Interior
6. National Information Technology Development Agency
7. Independent Corrupt Practices and Other Related Offences Commission
8. Office of National Security adviser
9. National Identity Management Commission
10. Nigeria Police Force
11. Defence Headquarters
12. National Intelligence Agency
13. Defence Intelligence Agency
14. Nigeria Security and Civil Defence Corps
15. Department of State Services
16. Central Bank of Nigeria
17. The National Assembly (Leadership and Relevant Committees)
18. Association of Licensed Telecom Operators of Nigeria (ALTON)
19. Association of Telecommunications Companies of Nigeria (ATCON)