Mandatory registration of prepaid SIM cards

Addressing challenges through best practice

April 2016

The GSMA represents the interests of mobile operators worldwide, uniting nearly 800 operators with more than 250 companies in the broader mobile ecosystem, including handset and device makers, software companies, equipment providers and Internet companies, as well as organisations in adjacent industry sectors. The GSMA also produces industry-leading events such as Mobile World Congress, Mobile World Congress Shanghai and the Mobile 360 Series conferences.

For more information, please visit the GSMA corporate website at **www.gsma.com**

Follow the GSMA on Twitter: **@GSMA**

For more information or questions on this report, please email **publicpolicy@gsma.com**

CONTENTS

Executive summary

Pre-paid SIM card registration is mandated in a number of countries and requires consumers to provide proof of identification in order to activate and use a mobile SIM card. A number of governments adopt this policy as part of efforts to help mitigate security concerns and to address criminal and anti-social behaviour. To date, there has been no empirical evidence that mandatory SIM registration directly leads to a reduction in crime. However, where the exercise is implemented effectively by taking into account local market circumstances, for example the ability of mobile operators to verify customers' identity documents, SIM registration can enable many consumers to access value added mobile and digital services that would otherwise be unavailable to them as unregistered users. However, if the registration requirements are disproportionate to the specific market, the mandatory policy may unintentionally exclude vulnerable and socially disadvantaged consumers.

Where governments are considering the introduction or revision of a mandatory SIM registration policy, the proposed solution should balance the cost of implementation (including the cost to consumers and any potential limitation on the size of the pre-paid SIM market) and privacy concerns relating to the use of consumers' registration information by government and mobile operators. Alternatives to mandatory SIM registration should also be considered as part of any impact assessment.

With the increasing importance of citizens having a secure digital identity and where there are issues with the availability of official identity documents, there may be a role for operators to support the government in the creation of a unique identity that can be authenticated and used for a variety of mobile and non-mobile services. This will, in part, help individuals who lack formal identity documents to access communication services but also potentially e-Government and other value added services.

This paper reviews recent requirements for mandatory SIM registration in various markets, reflects on best practice, highlights potential issues and suggests the following recommendations for policymakers when considering the introduction, or revision, of a mandatory SIM registration policy:

1. Consult, collaborate and communicate with mobile operators before, during and after the implementation exercise, while balancing national security demands against the protection of citizens' rights;

2. Set realistic timescales for designing, testing and implementing registration processes;

3. Provide certainty and clarity on registration requirements before any implementation;

4. Allow / encourage the storage of electronic records and design administratively 'light' registration processes;

5. Allow / encourage the registered ID to be used for other value added mobile and digital services;

6. Support mobile operators in the implementation of SIM registration programmes by contributing to joint communication activities and to their operational costs.

Introduction

In 2013 the GSMA published a white paper[1] addressing the opportunities and consequences of mandating registration for pre-paid SIM card users. Since 2013 there have been a number of developments with implications for SIM registration; there has been a rapid development of mobile services requiring validated identity, on-going national security concerns, new developments in national identity schemes and the continued growth of mobile penetration to serve increasingly vulnerable and socially disadvantaged members of society. All of these developments have implications for policymakers considering mandating SIM registration.

The specific concerns each government is looking to address through mandatory SIM registration initiatives do vary by country. Most Governments introduce mandatory SIM registration to address concerns over national security and criminal behaviour. In these countries security services see SIM registration as a tool in their fight against terrorism and organised crime. However this approach is not universal; there are also a number of countries that have no mandatory registration, choosing to address security concerns without requiring all customers to prove their identity to register for a mobile phone service. In some markets, mainly in Latin America, consumers are required to register their mobile handset's (IMEI) number, which may not always be registered against the specific consumer's mobile phone number (SIM). The regulatory focus in these markets is on addressing handset theft rather than the use of the phone for criminal activity by a named individual. In other markets, SIM registration has also been seen as a way to address antisocial behaviour, to reduce SPAM, to provide age verification and to help address mobile fraud. The requirements imposed on operators and the processes and solutions implemented in countries choosing to adopt mandatory SIM registration reflect these different priorities.

The effectiveness of SIM registration solutions also depends on the availability and pervasiveness of national identity schemes. These vary dramatically across countries – from countries that have all citizens registered on a verifiable biometric database, to those where large sections of society have no ID documentation at all. SIM registration solutions are not a substitute for national identity registers[2]. Where a comprehensive, verifiable and pervasive national identity scheme is not available, governments should not place excessive burdens on operators that may ultimately have a detrimental impact on citizens and their ability to access mobile communications. Mandated requirements for SIM registration need to be pragmatic, reflect the practical challenges faced by consumers wanting to access services and the ability for operator and channel partners to verify a person's identity.

Whilst addressing security and criminal activity concerns is important, policymakers and regulators should ensure there are also appropriate privacy safeguards and effective legal oversight to protect consumers' personal data and privacy. This is critical for building consumer confidence in any registration scheme. There are also economic and social considerations; if registration requirements are too stringent and do not reflect the national circumstances there is a real risk of excluding large sections of the community, often the most vulnerable or geographically the most remote. Whilst the direct impact to operator revenues can affect investment and the corresponding reduction in tax revenues is not ideal for governments, the impact on individual citizens can be very significant. It is important to consult with all stakeholders and to undertake a full impact assessment before mandating SIM registration or changing existing registration requirements to ensure there is an effective balance between different stakeholder needs.

1 http://www.gsma.com/publicpolicy/wp-content/uploads/2013/11/GSMA_White-Paper_Mandatory-Registration-of-Prepaid-SIM-Users_32pgWEBv3.pdf
2 See World Bank Report, Jan 2016 – Identification for Development Strategy Framework for a definition of different identity systems

Mobile as a contributor to society

Mobile delivers significant economic and social benefits. There are now 4.7 billion unique subscribers globally[3], of which 44% use mobile to connect to the Internet. By 2020 the GSMA forecast 5.6 billion people will have a mobile phone with over 60% of these people using the phone to access Internet services. In 2015, the mobile ecosystem generated 4.2% of global GDP and has had a significant impact on employment both directly, employing 17 million people globally, and indirectly supporting another 15 million jobs in other sectors. There is a direct effect on government revenues too, the industry pays $430 billion in general taxation and in 2015 paid $90 billion in spectrum licence fees.

As well as the economic benefits the industry brings to countries through investment and employment mobile also plays a key role in enabling digital inclusion and delivering social benefits. In the developing world, the number of people accessing the Internet over mobile devices had grown to nearly 2.5 billion by the end of 2015 with a further 1.3 billion people in developing markets are expected to access the mobile Internet by 2020. Mobile is also a key contributor to the financial inclusion agenda with Mobile Money services now available to 1.9 billion people in more than 90 countries.

However, there remains a significant challenge to bridge the digital divide. By 2020 it is anticipated that 40% of people in developing markets will still not have access to the mobile Internet (or any other internet service). Lack of Internet access would especially affect rural communities and the most socially disadvantaged, excluding them from the economic and social benefits being realised by other sections of society.

Mandatory SIM registration does have an effect on this socially disadvantaged community in many markets. The World Bank estimates[4] that 1.5 billion people across the world – the majority in Africa and Asia in – lack any form of official identity; registration systems with a mandatory requirement to provide proof of identity either exclude these people or make them dependent on others to gain access to mobile services. There are other challenges for many of these communities; these can be logistical, for example having to travel to the nearest town to register at a specific authorised location, or financial, where securing official papers is a prerequisite of getting a mobile phone and there is a charge for these papers. In these circumstances the 'barrier' to mobile access and digital inclusion becomes disproportionately high for this section of the community.

When considering changes to registration requirements or the introduction of mandatory SIM registration, governments need to consider their specific national circumstances, especially in relation to the availability of formal identity documents and the ability of operators and their channel partners to verify these documents. Setting the barriers too high will result in vulnerable and disadvantaged sections of society being excluded and, in the case of changed requirements, potentially disconnected.

3 Unless otherwise indicated all figures are from the GSMA 2016 Mobile Economy Report
4 World Bank. Identity for Development (ID4D) Strategic Framework. January 2016

The increasing importance of mobile and digital identity

Having a secure and authorised digital identity will become increasingly important. In most countries mobile is a good platform to deliver this, because of its ubiquity and security capabilities. Leveraging the mobile platform could also significantly help in meeting the United Nations Sustainable Development Goal target 16.9: "free and universal legal identity, including birth registration by 2030".

However, mandatory SIM or phone registration policies should not be seen as substitutes for national identity schemes. The purpose of the registration policy is predominantly to enable the identification of someone using a mobile service by verifying existing identity documentation from legal and functional government registers. Operators and their channel partners can only check the identity of the person registering and where required, capture specific information on the customer.

Once an individual registers their SIM card, they could use their mobile phone to log-in and access other value added services.[5] As the World Bank observe in their ID4 Development strategy[6], the pervasiveness of mobile technology provides promising solutions to enroll and authenticate individuals with a unique identification in remote and rural areas. Because the identity of the person has been verified through a 'know your customer' process (KYC) and the mobile device/SIM can be attributed to the individual it is possible to use this information for digital authentication to access a wide variety of different services in the knowledge that the person is who they say they are. This minimises the risk of fraud and improves the efficiency of the transactions, for example facilitating welfare payments directly into a mobile banking account. The mobile can provide multi-factor authentication to access the services with the secure mobile device being used as part of the authentication process.

The World Bank estimates that 1.5 billion people[7] do not have access to formal identity documentation. Mobile solutions are already being used to facilitate birth registration[8] and help address the significant problems associated with children not having a legal identity. Longer term, such solutions may help to partly address the lack of legal identity documents in the adult population. Addressing the challenge of creating an official identity for the adult population is more challenging. Whilst mobile registration databases should not substitute a national identity registry they may provide an effective functional registry that could be used for authorising consumers' access to other services. This will depend on the operator's ability to (a) ensure that the record created is unique and (b) provide verification and authorisation services to third parties. Where there are issues with the availability of official identity documents there may be a role for operators to support the government in the creation of a unique identity that can be authenticated and used for a variety of mobile and non-mobile services. This will in part help individuals who lack formal identity documents to access communication services but also potentially e-Government and other value added services.

5 http://www.gsma.com/mobilefordevelopment/programmes/digital-identity/
6 World Bank. ID4D Strategic Framework January 2016
7 World Bank. Identity for Development (ID4D) Strategic Framework. January 2016
8 http://www.gsma.com/personaldata/wp-content/uploads/2013/05/Mobile-Birth-Registration-in-Sub-Saharan-Africa.pdf

The use of mobile registration data to create an identity registry that can be used to access third party services (at the request of the relevant consumer) does need to be very carefully considered. The exact requirements, including whether a biometric and photograph are required and what supporting evidence of identity is needed needs to be defined. Finally, there is a need to consider the implications of possibly sharing any data from the identity registry with third party service providers and/or how authentication is implemented when consumers access third party services.

Mandatory SIM registration solutions

Where SIM registration is mandated, the requirement is for the operator to capture the identity details of the person responsible for the mobile and to make the details of this person available to the relevant authorities upon request. The specific requirements vary by country. Where national identity registries are available (e.g. Pakistan, Rwanda, the UAE etc.) they can be checked to authenticate the mobile registration data. Where governments do not have this facility the authentication is usually done by visual checks of a user's identity documents.

There is not necessarily a one to one relationship between a mobile and an individual. Many users will have multiple devices, for example: a phone, a PC dongle and a tablet may involve three different SIMs but all registered to the same individual. In many markets it is not uncommon for individuals to have different SIMs with different networks to take advantages of any differences in network coverage or different marketing offers. It is also not uncommon in many markets for the 'head of the household' to buy the mobile devices and activate the SIMs for family members. Duplication of SIM registration information is therefore not uncommon on operator databases, unlike national registers where there is a unique record for each individual.

The ability of an operator to use the registration data to offer their customers personalised services varies by market. In some markets there are strict prohibitions on the use of the data by operators for additional services on offer beyond mobile connectivity, unless the customer's consent is obtained. In other markets the registration data can be used as a proof of identity for other specific value added services (e.g. mobile financial services in Pakistan). This is especially the case where the ability to verify the data exists. Generally, verification gives a higher level of assurance and can help operators comply with Know Your Customer (KYC) requirements and enable their customers to access financial and government services.

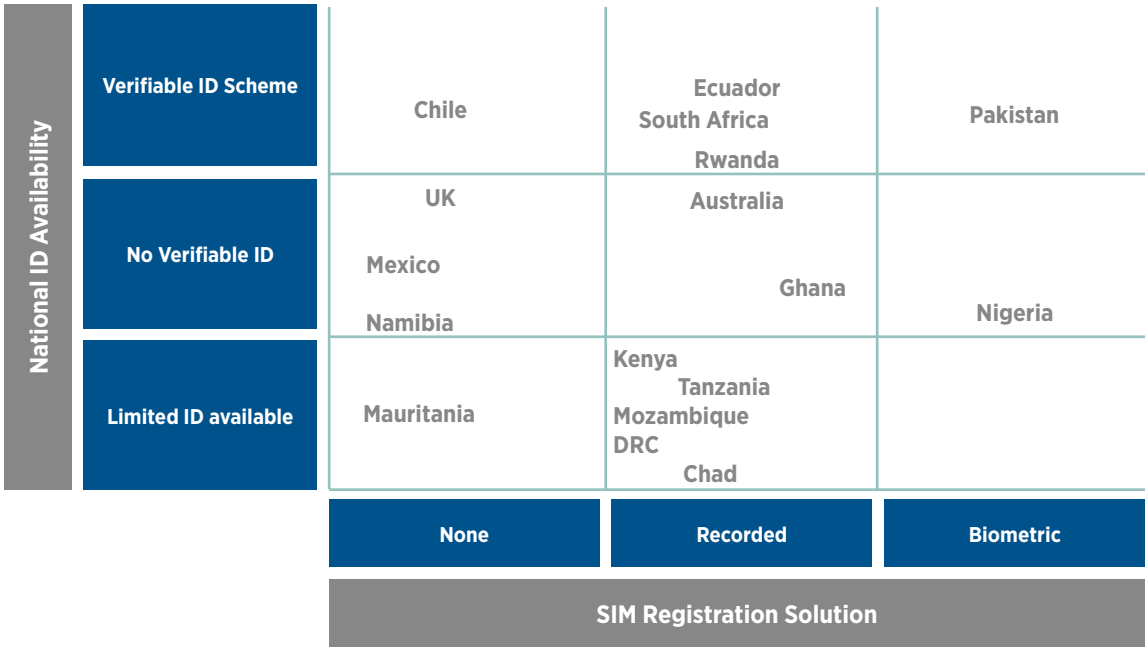
DIFFERENT APPROACHES TO MOBILE / SIM REGISTRATION

The availability of national identity documents and whether the identity documentation being used can be validated against a government registry, either at point of sale or at point of activation, has a significant bearing on the registration solution. Verification and authentication are critical elements in limiting identity fraud. Without these, as the Australian law enforcement agencies noted[9], identity checks can be relatively easily circumvented due to the difficulties validating identity documents in a retail environment. Verification does however require that there is an identity register that can be interrogated and that privacy concerns can be managed where these registers are interrogated as part of the validation process. Where a national registry is not available it is usual that various different identity documents can be used to verify a person.

9 Australian Government, Department of Broadband, Communications and the Digital Economy. Proposed Changes to Identity Verification Requirements for Prepaid Mobile Services. Feb 2013.

Figure 1

Different National approaches to SIM registration



A number of markets do not mandate mobile registration; in many cases this is a conscious decision reflecting that either the cost of the solution does not justify any potential benefit or that the security concerns (which mobile registration may be targeted to address) can be tackled more effectively in other ways. Increasingly, there are markets where biometric data are required as part of the registration process. These can be fingerprint data, iris scans, photographs or a combination of these and generally involve high up front costs for purchasing biometric readers, back-end infrastructure and training for those registering SIM card users. Biometric solutions can be stand alone, as is the case in Nigeria, or integrated and validated against a National ID database, as in Pakistan where there is integration with NADRA.[10] For the majority of markets however, the requirement is to use one of a variety of 'authorised' existing personal IDs as evidence of a person's identity to register a SIM.

Mandatory mobile registration solutions are not implemented in 'green field' environments so it is not possible to pick an ideal world solution – each solution is market-specific. It is however insightful to understand the advantages and disadvantages of the alternative solutions implemented to maximise the effectiveness of the chosen mandatory registration solution.

VERIFIED REGISTRATION SOLUTIONS

Where there is a national identity register and it is possible for mobile operators to check a person's details against this register, a verification check can be added to the registration process. The check confirms that the identity number and the personal details given by the mobile user at the point of registration correspond to the details on the national identity register.

Real-time verification against a national identity register provides the most comprehensive mandatory mobile registration solution. This gives the government and the operator a high degree of confidence that the details presented by the mobile user during registration are correct and the person is who they say they are. The pre-requisite for this is that there is a comprehensive national register available, which includes records for all citizens.

The customer verification can be against the national identity number and specific verifiable data relating to the individual. In some cases biometric verification is required. Using biometric data to verify the identity of an individual is only appropriate where the national identity registry already stores this information and where all points where a customer can register for a

10 NADRA is the National Database and Registration Authority in Pakistan, responsible for issuing biometric identity cards and maintaining the national identity register.

phone (or update their registration) are equipped with the capability to capture and check biometric data. For verification purposes there is no need to collect biometric data if it is not used to help as proof of identity. In non-verified solutions the biometric data may be an important part of the creation of a unique identity, this 'use case' will be covered below.

VERIFIED SOLUTIONS	
ADVANTAGES	**DISADVANTAGES**
• Verification 'assures' the identity of the registered user • Identity can be used for KYC on other services (if regulations allow this) • Least likely to suffer from identity fraud or compliance abuse • Reduces the risk to operators of unintentional compliance failures • Only 'authentication' data needs to be stored and not identity data reducing the risk of privacy and identity fraud issues	• Requires a National ID register to verify against • Requires technical integration between the operators' retail locations • Dependent on electronic registration forms and 'networked' capability in all retail locations • Expensive to implement, especially where there is a biometric requirement • Verification adds to the lead time for delivery (as it requires technical development) • Biometric verification is complicated and does not have 100% matching

The main advantage of having a solution with verification is that it is the most effective solution and is least likely to suffer from issues of identity fraud. There are secondary benefits, because a person's identity has been verified with a high degree of assurance[11], there is a high degree of confidence that a person is who they claim to be. This allows for the mobile registration to be used as a form of digital identity to authenticate mobile users when accessing other government and value added services. For customers, this saves them having to go through a registration process for each individual service. It also adds value to the registration process for operators by enabling them to use verified registration information in multiple services and for service providers it gives them confidence that the person is who they say they are, that there is some protection against fraud and they are not required to implement their own KYC process.

The main challenges are the implementation cost and the technical challenge of integrating the solution and enabling all of the retail locations and channel partners with the capability to register new users, or validate existing ones. There also needs to be consideration of how foreign nationals can register, how businesses can provide employees with pre-paid services and how other 'exceptions' can be handled during the registration process.

11 Examples of existing standards for security assurance level for digital identity and authentication include: ISO/IEC DIS; UK Cabinet Office; European Commission, etc.

PAKISTAN CASE STUDY

BACKGROUND

SIM registration requirements were introduced into Pakistan in 2008; the initial paper based solution was seen as unreliable and ineffective. In October 2013 the government proposed the use of biometric registration linked to the National Database and Registration Authority (NADRA) national identity register. In mid 2014 the government in Pakistan introduced the requirement for biometric identity validation for all newly provisioned SIMs. Following a terrorist incident in December 2014 this requirement was extended to all provisioned SIM cards, requiring re-registration of most of the 135 million provisioned SIMs. An accelerated implementation was agreed with 108 million SIMs registered across the five operators in Pakistan by the three-month deadline, 27 million SIMs were disconnected.

SOLUTION

- All customers are required to provide a biometric (fingerprint) along with their national ID reference and other details. The biometric and ID data is verified 'real time' at the operator retail location against the NADRA database.
- The verified identity is stored on the operator systems with the approval notification from NADRA. This approved identity is valid for the provision of other value added services including financial services and e-government services.
- The Pakistan Supreme Court ruled there should be a maximum of 5 SIMs per person. There are provisions for corporate SIMs.

LESSONS LEARNT

There were a number of different factors that enabled this impressive logistical exercise to be completed:

1. An existing electronic government ID registration scheme (NADRA) was already in place with the technology (including the biometric technology) and the integration into the operators' systems already proven. This was an enhancement on an earlier paper based system that had proven to be unreliable and ineffective.
2. In parallel to the SIM registration exercise there was a NADRA e-registration programme (including storing citizens' thumbprint electronically) to ensure there was an accurate government ID registration record to verify the SIM registration against. Citizens were made aware that without the e-registration on NADRA their existing paper ID would be invalidated.
3. The government led a huge nationwide communication campaign on TV and Radio to raise awareness of the need to re-register SIM cards which was supported by the operators' own initiatives. The message was very clear, 'if you do not re-register you will be disconnected'.
4. During the initial implementation and re-registration exercise there was no charge to the operator (or the customer) for the re-registration against the NADRA database. (NADRA usually charge operators a fee per verification).

PAKISTAN CASE STUDY CONTINUED

Whilst overall the programme was successful, there were areas where improvements could have been made:

1. Because of compressed timescales for implementation the cost of the biometric equipment and supporting devices was disproportionately high.

2. The implementation meant that all other activities and investments by the operators were put on hold, delaying any potential benefits to the economy and society that these could have realised.

3. 27 million SIMs were not re-registered. It is likely a large number of these SIMs belong to customers who re-registered an alternative SIM. A number may however belong to socially disadvantaged and potentially vulnerable people. Given the aggressive implementation timescales it is this cohort of citizens most likely to be disadvantaged and disconnected.

BENEFITS

Following the re-registration exercise there have also been a number of benefits:

1. The clean data, using verified registration information, has allowed operators to offer customers value added services.

2. There was an agreement between the Financial Regulator and the Telecoms Regulator that the KYC for a mobile wallet would be satisfied through this new SIM verification. This has had a very positive impact to the financial inclusion agenda.

3. Operators have a better record of customers, which helps them to effectively manage their customer relationships and offer appropriate products and services.

The Pakistan case is a good example of biometric verification against a national identity register. With Bangladesh, Indonesia, Saudi Arabia and the United Arab Emirates introducing requirements for biometric registration there is an emerging trend towards using biometric solutions with verification linked to National ID schemes. There are however many examples where the verification does not require biometrics; Ecuador have a comprehensive national identity scheme (the national ID number is used for passports, driver's licenses and the identity card) with registration of a mobile phone verifying a person's identity against this registry. Rwanda also has a comprehensive national identity register and this is used to verify a person's identity when they register.

NON VERIFIED REGISTRATION SOLUTIONS

In the majority of cases a variety of different identity documents are used to provide a proof of identity during the registration process. Legal registers and identity documents include birth certificates, passports and national identity cards, providing individuals with a proof of identity. Functional registries support specific services and include driving licences, voter rolls, health records, student cards and can include private sector 'identity' registers. Which of these forms of ID are appropriate to validate identity for SIM registration will depend on the market. In some markets driver licenses have a photograph and a home address and may be an appropriate from of ID to use for the registration, in others there may be a requirement for a secondary form of ID to be presented, especially if there is not a photograph on the license.

The 'authorisation' of a person's identity during a registration process is usually dependent on the physical presence of the person, providing one (or more than one) acceptable form of ID and completing the registration form. Some markets allow for other verification methods. The GSMA 2013 white paper[12] highlighted the changes made to the Australian registration options to make it easier for consumers to register for pre-paid phones whilst also providing the security services with confidence that the registered user is legitimate.

The SIM registration process may also require a photograph to be taken or the collection of biometric data. Where there is no national registry database this data can't be verified but it can help to create a unique record and act as an 'identity' for the individual registering. For example, Nigeria's mandatory SIM registration solution does not validate the SIM registration data against a national database. The identity validation is a standard check against existing identity documents and the physical presence of the individual. There are known challenges with the data collected, for example there is no formal address system in Nigeria so validating address information is problematic. The Nigerian solution does however require a photograph and a biometric fingerprint as part of the registration. The combination of the biometric data and photograph, personal details captured during registration like date of birth, the mobile phone and identity papers documents give a good assurance that the registered person is a unique individual. As there is no validation that the identity provided for the registration is real (it is possible that fraudulent documents are used) professional criminals can create false registrations. The photograph and the biometric do however link an individual to the phone/SIM being registered.

NON VERIFIED REGISTRATION SOLUTIONS	
ADVANTAGES	**DISADVANTAGES**
• Typically leverage existing identity documents to support the registration process	• Lower assurance than a validated solution and harder to detect fraud
• Identity documents are generally more widely available	• Can require sensitive data to be stored as proof of ID (rather than an authorisation token)
• Not dependent on integration to a national register	• 1.5 billion people globally do not have any form of official identity so may be excluded
• Lower cost and faster to implement than validated solutions	• Risk of compliance failure and data quality problems, especially through independent channels

12 http://www.gsma.com/publicpolicy/wp-content/uploads/2013/11/GSMA_White-Paper_Mandatory-Registration-of-Prepaid-SIM-Users_32pgWEBv3.pdf

Where there is no online verification of identity (which is always electronic) there may be a question of how records are captured and stored. The Australian 2013 consultation on their existing SIM registration programme, highlighted that paper based solutions are inefficient and expensive for the operators whilst also being difficult for security services to gain timely access to recorded information. Electronic records including, where appropriate, copies of relevant documents, are easier to store, easier to retrieve and less expensive. There does need to be adequate privacy protection for the records and effective rules and procedures to authorise access to the records. However, assuming these are in place, electronic record capture and storage is a preferred solution for SIM registration data.

CHALLENGES WITH AVAILABLE ID

When people have no proof of identity it is difficult for them to register their SIM card if an identity document is mandatory for the registration to be completed. In a number of markets the solution is for an individual who has identity papers to register on behalf of the person that hasn't, for example a husband registering for his wife or children. In this situation the person that registers is liable for the phone and responsible for its use. Whilst this ensures the phone is registered, the actual identity of the person using it is not known. The person using the phone will also not be able to use it for any value added services (such as mobile money services) as the details associated with the phone, which will be required for authorisation, are not theirs. In Chad, the process is different. Even in the case that the individual has no formal ID the registration is in the name of the individual using the phone. However, they can only register if they are sponsored / guaranteed by someone with formal identity documents. The identity of the sponsor is stored with the details of the registration however the liability of the phone is with the owner. The owner of the phone can also use the phone registration to access value added services including payment services.

While mobile can enable the creation of a unique identity that may provide access to some services, SIM registration databases are not identity databases and do not replace legal registers. The role of the SIM registration database is not to create an identity for individuals that have no formal papers, but merely to capture details from the presented documentation. The process is not entirely passive; At the point of registration there will be checks to ensure the identity being presented is valid. Quality assurance of the registration data is difficult. This is in part because the registration channels are very distributed, often through small third party resellers but validating the provenance of wide range of identity documents can also present a challenge. Checking for obvious 'errors', either missing data or duplicate records can be, to an extent, automated with electronic records. Where there are clear definitions relating to data quality it is also possible to automate these checks too. Qualitative judgements are however considerably more difficult to make and unrealistic expectations should not be placed on the channel partners or the operators. Ultimately it is an individual's responsibility to provide legal documentation. Consequently, where the individual intentionally defrauds the operator by using a stolen or fraudulent ID, without an effective validation process against a primary register it is extremely difficult for the operator or channel partner to detect.

ALTERNATIVES TO REGISTRATION SOLUTIONS

SIM registration is not mandatory in all markets in the world. A number of markets that have serious security and criminal threats including the USA, Mexico and the UK choose not to impose registration obligations. This reflects a balance between the effectiveness of the possible solution, the cost of implementing the solution (including the cost to consumer and limitation on the pre-paid market) and privacy concerns relating to the use of the registration information by government and operators. The main limitation for SIM registration solutions remains the potential for fraudulent registration, issues with phones being transferred to other people and the difficulty of tracking or blocking international roaming phones. The most serious terrorists and criminals are also likely to be the most effective at evading any barriers, including SIM registration, that are placed in their way.

The alternative process used by security services is usually addressed by 'lawful interception of communications' capabilities. These allow security services to monitor communications in 'real time' or to access past, stored records. Obligations are placed on operators, usually on a cost-recovery basis, to provide the capability to intercept communications. SImilarly, law enforcement agencies are obliged to justify the

request to place an intercept on a specific phone, usually through a court order. For serious crimes and terrorism communications, security experts considered intercept to be an effective surveillance mechanism.[13] It is however also essential that these capabilities are not abused in ways that might compromise citizens' privacy rights. With the exception of a small number of very specific circumstances, the interception of private communications is illegal.

Operators can also have requirements placed on them to provide the location of a specific mobile phone. This can be in exceptional circumstances, for example a life threatening emergency, or, as with intercept regulations, where security services wish to trace the location of a specific phone. It can also be part of a specific service like the e-call service[14] in Europe. Mexico repealed their mandatory SIM registration requirement, called RENAUT, and replaced it with a 'Geolocalization' (geolocation) solution.[15] This allows authorities, which have obtained a court order, to request an operator to provide location details for a specific mobile device. The primary focus of the regulation is to address kidnapping. It is expected that by 2017 mobile operators will be obliged (under geolocation rules relating to the 911 emergency service) to send mobile users' location to security authorities in order to provide assistance in emergency situations.

ALTERNATIVE REGISTRATION SOLUTIONS

ADVANTAGES	DISADVANTAGES
• There are no restrictions on the sale of pre-paid SIM cards • There are no data protection concerns related to registration data • There is no inconvenience for the customer	• Intercept is very privacy invasive and does require adequate protections • The networks need the capability to support intercept and location tracking • There is a risk governments attempt to request blanket intercepts and these can be abused • It is inevitably a breach of privacy for associated parties – many of who are innocent of any crime

It is important that any solution can effectively address the specific criminal activity it is designed to address. It is also critically important that there remains an effective balance between the rights of citizens and the need to protect citizens from external threats. In some circumstances mandatory SIM registration may not be the most effective solution to the specific concern needing to be addressed or may only form part of the solution.

13 Page 227 http://ec.europa.eu/dgs/home-affairs/e-library/docs/20150312_1_amoc_report_020315_0_220_part_2_en.pdf
14 https://ec.europa.eu/digital-single-market/ecall-time-saved-lives-saved
15 Ley Federal de Telecomunicaciones y Radiodifusión

MEXICO CASE STUDY

BACKGROUND

In 2009 Mexico introduced mandatory SIM registration ('RENAUT') with the objective of addressing criminal activities. Despite serious concerns being raised about the practicality and the effectiveness of the proposed solution, including concerns within the Mexican government from the Human National Rights Commission, industry, civil society and NGOs, the decision was taken to mandate registration for all mobile subscribers. When the 'RENAUT' rules came into effect in April 2010 there were significant on-going concerns over privacy and data security and problems registering large portions of the population who lacked official ID papers, against very short implementation timescales. The solution also failed to address criminal activity and drove up handset theft. Following consultation with the industry, academics and NGOs, the RENAUT registration programme was stopped in 2012. The database was decommissioned and the significant financial investment by all the operators and the authorities was written off. An alternative programme was introduced into the Telecommunications and Broadcasting Law ("Ley Federal de Telecomunicaciones y Radiodifusión") to address the unique Mexican market situation. This has been in effect since August 2014.

SOLUTION

The new Telecommunications and Broadcasting Law, and other regulatory provisions do not require a user to provide registration details to use pre-paid services. The law includes several obligations on mobile operators to help the government and security services address criminal activity:

1. Service Suspension: Operators are required to suspend telecommunication services of lost and stolen phones from all networks once the loss or theft has been reported. Operators can only reconnect the service once proof of ownership is provided. This measure was introduced to reduce mobile handset theft.

2. Maintain a 'stolen handsets list': To be shared among operators and updated every 24 hours.

3. IMEI Registry: From January 2016, operators were asked to set up a database of the handsets' IMEIs using their network. This registry shall be updated every 24 hours. Mexican authorities only imposed this requirement on mobile operators but not handset vendors.

4. Duplicate IMEIs: Operators must send customers a SMS when using a handset with a duplicate IMEI and offer them options to substitute it. [However, in several IMEI duplication cases there were reported difficulties in determining which of the duplicate device's IMEI is the authentic one].

5. Handset Type Approval (Homologation): Operators shall ensure that the handsets registered and using their networks conform to a Type Approval.

6. Type Approval notice: Operators must send customers a SMS when the handset used does not conform to the certified Type Approval, and offer them options to substitute it.

7. Geolocation: Upon receipt of a Court Order operators need to provide authorities the location details of a specific phone if the authorities suspect the device is being used to commit a crime. Authorities and operators are currently working on implementing the rules and addressing the technical geolocation challenges, including whether network based location information is used or (where available) device based data. Given the sensitivity of the location data and the need for legal oversight, sufficient safeguards need to be in place to protect the privacy rights of citizens and to prevent abuse of the capability. These safeguards are currently being discussed.

8. Geolocation for 911: Authorities and operators are investigating the possibility of using geolocation data to address emergency situations including hijacking and other scenarios where information is time critical. The legal processes and safeguards are currently being assessed to allow this application of the geolocation data.

MEXICO CASE STUDY CONTINUED

LESSONS LEARNT

Market Circumstance – solutions need to reflect the specific market circumstances and the issues being addressed. Lack of ID, concerns over privacy, data security and a lack of verification data muted the effectiveness of the solution.

Unintended consequences – Reportedly, criminals stole handsets to avoid the risk of being traced by security authorities. This resulted in the implementation of IMEI blocking to address the issue of handset theft.

The policy assessment of the RENAUT SIM registration solution showed it had failed to address the security concerns it was designed for, had raised privacy concerns for the registered users and also resulted in a number of cases of stolen identity.

Alternative solutions – The new 'Geolocation' solution is an alternative approach to address security concerns and criminal activity. It does not require all customers to register, does not constrain the distribution of pre-paid SIMs and is within the capability of most mobile networks. It also removes the huge logistical challenges (and costs) of implementing a pre-paid SIM registration scheme.

On-going privacy concerns – Civil society bodies are voicing privacy concerns over how the geolocation data might be used, and on the independence of the judiciary.

While the new geolocation solution has not gone without criticism, the following benefits were noted:

1. It does not require prepaid SIM customers to register.
2. It provides the location details of devices suspected of being used in crimes.
3. It focuses on the device / phone number and not the person.
4. No personal information needs to be held/ shared centrally.

Despite the lack of any empirical evidence, many governments believe mandatory SIM registration does help in the fight against crime and terrorism. However, there are many others that, on balance, believe they can address the issues in other ways and see the benefits of an 'unregistered' pre-paid mobile SIM market. These are national decisions and are dependent on national circumstances and may also be dependent on the issues the registration is targeted to address.

Implementation recommendations for policymakers

Introducing mandatory SIM registration (or changing existing SIM registration requirements) is a significant undertaking for all parties involved. Not only does it affect all customers who will be required to update their registration details, it also impacts channel partners and agents as well as the operators themselves. It is also not an insignificant undertaking for many governments, especially where there is a dependency on national identity schemes or where such schemes are necessary for delivering part of the registration solution.

There are also significant direct and indirect costs. These include the cost to individuals of having to update their details, in most cases by visiting an authorised location, and can require people to have to buy authorised identity papers if they do not have them or pay for copies of existing documents. Operators also have direct costs, which include any equipment costs, development costs and the cost of hiring extra staff to manage the process. The financial, logistical and operational impact can be so significant for operators that they may even stop accepting any new customers and stop network investments during the registration period.

Whilst it is inevitable there will be disruption, there are a number of lessons from implementations in different markets that can help minimise the impact and maximise subsequent potential benefits that can be derived from the registration exercise:

1. Consult, collaborate and communicate with mobile operators before, during and after the implementation exercise, while balancing national security demands against the protection of citizens' rights;

2. Set realistic timescales for designing, testing and implementing registration processes;

3. Provide certainty and clarity on registration requirements before any implementation;

4. Allow / encourage the storage of electronic records and design administratively 'light' registration processes;

5. Allow / encourage the registered ID to be used for other value added mobile and digital services;

6. Support mobile operators in the implementation of SIM registration programmes by contributing to joint communication activities and to their operational costs.

1. Consult and collaborate with operators before, during and after the implementation, while balancing national security demands against the protection of citizens' rights

The implementation of mandatory SIM registration, or changes to existing requirements, inevitably impacts all pre-paid mobile users. Ensuring that the proposed solutions minimise disruption, maximise the potential benefits for all stakeholders and provide essential protection for citizens' rights is a priority for all implementations. Most solutions are a trade-off between a number of conflicting demands including: supporting security services and protecting citizens rights, assuring the identity of registered users and excluding vulnerable members of society, implementing solutions quickly and minimising disruption, minimising security threats and maximising social and economic benefits. With mobile telecommunications being so pervasive it is essential that mandatory SIM registration programmes are carefully managed to minimise unforeseen consequences and maximise potential benefits.

CONSULTATION

Engaging and consulting with operators prior to implementing any changes is essential to minimise potential disruption and maximise the potential benefits that can be derived from any exercise. The consultation process also helps to get alignment across the operators, which simplifies the implementation challenges. A wider range of stakeholders should be invited to contribute to the consultation process; security services will need to be involved but it is also important to include representatives of civil society to ensure there is a reasonable balance between the demands for national security and the protection of citizens' rights (privacy, data protection, freedom of expression etc.). Engaging more widely to understand the wider benefits that can be derived from the registration solution is also beneficial. For example, if mobile registration is communicated and implemented effectively it can be used to enable and incentivise access to payment and financial services, mobile health services, e-government services and a range of other applications that depend on a proof of identity. Where practical, there should be an attempt to align the KYC requirements across sectors to remove potential barriers to the use of a mobile identity in enabling these value added services. This maximises the potential economic and social benefits from the mandatory registration exercise and ultimately minimises the disruption and 'overhead' for consumers. The consultation process should invite participation from the wider stakeholder community and consider the broader potential benefits that mobile SIM registration can deliver for the wider economy.

The consultation process should also include an impact assessment to determine the feasibility, benefits and costs of possible registration solutions, balancing the different policy priorities. In the 2013 Australian consultation[16] reviewing their existing mandatory registration solution, the preferred option was to require verification against a national Identity register. However, concerns over availability of the national register for commercial enterprises and practical concerns over the ability of the operators to coordinate implementation meant that the decision was taken to phase the implementation and not to demand a hard cut-over. Whilst it was acknowledged this would delay the realisation of some of the benefits, it was concluded that, on balance, this was preferable to risking considerable disruption.

16 Department for Broadband, Communication and the Digital Economy. Regulation Impact Statement. Proposed Changes to Identity Verification Requirements for Prepaid Mobile Services. February 2013

CLARITY OF OBJECTIVES

It is essential that the objectives and the desired outcomes from any registration exercise are clearly stated and that the solutions implemented address the specific problems identified. Clarity of the objectives also makes it easier to undertake accurate impact assessments and to evaluate different implementation options. Governments often see mandatory SIM registration as a tool to address 'criminal behaviour'. When outlining their objectives policymakers should specify exactly what behaviour it is that needs to be addressed and how mandatory SIM registration would specifically address the issues. In some markets terrorism is the focus and politicians believe there is a direct link between unregistered SIMs and terrorist activity. Nigeria's President Buhari stated *"You know how the unregistered [SIM cards] are being used by terrorists and between 2009 and today, at least 10,000 Nigerians were killed by Boko Haram."*[17] In many Latin American markets the focus is on handset theft and on criminal activity including hijacking. As the Mexican case shows there are different ways of addressing the problem. In Ecuador where there are reportedly approximately 1000 handset thefts a day, the focus of their registration policy is on registering IMEIs to specific users and optimising the processes to block lost and stolen handsets.

17 http://www.bbc.co.uk/news/business-35755298

ECUADOR CASE STUDY – ADDRESSING HANDSET CRIME

BACKGROUND

Ecuador introduced mandatory IMEI registration in 2009 with a deadline to have all customers registered by July 2012. All mobile users in Ecuador are registered. The objective of the solution was to address issues with handset theft although there were also concerns of criminal activity, including hijacking.

Ecuador has a comprehensive Civil Register and has provision to allow foreign nationals to register and for refugees to be able to access services. Although every citizen receives a Civil register number from birth, and this number is used for all official documents, citizens have to be over 18 before they can register for a phone. Parents can register on behalf of children and there is no limit on the number of registrations an individual can make.

The solution focuses on IMEI registration (this is the unique reference number for the handset), which the mobile operator is required to store against each customer's SIM (mobile phone) number. Consequently, as the customer needs a SIM to access the mobile network the operator has details of both the IMEI and the SIM associated with each of their registered customers.

SOLUTION

Operators will not connect a handset to the network unless the IMEI is registered with the customer's details and they have received verification from the Civil Registry.

No mobile registration data is stored centrally, this is all held by the operator, including the verification data from the registry.

Arcotel (the regulator) holds an IMEI blacklist of all lost and stolen handsets. There are defined processes to verify ownership of handsets, customer details and to block handsets nationally on notification. There are also processes to lift the block if the handset is found.

Tools are provided to allow customers to check their registration details are correct. Unless these are maintained it is very difficult for a customer to unblock a phone, this acts as incentive to maintain personal registration records.

Pre-paid registration and verification can be completed via IVR or via a call centre. There is no requirement to store copies of ID documents. Post-paid requires face-to-face; the registration information required for pre-paid and post-paid customers is tailored to each contract type.

Operator compliance is checked through audits of their registration data.

LESSONS LEARNT

1. The implemented solution leveraged the Civil Registry to validate identity giving a high degree of assurance that the verification is correct.
2. The solution is very tailored to addressing a particular problem and citizens understand the practical benefits to them of ensuring they have registered correctly.
3. The registration data has improved internal operator processes (e.g. refunds). The registration process is tailored for pre-paid and post-paid customers.

IMPLEMENTATION CONSIDERATIONS

Logistical practicalities and legal implications need to be carefully considered before defining SIM registration solutions. These include the existence of conflicting laws or citizens' rights, the role of channel partners in the registration process, the physical capacity to process subscriber registrations, the availability of required equipment (e.g. scanners / copiers), and requirements for any integration and verification solutions. The practical implications of any registration requirements also need to be considered. In Chad, for example, there is a requirement for the person registering their phone to provide a photocopy of their identity document (or the identity document of their sponsor). Whilst the availability of identity documents is a challenge (only 20% of Chadians have any), access to photocopiers is significantly more challenging as outside the urban areas only 1% have access to electricity with access to photocopiers even more limited. The intention of the registration requirement in Chad is not to exclude people from having a mobile phone but the implementation requirements create barriers that make the process more difficult for consumers than they need to be.

The implementation requirements can also reflect where in the process the registration and identification is required. This can be at the time the SIM is purchased or at the time of activation. In many Latin American markets the registration details are assigned to the handset (IMEI) and not always against the phone number (SIM); Again the practical considerations of when and where registration details are captured need to be considered depending on what information is required.

The role the government and the regulator play in the registration process also needs to be considered. Where there is a dependency on the availability of national identity it is important to consider that registration should not become a significant barrier for people accessing mobile communications services. In Pakistan the linkage of SIM registration to the NADRA national ID scheme may have helped accelerate registration for the final 10% of the population that NADRA did not previously cover. The government and the operators worked very closely together to maximise the opportunity for people to complete their registration on time. Even with this close cooperation the registration deadline was extended before, ultimately, 27 million SIMs were deactivated. In Nigeria, the Nigerian Communications Commission (NCC) directly supported the initial registration activity by helping to undertake the registration of mobile users on behalf of operators. These activities can help if they are closely coordinated and there is a clear understanding of the roles and responsibilities of all people involved in the process.

Throughout the design, implementation and on-going management of a registration scheme there should be an active working group that includes the operators, security services, the government and regulator. They should jointly manage the process as well as addressing potential issues and challenges. This open dialogue is essential to ensure effective implementation and minimise the potential for disputes.

COMMUNICATION

The final area where coordination is required and where proactive involvement from government can make a significant difference is communication. Governments can communicate the context for the mandatory SIM registration requirements and the importance of any requirements to meet their national security priorities. Without an effective government campaign on TV, radio and the press to communicate to citizens the need to register it can be very hard to get citizens to complete the process. The campaigns will be more effective when they are united under a common theme; The United Arab Emirates' "one mobile, one identity" campaign is an example of this approach.

It is important that governments highlight the 'civic value' of registration. Operators have the ability to target communication to individuals through text campaigns, to promote the requirements through channel partners and retail stores and to even put special teams into areas to help the registration process (there are examples of these different activities from markets across the world). Customers will however see many of these campaigns as commercially driven unless they are supported by overarching messages from government.

2. Set realistic timescales for designing, testing and implementing registration processes

Whilst there will be pressure to implement quickly, the most important consideration is to implement as effectively as possible. Processes and technology solutions need to be robust and scalable with the capacity to manage the demand.

DESIGN & TEST

Systems need to be extensively tested across all operators to ensure data capture is effective especially if validation against a central database is required. Procedural issues and technical problems can lead to consumer frustration and increased costs. This is especially important where the solutions require verification against central identity registry and where there is a biometric requirement. Full-scale implementation should not go ahead until the end-to-end solution is fully tested and the solutions have been proven to be reliable. As biometric verification is particularly challenging and repeated failures to verify customer biometrics cause significant frustration (not least because it may be unclear if the issue is with the national register or the operator biometric database) it is critically important to extensively pilot solutions in a 'real world' environment prior to full scale implementation.

NEW CUSTOMERS REGISTRATION OR RE-REGISTRATION OF EXISTING CUSTOMERS

Phasing in new registration requirements by limiting the requirement to new activations controls the initial demand and reduces the logistical challenges of simultaneously managing millions of customers. Where new technology is being used it also minimises the risk of technology issues having a significant effect. While it would take longer for an operator to register its entire customer base, this may form part of a phased approach to implementation where new requirements are being introduced. As existing customers will already have a registration based on the existing systems, phasing the introduction by limiting the registration requirement to unregistered new customers minimises the logistical challenges and disruption to customers.

Re-registering an entire installed base of mobile subscribers is a huge logistics exercise. Overly ambitious timescales can be expensive and create frustration with citizens. In areas of civil unrest they can also create a security risk, as large queues of customers are required to wait to re-register their phones before deadlines. Where there is a requirement to re-register the entire customer base it is important the timescales are realistic and that registration milestones are set to assess progress and action taken to address issues if delays become apparent.

DEACTIVATION

In an ideal world the only SIMs that would be deactivated and barred from accessing mobile networks would be those that customers deliberately had deactivated, perhaps because they decided to keep a different SIM. In reality, this is rarely the case with large numbers of customers' SIMs deactivated, only to reactivate the service after they have been excluded. Whilst the security priority may be to exclude unregistered SIMs, there is a need to balance this priority against the financial and social impact of excluding large numbers of people. Setting reasonable timescales for registration and potentially limiting services for customers that haven't registered are both approaches that can mitigate the risk of deactivation. To encourage registration a number of markets block some aspect of the service for a period before deactivating it completely. Niger, for example, blocked outgoing calls for three months prior to deactivation.

The people most at risk of deactivation are also the most vulnerable and socially disadvantaged citizens, especially those in rural areas. These citizens are often the same citizens that lack official ID papers and have

the least access to locations that allow them to register. If implementation timescales are set too aggressively it is this community most likely to suffer.

Whilst financial considerations rarely have a bearing on decisions related to mandatory SIM registration there is potentially significant impact on operator revenues and on tax revenues from deactivating large numbers of people who have failed to register. There is also significant evidence that the economic and social costs of exclusion are high. There is an impact on GDP, an impact on investment and all of the negative effects of digital exclusion for citizens. The registration process should look to encourage active users to register and to use mobile services; they should not exclude citizens, especially those who fail to register unintentionally.

BANGLADESH CASE STUDY – PILOTING AND PHASING IMPLEMENTATION

DESCRIPTION

The Bangladesh Telecommunications Regulatory Commission (BTRC) and the government decided to introduce mandatory SIM registration using biometric identity with verification against the National Identity register (NID).

The programme started in September 2015 with a test and trial phase. All operators are connected to the NID via an Application Programming Interface (API) to link their registration information with the NID scheme. From 1 January 2016, all new registrations are obligatory using the NID and without a validation the SIM will not be activated. From Feb 1st operators were obligated to re-register existing subscribers (not only new) and by the end of April 2016 it is planned that 80% of all subscribers will be registered.

As 8% of the population lack a biometric NID there is a registration process that allows registration by the operator – using passport, birth certification or other 'official' identification. The user will however need to have registered and validated against the NID within 6 months or the service will be deactivated. There is a different process for corporate SIM registration of post-paid contract subscribers.

The implementation in Bangladesh was on-going in April 2016 (at the time this paper was published) but there are some valuable lessons from the programme so far.

CHALLENGES

There are a number of known challenges facing the implementation that are currently being addressed:

- 10% of the biometric matches 'fail' either because of an issue with the NID or an issue with the operators' biometric optimisation of the process. The technology has improved the performance since the initial pilot but improvement is still required.
- The processing speed for the SIM validation request against the National ID in the trial was not adequate (too slow). This has been identified as an issue and is being addressed.
- SIM tax: there is a SIM tax of c.USD1.2 per SIM. This currently applies to new registrations and to re-registration. There are on-going discussions with the Ministry of Finance to remove the tax obligation, this is possible but not yet confirmed.
- As there are 137 million SIMs in the market, the potential costs for retailers to undertake registration is high (even without SIM tax) and this may lead to some inertia.
- There has been a legal challenge on the rights of private companies (operators) to capture biometric data. At the time of writing this paper, this challenge remains open.
- There are ongoing discussions with the financial regulator as to whether the verified biometric registration can be used for financial services (or whether a separate registration is still required).

LESSONS LEARNT

- There is a consultative approach between the BTRC and the operators to minimise the disruption caused by the introduction of mandatory SIM registration.
- The implementation has been piloted and the introduction is phased. The BTRC are also taking a cautious approach and do not want to disconnect large numbers of users.
- There has been an extensive communication campaign by the government to raise the profile of the biometric SIM registration requirement.
- There remain a number of open issues and challenges that will put pressure on the implementation as it progresses. Resolving some of these before scaling the implementation may have removed some of the implementation pressure.

3. Provide certainty and clarity on data requirements before implementation

Defining the exact specifications for the data required during registration is essential to prevent disagreements over data quality that can result in customers needing to revalidate details. All data requirements need to be defined, and agreed, prior to implementation. This includes defining the mandatory data fields required on any registration form, the 'proof of ID' records that can be used or need to be presented, specifications for photographs if required, biometric details when appropriate, archiving requirements and data protection requirements. Given the huge logistical implications of making subsequent changes and the impact on consumers of these changes it is important to ensure the specification is well defined and understood from the outset. This should form part of any consultation process.

AVAILABILITY OF IDENTITY DOCUMENTS

Any requirement for registration data needs to reflect the availability of identity documentation across the population. Where National identity documentation is widely available it is usual that this is the primary proof of identity. In many countries this is not the case and a variety of different forms of identity are used to prove an individual's identity, these can include passports, driver's licences, student cards, government ID cards, refugee cards and other official documents. It is important to provide an option for foreign nationals to register for local SIM cards too – passport details or resident permits are the usual identity documents for these customers. There needs to be a pragmatic solution to handle customers who have no formal identity that allows them to get access to communication services and doesn't unintentionally exclude them.

PROTECTING PRIVACY

The information being captured should be the minimum required to prove the person's identity and to allow access to mobile communications services. Mandatory SIM registration should not be used to collect general census information on the population. In most cases the purpose of mandatory SIM registration is to exclude criminals from accessing mobile services and to trace users suspected of criminal activity. Collecting a wider range of data on sex, religion, ethnicity or other profiling data will raise concerns over the purpose and use of the registration information. Unless the use of this data can be demonstrated to help address the issues mandatory SIM registration was introduced to address, it should not be collected.

The information captured during the registration process should also only relate to persons being registered (or, where relevant, their sponsor). Collecting information on third parties as part of the registration process, including other people's phone numbers, should be avoided as it raises privacy concerns.

VERIFICATION

As previously discussed, any registration system will be more robust if there is the possibility to verify information against a National register. Any verification requirements have to be appropriate for all of the channels that can be used to register and activate a SIM. In many cases these are third party agents working in remote, rural locations. Verification requirements need to be designed pragmatically to ensure that these distribution channels remain viable as they provide a valuable service to large sections of the community.

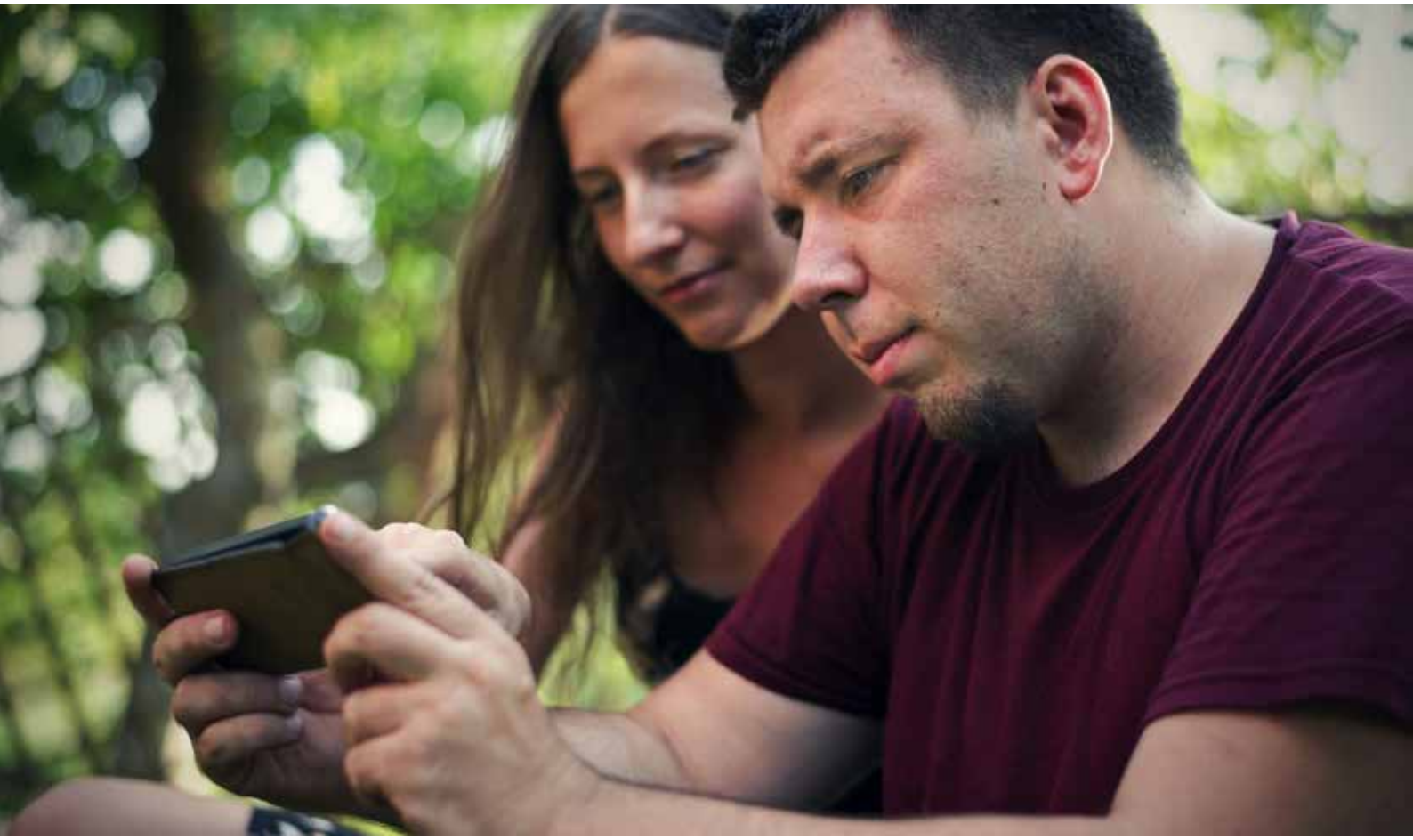
In the majority of cases the verification is a manual process of checking a presented identity document against the person physically present at the time and recording the details. Quality checks can be completed

to ensure the correct fields have been completed and to check for obvious discrepancies but where validation is based on visual inspection it does depend on the judgement of the person undertaking the check. Understanding exactly what information needs to be captured and the important of accurately collecting this information is critical to avoid compliance issues.

IMAGES AND BIOMETRICS

It is not uncommon to have a requirement to keep a copy of the identity document used as proof of identity. Many countries also require a photograph of the user; in some countries there is also a requirement to capture biometrics, usually fingerprints. As with other forms of data it is important that the specifications for all types of images and biometrics are clearly defined to ensure consistent quality. These requirements need to be pragmatic and do need to reflect the physical and environmental constraints of the likely locations where registration is undertaken. These can be at retail stores and channel partners. The priority is to define the requirements so they are achievable in the environment the registration will be undertaken in, for example defining the format of any ID photograph. This will help to prevent subsequent issues with compliance. Requirements should be realistic and the rules easy to understand for all of the people implementing them, including the frontline staff in the retail locations.

Some individuals do have issues providing readable biometric data; for example, it is not uncommon for construction workers to have indistinct fingerprints. Where biometrics are being used as a primary source of identity it is important that there is an 'exception' process to address individuals that otherwise would be excluded because they can't provide fingerprint information. Ideally this process would not make the individual dependent on someone else for the provision of their phone service, not least because without a verified identity they would not be able to access value added services.



4. Allow / encourage the storage of electronic records

Making the registration process as simple as possible and the management of data as easy as possible is critical to implementing an effective programme. Encouraging electronic registration solutions is best for citizens, security services, operators and governments.

Electronic records are now easier to capture, easier to store and easier to retrieve. They allow for instant provisioning of the service without the need to validate receipt of a paper record (the time delay between postage and receipt is a potential security risk). Records do need to be secure, both at an individual level where personal information needs to be protected and secured to prevent potential identity theft and at a system level. It is essential that the security of the electronic personal data records is maintained. Whilst data protection rules are not unique to SIM registration data it should be acknowledged that the data are likely personal in nature and that only authorised people in specific, defined circumstances should be allowed to access it without the affected consumer's consent.

Physical records are expensive to handle, hard to store, difficult to retrieve and have limited value for analysis. As mobile data networks become increasingly pervasive the need for paper-based solutions becomes increasingly less relevant. If there is a requirement to store physical records of registration information it is important for policymakers to define the details of how the records need to be archived, how long the records need to be kept and how old records need to be destroyed securely.

TANZANIA CASE STUDY – USE OF ELECTRONIC RECORDS TO IMPROVE THE REGISTRATION PROCESS

DESCRIPTION

SIM registration was introduced in 2010 using a paper-based system of forms and copy of the customer's ID. A customer can use up to 12 different ID documents to prove their identity. The paperwork for newly activated SIMs must be received by the operator within 30 days or the account is suspended.

In 2015 electronic records were accepted for registration. The record contains an electronic form with photographs of the ID document and of the person. This simplified the process, speeded up confirmation by the operator that the record was complete and improved reliability. The new electronic records can be used as KYC for other services.

LESSONS LEARNT

Improved process and quality assurance:
The electronic data capture allows for some data entry validation. The Android / IOS application, utilising mobile data networks, has provided rapid reach and an affordable solution for channel partners.

Efficiency: Electronic record storage is more secure, easier to recover records if required and cheaper to manage. It is also faster, potentially closing loopholes in security arrangements.
The applications do improve the overall customer experience.

Accuracy: Electronic records help to improve initial data collection. However without validation against a National ID challenges remain with overall registration assurance.

5. Allow / encourage the registered ID to be used for other value added services

There are significant benefits in allowing mobile registration data to be used as a 'digital identity' for access to other services. In many markets this is already allowed with mobile registration being used for access to payment and other value added services. This is however not always the case. Some markets explicitly prohibit the use of the data for anything other than SIM registration and some regulators from other sectors insist on a secondary 'know your customer' (KYC) check before a service can be activated.

MOBILE 'DIGITAL IDENTITY'

Where it is possible to verify a person's ID against a central customer register, allowing the use of this information for KYC for value added services benefits consumers (it saves multiple registrations), can accelerate access to services and saves cost for operators.. Secure mobile authentication and/or authorisation, linked to registration can enable a number of value added services for consumers. In circumstances where verification of ID documents is not possible it may still be possible to create a mobile 'digital' identity at the point of registration or even after activation where customers provide a secondary form of authentication. Once the registration data is verified and linked to a secure authentication process, customers should be able to access a range of value added services without the need to go through multiple registrations. Where the mobile is used to provide secure authentication there are added advantages for the customers as they no longer need to use multiple different authentication methods (e.g. usernames and passwords) to access the value added services.

SOCIAL AND ECONOMIC IMPACT

The potential positive contribution of mobile registration should be considered as well as any role it may play for addressing security concerns. When implemented effectively, and assuming the appropriate consumer safeguards are in place, mobile registration can facilitate financial access, help National ID registration and enable access to government services. Whilst mobile services deliver social and economic benefits on their own, enabling other services delivers incremental value. In 2015 the indirect benefits of mobile on the wider economy through general economic development and productivity improvement was 2.7% GDP growth, which globally equated to $2.025 trillion.

Whilst addressing security and crime is the main reason governments give for the introduction of mandatory SIM registration requirements, the opportunity to add social and economic value should not be ignored. For many customers this can add significant value and it can also help other government departments achieve their public policy objectives and goals. Given the significant costs involved in implementing the registration process, maximising the benefits that can be derived from the exercise is very important.

PAKISTAN AND NIGERIA CASE STUDY – DIFFERENT APPROACHES TO USING REGISTRATION DATA AS A DIGITAL IDENTITY

DESCRIPTION

Both Pakistan and Nigeria collect biometric data during the mobile registration process. In Pakistan, operators validate the biometric against a National ID database (NADRA). Nigeria has no validation but the biometric (thumbprint impression) along with an ID reference and a photograph are held on file.

The Pakistani government and Telecoms regulator have actively encouraged the use of the mobile registration to enable value added services. The validated ID is accepted as meeting the KYC requirement for mobile banking and the government is looking to use the ID to provide access to e-government services.

Nigeria specifically prohibits the use of the ID information for anything other than mobile registration.

LESSONS LEARNT

Validation: The validation against a National ID database using biometrics gives a high level of assurance that the identity of the registered individual is correct. This opens up the potential for mobile to be used as a digital identity for accessing value added services.

Benefits: Increasing the opportunity to use of the mobile registration data for value added services increases the incentive to clean and maintain data. This benefits consumers, government and operators.

Amortising costs: By using mobile registration as a digital identity, costs for consumers and operators are shared across all mobile services. This encourages uptake of services, including financial services and e-government services.

6. Provide financial and logistical support to mobile operators for implementing the mandatory registration exercise

Registration is challenging for operators and requires effort from consumers. Minimising the barriers to re-registration for consumers is critical. Governments can help with logistical support and consumer awareness campaigns, and can ensure there are no financial implications for consumers. Governments can also provide support for operators directly by providing support to operators that reduce the registration costs.

FINANCIAL SUPPORT

All mandatory SIM registration programmes are expensive to implement as they involve system development, logistics and communication costs. Solutions that involve biometric registration will also require investment in biometric equipment for all of the locations that will be registering customers. These costs can be significant, especially where the obligation on operators is to implement the registration exercise over short timescales which requires them to equip as many locations as possible.

Given the principal benefit of mandatory SIM registration solution is one of national interest, the use of Universal Service funds or government grants may be appropriate to support the operators during the implementation. It is likely, to ensure transparency, that these funds will only be provided to cover direct costs, including equipment costs. The advantage to governments supporting operators is twofold. Firstly it will ensure that operators aren't required to pass on any increased costs to their subscribers (this is unlikely to be a direct pass though but may be reflected in general tariffing or activation charges). Secondly it will ensure that capital investment budgets within the operator are allocated to network investment, which will deliver wider benefits to the economy, rather than directed to SIM registration requirements.

MINIMISE CHARGES AND FEES

Minimising financial costs to consumers and operators involved in registration is critical to reduce consumer barriers in implementing SIM registration. This is especially important with mass revalidation of existing customers. Governments should address incremental costs for consumers when they mandate SIM registration or re-registration. SIM activation taxes should not be applied to active SIMs if all the customer is doing is registering their details (they could still apply for new activations). Taxes should also not be re-applied to customers re-validating their ID when the registration requirement changes.

Where fees are charged for validating a person's ID against a central registry, these fees should be waived during the re-registration exercise. Waiving these fees has the same effect as suspending SIM activation taxes, i.e. it reduces the cost for an individual to register. As the purpose is to register as many customers as possible and to minimise disruption as much as possible addressing potential financial barriers is critical.

GOVERNMENTS' ROLE IN SUPPORTING IMPLEMENTATION

DESCRIPTION

The government in Pakistan led a Nationwide communications campaign, supported by operators, to encourage people to register. They set up National ID centres to ensure consumers had a valid National ID and waived look up charges to the NADRA database during the re-registration programme.

Bangladesh currently has on-going discussions on whether SIM activation taxes should apply to re-registration. It is seen as a major risk to the programme with the BTRC and operators united in their request to waive the fees.

The NCC in Nigeria set-up registration centres to allow existing customers to register directly with them and not via their operators during the initial phases of the programme. Whilst helpful, closer coordination with the operators could have reduced some duplication of effort and maximised the value of the investment.

LESSONS LEARNT

Communications: A government led national campaign highlighting the consumer imperative to register is invaluable. Consumers respond better to these campaigns than operator led initiatives.

Charges and fees: Consumers should not be charged for re-registration, operators should not be expected to carry costs for fees and taxes. Reducing financial barriers is critical.

Hidden costs: Costs also need to be considered, having a requirement of official papers that are not widely available and charged for may result in exclusion of many people with no ID and / or increase incentives for individuals to try to circumvent rules.

Support: Operations support can be helpful if it is well coordinated. Financial support to cover exceptional costs including hardware (possibly from Universal Service Funds) should be considered.

Implementation conclusions

Mandatory SIM registration is a policy adopted by a number of governments as part of efforts to help mitigate security concerns and to address criminal and anti-social behaviour. Introducing or changing mandatory SIM registration solutions is logistically challenging for all parties involved including consumers, operators, their retail partners and governments. Any decision to implement, or change, a SIM registration policy should only be taken after consultation with all stakeholders and after completion of a comprehensive impact assessment that reviews all possible options to address the specific concerns in the market, including consumers' privacy concerns and expectations.

Where public consultations are carried out to assess the implications of mandating SIM registration, the exercise should:

- Consider the costs and benefits of mandating registration (as opposed to encouraging voluntary) registration;
- Ensure that the proposed registration solutions take a long-term perspective and take local market circumstances into account (e.g. ability of mobile operators to verify identity documents) to mitigate the risk of excluding vulnerable consumers from mobile and digital services; and
- Ensure the proposed solution creates the maximum possible value to society – e.g. by supporting Digital Identity initiatives which could enable consumers to access value added services (this may well encourage them to register voluntarily).

There are a number of best practices that have been identified from different mandatory SIM registration programmes across the world. In order to minimise the implementation challenges and maximise the subsequent potential benefits that can be derived from the registration exercise, this paper outlined the following recommendations for policymakers:

1. Consult, collaborate and communicate with mobile operators before, during and after the implementation exercise, while balancing national security demands against the protection of citizens' rights;
2. Set realistic timescales for designing, testing and implementing registration processes;
3. Provide certainty and clarity on registration requirements before any implementation;
4. Allow / encourage the storage of electronic records and design administratively 'light' registration processes;
5. Allow / encourage the registered ID to be used for other value added mobile and digital services;
6. Support mobile operators in the implementation of SIM registration programmes by contributing to joint communication activities and to their operational costs.

To download the report,
please visit the GSMA website at
www.gsma.com/mandatory-sim-registration

GSMA HEAD OFFICE
Floor 2
The Walbrook Building
25 Walbrook
London
EC4N 8AF
United Kingdom
Tel: +44 (0)207 356 0600
Fax: +44 (0)20 7356 0601