How eSIM devices will impact electronic Know Your Customer (eKYC)

CONNECTIVITY

POSTED ON 07.27.20

By the year 2025, there will be over 2.5 billion consumer devices with an embedded SIM, or eSIM, providing connectivity. Smartphones, watches, tablets, laptops – to name just a few devices – will revolutionize the way mobile network operators engage with customers and design the mobile subscriber experience.

Since an **eSIM** is embedded in the device, it eliminates the need for customers to go to a store to activate a subscription. Now they can **activate anytime and anywhere** – from the comfort of their own home, or on-the go like when travelling abroad. Customers can browse different subscription plans directly on the device, complete the enrollment process, and then instantly download the eSIM profile onto the device.

In a retail environment, mobile network operators (MNOs) can verify the identity of the customer by asking for ID documentation and performing other know-your-customer (KYC) checks. With the growth of eSIM devices, MNOs are under pressure to offer a similar onboarding experience but in a remote environment and without the support of a brick-and-mortar shop and trained representative.

In particular, MNOs need to **verify the identities of their customers** in this increasing digitalized world, not only to comply with KYC and AML (Anti-Money Laundering) regulations and fight against identity fraud, but also to offer a personalized experience and create new revenue streams.

Compliance with AML and KYC regulations

To fight against terrorism, money laundering, and other criminal activities, governments in more than 150 countries require proof of identity for access to mobile services[1], which includes eSIM devices. In addition, MNOs are increasingly offering customers financial services and must comply with the same KYC and AML regulations applied to financial institutions.

In many cases, proof of identity is limited to showing a physical identity document to a sales person. This leads to high fraud rate, as in-store representatives are unlikely to be trained in document fraud detection, or could be bribed to waive the ID verification. Furthermore, a face-to-face KYC process is cumbersome, forces MNO to invest heavily in stores, kiosks, and personnel, and forces customers to travel to these locations, which can be difficult for rural and remote communities.

The combination of eSIM devices and eKYC are fundamental to addressing these issues – offering a convenient digital onboarding process while complying with AML/KYC regulations and reducing fraud.

Fighting against identity fraud

Subscription fraud, which involves identity theft and fraud, is one of the fastest growing and most prevalent types of fraud in the telecommunication industry. It now accounts for up to 35-40% of all fraud in the industry, totaling $30 billion globally according to CFCA[2].

Capitalizing on fabricated or stolen identity credentials that are sold on the dark web following massive data breaches and social engineering attacks, fraudsters sign up for new accounts or take over existing ones. It enables them to defraud telecom operators by getting their hands-on expensive smartphones and abusing service contracts.

Telecom fraud also provides a gateway for fraudsters to take over the other accounts of their customers, including financial services that rely on SMS verification for authentication. This is the typical case for SIM swap fraud, where a fraudster transfers a customer's phone number to a new SIM and intercepts the verification SMS before the customer is alerted.

In one case, a U.S. investor lost $23.8 million in cryptocurrency due to SIM swap fraud, and launched a lawsuit against their MNO on grounds of gross negligence and failing to protect their digital identity[3].

Trusted digital identities for a seamless digital experience

Now more than ever, the need for trusted digital identities is the key to digital transformation and growth across all industries – not just the telecom sector. As smartphones, wearables, and PCs become connected to cellular networks and provide an always-on experience, consumers will expect a seamless **digital onboarding journey**.

The smartphone in particular is key to unlocking this digital onboarding journey. The vast majority, if not all, of the smartphones shipped today include some form of biometric sensor technology[4]. This means that people with these devices are able to utilize the cameras and fingerprint sensors to verify their identity remotely.

For example, taking a photo of an official ID document means that it can be analyzed and verified for its authenticity – far more accurately than any salesperson is able to detect.

Similarly, **a selfie portrait can be taken on the smartphone**, its biometric template extracted, and then compared with the portrait in the ID document or even against a trusted, national database. The same applies to fingerprints. They too can be captured and verified using only a smartphone camera.

The technology capable of **accurately verifying the identity and liveness of individuals** is here, and is in the hands of billions of people worldwide.

Combining these identity verification technologies with eSIM devices means that MNOs will have the opportunity and means to create the digital onboarding journey that their subscribers expect, while simultaneously fulfilling KYC and AML regulations and significantly reducing fraud.

Beyond the persona: leveraging device identity for another layer of security

Creating a trusted identity goes beyond verifying who a person is. An identity can also be verified based on what people know or what they possess. Whenever customers are performing actions or transactions – like opening a new account or accessing an existing account – the more factors taken into consideration results in a higher level of assurance that

the consumer is who they say they are.

SIM swap fraud is one way that fraudsters have been able to circumvent the “what you possess” factor. By transferring the mobile number to a new SIM in their possession, fraudsters are able to intercept verification messages and then access victims’ accounts.

eSIM devices hold the promise of reducing this type of fraud. Not only is the eSIM embedded in the device, making it physically impossible to remove and use in another device, but the very architecture of remote SIM provisioning (RSP) as defined by the GSMA forbids a profile from being transferred from one device to another without explicit consent of the user. In other words, **eSIM devices are more impervious to fraud**.

In addition to this, MNOs can capture the unique identifier of the device (the IMEI or International Mobile Equipment Identity) as well as the eID (the unique serial number attached to the embedded SIM) during the onboarding process. Then later, when the customer is requesting access to their account or trying to perform a sensitive transaction, the MNO can compare and verify the device IMEI and/or eID being used against the values captured during onboarding.

Creating value

In today’s world, our digital identities have a lot of value. They enable mobile customers to access key services such as banking, e-commerce, health, and travel.

MNOs have a unique position to provide digital identities to consumers: an unparalleled global reach, consumer trust, and huge amount of mobile device data, including roaming, SIM swapping, lost & stolen devices, and location data.

Therefore, MNOs could turn the constraints of having to comply with KYC regulations and fighting against fraud into new revenue streams. Primarily, it would enable them not only to offer a complete and **seamless digital experience**, notably for eSIM activation, but also to use their customer insight to better segment, target and personalize their offerings.

Subsequently, they could also derive revenue from providing identity services, such as identity verification, authentication and fraud detection, to adjacent service providers.

Thus, digital identity could contribute to a telecom operator’s differentiation strategy in a highly competitive mobile market.

---

[1] GSMA Access to Mobile Services and Proof of Identity 2019 (https://www.gsma.com/mobilefordevelopment/resources/access-mobile-services-proof-identity-global-policy-trends-dependencies-risks/)
[2] https://www.telecomengine.com/article/telecom-fraud-29-billion-and-counting-why-it-matters-more-than-ever-in-the-digital-era/
[3] https://www.reuters.com/article/us-cryptocurrency-at-t-lawsuit-idUSKBN1L01AA
[4] https://mobileidworld.com/smartphone-biometrics-are-officially-mainstream-acuity-102124/
