THALES

gemalto
a Thales company

From necessity to opportunity:

How Mobile Network Operators stand to benefit from trusted digital IDs

Table of Contents

1. Identity in era of digital transformation

Digital transformation is already well on its way. The ubiquity of mobile phones, in particular, is prompting businesses and organizations to fundamentally re-think how they reach their customers and design their services.

The scale of this change is colossal. In 2017, the world's mobile industry welcomed its 5 billionth unique mobile subscriber – meaning that more than two-thirds of the planet's population is now connected to a mobile service.[1] How we access the internet is changing in lockstep. In 2018, it's estimated that 73% of internet use will originate from a mobile phone.[2]

In 2018, an estimated

73% **of internet use will originate from a mobile phone**

As with all other industries, Mobile Network Operators (MNOs) need to adapt to this rapidly changing atmosphere. They are grappling with the need to claim territory in the digital market and provide more and more innovative services to meet the growing demand from their customers.

While they go about reshaping their business model, MNOs simultaneously face the need to streamline their operations and acquire new customers. In response to these diverse challenges, MNOs can begin by changing the way they manage their customer's identities. The following drivers of change illuminate both the need for and opportunities inherent in offering trusted digital IDs.

1.1 Consumer needs for convenience and security

People are rapidly becoming accustomed to seamless and enjoyable digital journeys, and have begun to expect simple and fast access to a wide range of services. In fact, 66% of users say they would perform even more transactions on their phones.[3]

The convenience and cost-effectiveness of mobile access has moved our most important procedures and transactions to our smartphones. Yet this change is accompanied by a pronounced need for secure identity verification. 43% of users fear fraud, phishing, hacking and getting their personal information stolen (after losing their mobile phone and data and running out of battery).[3]

In short, fraud protection and digital security methods need to keep pace with increasing convenience so customers can feel safe accessing a new generation of services.

[1] GSMA Intelligence (2017)
[2] Zenith's Mobile Forecast report (2017)
[3] GTO 2017 survey 1,300 interviews conducted across Brazil, UK, South Africa, Singapore, the Netherlands and the U.S.

1.2 Government initiatives and regulations

Across the world, governments are passing legislation to protect their citizens from scams, fraud, and crime. Identity verification is front and center, as crimes like money laundering and terrorist activity typically involve fake or stolen identities, and accounts tied to false or absent identities.

In response, regulations like Know Your Customer and SIM card registration require businesses to have more rigorous processes and secure systems for verifying the identity of their customers. This is certainly in the interest of MNOs, as subscription fraud represents 20% of all telecommunications fraud.[4]

Other regulations are aimed at streamlining and fostering compatibility across systems and agencies. eIDAS, for example, is paving the way for single digital European market, with national digital IDs accepted across borders. New technologies and standards are not just helping multiply government initiatives — such as with national ID schemes and smart borders — they are also helping private companies accelerate their own digital transformations.

Subscription fraud represents

20%

of all telecommunications

fraud

WHAT IS A TRUSTED DIGITAL ID?

A digital ID is the network- or internet equivalent of a person's real identity, which is used for identification when accessing a service or performing a transaction on a computer, cell phone or other personal device. It includes a collection of electronically captured and stored identity attributes that distinguish a person within a given context.

There are a variety of attributes that can be used, such as:

Biographic data
(i.e. name, age, gender, address)

Biometric data
(i.e. fingerprints, iris scans, hand prints)

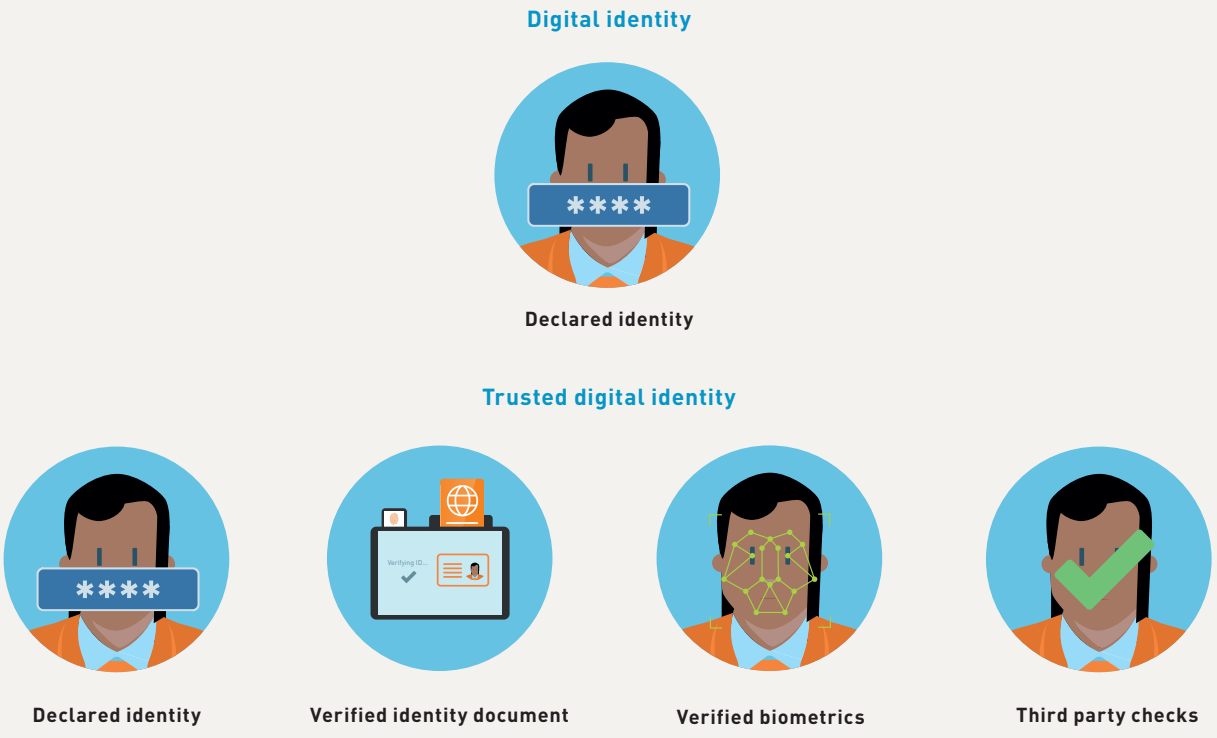
An object the person has
(i.e. mobile phone, specific token)

A basic digital ID can be as simple as a username and password combination. Digital IDs increase in security with the amount of attributes added.

Trusted digital IDs are created when the information provided has been verified, or checked for authenticity.

[4] http://www.cfca.org/fraudlosssurvey

DIGITAL IDENTITY VS. TRUSTED DIGITAL IDENTITY



1.3 A shift towards trusted digital IDs

The average person already owns multiple digital identities, which are used to access a range of different services. In many forums, such as for media and entertainment, these identities don't necessarily need to reflect the actual identity of the person — a pseudonym may be used. Yet as more and more important services move online, such as paying taxes or voting in elections, it's critical that digital identities reflect real, verifiable identities.

Companies and governmental organizations across the globe are increasingly adopting trusted digital IDs as a secure way to verify their employees' / customers' / citizens' identities. In contrast to a simple username and password combination for instance, a trusted digital ID is created with verified attributes (like verified ID documents or biometrics), thus providing a certifiable link between an individual and their digital identity. These attributes may also include cross-referenced verification with third parties like government databases, credit card numbers, etc.

Not only do MNOs get to make this shift, they potentially have an important role to play in helping other sectors make the change as well.

2. How can trusted digital IDs change the game for MNOs?

2.1 Streamlined operations

Trusted digital IDs make it possible for MNOs to simplify and digitalize their workflows — reducing the manual entry, photocopying, or paperwork that can take several days to process. Not only does this slim operating costs, it also benefits customers by slashing the time it takes to subscribe and by making it possible to activate various services instantaneously.

2.2 More consistent customer databases

In creating a digital ID, personal information is extracted and automatically populated in the customer CRM. This creates efficiencies on multiple fronts. Customer representatives don't need to waste time manually entering data and errors are reduced. The MNO's database becomes more consistent and information-rich, which presents opportunities for marketing segmentation and data monetization.

Digital IDs open up greater possibilities for remote customer onboarding, so customers can subscribe on their own time and in the comfort of their own home.

ENROLLMENT
UP TO 5x
FASTER

2.3 Protection from fraud

Put simply: fraud is costing MNOs dearly each year. And it's on the rise. In the face of such heavy financial losses, as well as damage to brand reputation, getting subscription fraud under control is a key priority for MNOs.

Trusted digital IDs effectively address the problem of fake identities both at physical points of sale and in online channels. If the prospective customer's identity can't be authenticated, they can't proceed. Further, when an existing customer seeks to, for example, acquire another phone and subscription, the use of their unique digital ID confirms that the customer is not an imposter. Sales teams no longer need to guess at intent or gauge identity documents visually — digital IDs introduce secure verification that dramatically reduce the incidence of fraud.

Subscription fraud cost MNOs

$5.07

billion in 2016

2.4 Compliance with regulations

Governments are pursuing stronger measures to prevent terrorism, money laundering, and other crimes that involve assumed identities. The legislation crafted in response calls for high security ID verification, and the requirements that MNOs must meet continue to change at a rapid pace. For example, pre-paid SIM card registration is already mandatory in 90+ countries, according to the GSMA.

Additionally, seeing as MNOs are increasingly offering new financial services, they are required to comply with anti-money laundering (AML) and anti-terrorism (CFT) legislation. They are also subject to meet Know Your Customer (KYC) ID verification procedures.

Trusted digital IDs provide MNOs with a straightforward way to comply with such regulations, without passing the burden to their customers (enduring a waiting period, filling out extensive forms, etc).

2.5 Providing value through secure access to services

Trusted digital IDs can serve a purpose beyond fraud protection and effective systematization — they represent an opportunity for MNOs to create new value for their customers. This value centers around the pressing need to accelerate digital security in tandem with convenience. A trusted digital ID can act as a reliable gateway for customers to access multiple security-sensitive services, including mobile operator services, financial services, and eGov services.

Mobile operator services: prepaid and postpaid, mobile money, device swap, IoT services

Financial services: Banking, eCommerce, online bill pay, money transfers

eGov services: eVoting, tax payment, eSocial services, Insurance, eHealth, Social Security

The creation of new value starts with the MNO providing their customers with a quicker, more seamless way to activate, log into, and engage with their services. A digital ID makes it simple and convenient for customers to sign up to additional services, making it easier for the MNO to cross and upsell.

The value can then spread outwards. Not every sector, and certainly not every company, will be creating their own bespoke digital ID solution — they will be looking for partners. MNOs are well positioned to take advantage of this fact. In serving as a digital ID enabler, MNOs can explore new business models and tap into a new, stable source of revenue from third parties.

3. How do trusted digital IDs work in practice?

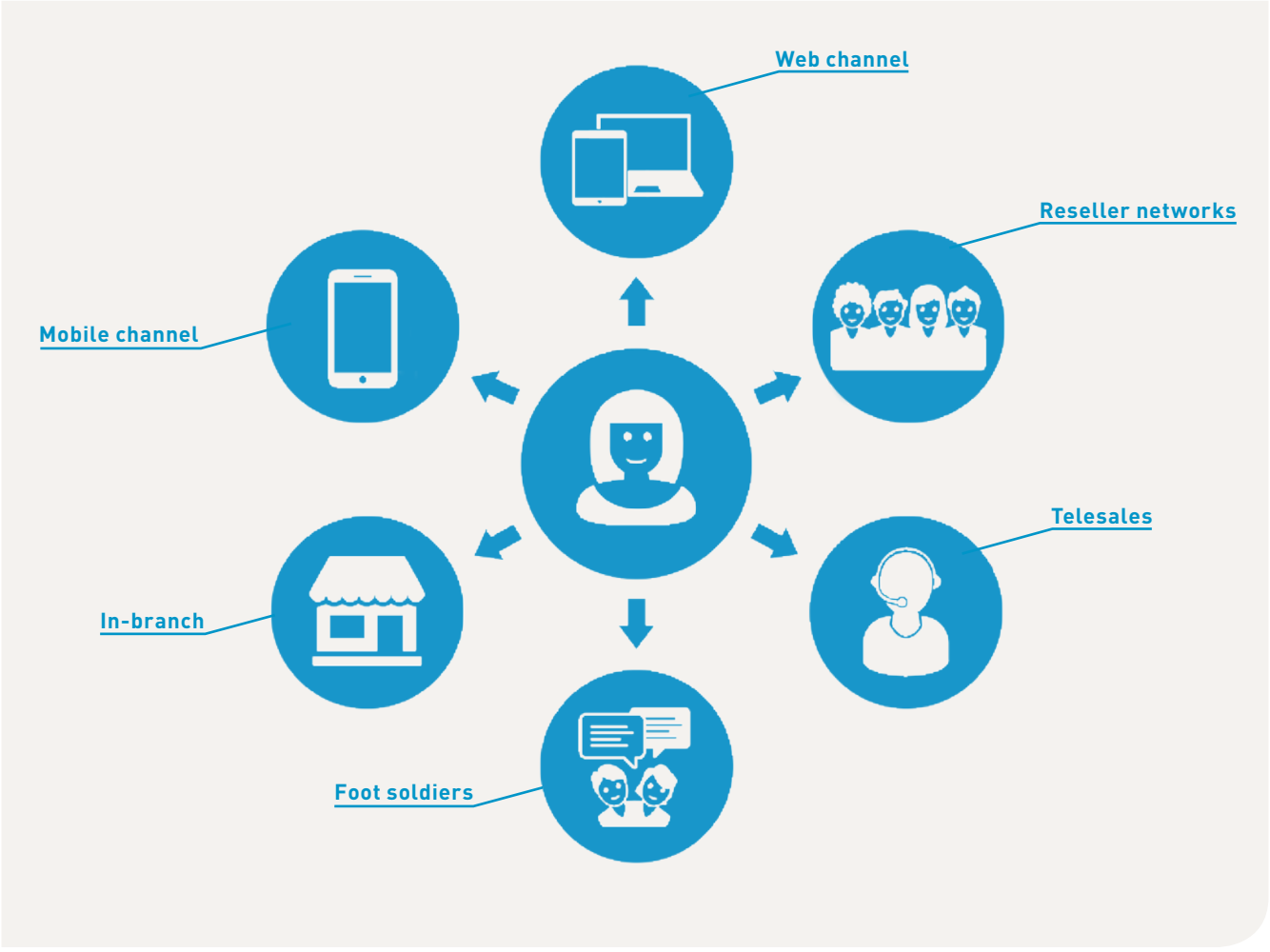
3.1 Omni-channel as a must

MNOs onboard customers in a diverse array of scenarios. Subscriptions and services can be conducted by foot soldiers, telesales representatives, or in-branch customer representatives — or it can take place online without supervision.

Many digital ID solutions only support remote implementations, excluding other channels that are fundamental to the MNO's customer acquisition, such as their point of sales, reseller networks and other channels.

Yet providing a seamless omni-channel experience is of core importance to MNOs, as customers have next to no tolerance for a heavy process.

Whether customer onboarding takes place in person or remotely, the security and accuracy of the trusted digital ID creation process needs to remain consistent. And the customer should enjoy the same or similar journey regardless of the channel.



4. Step-by-step creation of a digital ID

A trusted digital ID is created by conducting three general steps: capture, verify, digitalize. The details of each step may vary according to the extent of the information the MNO wishes to capture and the regulations they are subject to, for example, around personal data privacy.

4.1 Capture (ID documents and biometrics)

Even though the onboarding scenarios — depending on the channel used by the customer — may be different, the process of capturing identity attributes should be carried out in a similar way. The hardware needed can range from a mobile phone to specialized high end scanners. The choice of hardware has implications for the level of quality, the types of verification that can be conducted and ultimately for the accuracy of the results.

DEVICES TO CAPTURE ID ATTRIBUTES

In-branch, attended

Scanner
Smartphone
Tablet

Email
Web Service
Biometric tablets

UV, IR Readers
Biometric readers

Remote, unattended

Web Service
Mobile

Tablet
Kiosk

To begin, the subscriber's information is captured from an identity document (passport, driver's license, or national ID, resident permits etc.). In this process, information such as name and birthdate can be extracted through image analytics (optical character recognition). This technology helps ensure that accurate and detailed customer information is entered in the CRM. If required, other information, such as a subscriber's postal address on a utility bill, can be extracted to complete the customer profile or enable further verification.

A biometric capture device (such as a mobile phone, web camera, tablet or kiosk or specialized fingerprint scanner) is used to capture the user's biometric information. Types of biometrics that can be collected include information from the face, fingerprint, handprint or iris.

4.2 Verify

Identity verification aims to verify the authenticity of the end user ID document and validates if the person is who they claim to be. This may require a combination of solutions, depending on the level of assurance needed.

a. Verify ID

After it has been captured, the system verifies the authenticity of an ID document with dedicated software. Different methods can be used to check different features of the provided identity document against an ID database.

In this phase, the personal information of the card holder can also be extracted to automatically populate the fields in registration forms, the CRM, etc. This results in a faster and simpler onboarding process for customers, as well as time savings and greater data accuracy for MNOs.

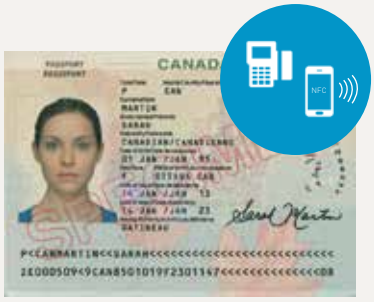
There are three different levels of document verification:

WHITE LIGHT

- Verifies elements of most ID documents under white light
- Mainly used remotely/online
- Often uses consumer devices (smartphone, webcam...)

INVISIBLE LIGHT

- Verifies security elements of most ID documents under white, ultra-violet and infrared light
- Mainly used in-branch
- Uses high end scanners

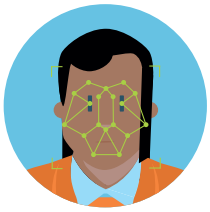


ELECTRONIC

- Verifies electronic information on the chip of contact or contactless documents
- Can be used in-branch or remotely
- Uses NFC devices and special software

b. Verify biometrics

Biometric technology is used to verify if the person presenting the document is who they claim to be. It also presents an opportunity for later use as simple and modern way to access services that require identification — and in particular when verification needs to be conducted remotely. The two technologies most commonly used are facial recognition and fingerprint scans.



Facial recognition technology analyzes the user's face, using algorithms that determine the relative size, position and/or shape of facial features like eyes, nose, cheekbones and jaw. These features are then used to compare to another image (e.g. the ID picture) to determine if these features match. Furthermore, liveness detection through video, eye blinking or other techniques is employed to assure the presence of a real person, and not a photograph or 3D model.

Fingerprint authentication is conducted by analyzing several features of the friction ridges at the tip of the finger and identifying the unique print pattern. This print pattern is then compared to the print associated with the owner of the ID card. This can be done locally by comparing the fingerprint with data on the chip or remotely with a third party database.

4.3 Digitalize ID

After a match is established between the biometric data and the identity document, a digital ID may be created. Going forward, the user's digital ID can be used to easily log in to the service. The user can gain access by simply presenting the requested biometric attribute, such as their fingerprint. This function enables users to more freely access the MNO's services by lowering the authentication friction they would otherwise encounter. The MNO can also provide this convenient verification method to third party services that require the verified identity of their users.

5. Our core expertise: Digital identity

At Gemalto, we work with some of the world's biggest businesses and governments, providing flexible technological solutions that help them meet the need for greater security and convenience simultaneously.
Our technology serves as the basis for 150+ eGovernment programs and our biometric ePassport technology is used by 80+ countries, with over 200 biometric deployments and counting. Digital identity remains at the core of our expertise, as we help hundreds of our partners implement advanced authentication and security solutions.

150+
eGovernment programs

We have served as a trusted partner to MNOs since the beginning of our company. We provide SIM cards and managed services to more than 700 million subscribers, as well as supply MNOs with state-of-the-art products and services, compliant with the latest GSMA specifications. Our products comply with most demanding international standards, such as those demanded by the U.S. Department of Commerce, the FBI, Interpol and the American National Standards Institute.

By merging our expertise in digital identity with our long-standing partnerships with MNOs, we seek to help MNOs provide the best possible experience to billions of people.

700
million
subscribers

6. Gemalto: A partner in digital transformations

The evolution of technology is following an exponential curve, with each new generation of technology arriving quicker than the last. In this rapidly changing and highly customer-centric environment, businesses constantly need to enhance their offers and keep up with the latest trends.

This is where Gemalto comes in. Our central mission is to stay several steps ahead of technological developments. We serve as a partner to businesses looking to make important leaps, offering both the technology and integration guidance. This enables our partners to continue to focus on their core competencies, while diversifying and strengthening their offer.

Rather than simply being a security imperative, digital IDs constitute a great monetization opportunity and an exciting future for MNOs. As with our other solutions for MNOs, ranging from IoT to connectivity to SIM and secure elements, we are ready with easily deployable digital ID technology.

For more information about our portfolio of trusted digital ID technology, please see our brochure:
Gemalto's Trusted Digital ID Technology for Mobile Network Operators.

ABOUT GEMALTO

Gemalto (Euronext NL0000400653 GTO) is the global leader in digital security, with 2017 annual revenues of €3 billion and customers in over 180 countries. We bring trust to an increasingly connected world.

From secure software to biometrics and encryption, our technologies and services enable businesses and governments to authenticate identities and protect data so they stay safe and enable services in personal devices, connected objects, the cloud and in between.

Gemalto's solutions are at the heart of modern life, from payment to enterprise security and the internet of things. We authenticate people, transactions and objects, encrypt data and create value for software – enabling our clients to deliver secure digital services for billions of individuals and things.

Our 15,000 employees operate out of 114 offices, 40 personalization and data centers, and 35 research and software development centers located in 47 countries.

For more information visit:
https://www.gemalto.com/mobile
https://www.gemalto.com/mobile/id-security

GEMALTO.COM/MOBILE

THALES

gemalto
a Thales company