IDENTITY & SECURITY

# DIGITAL IDENTITY

SAFRAN

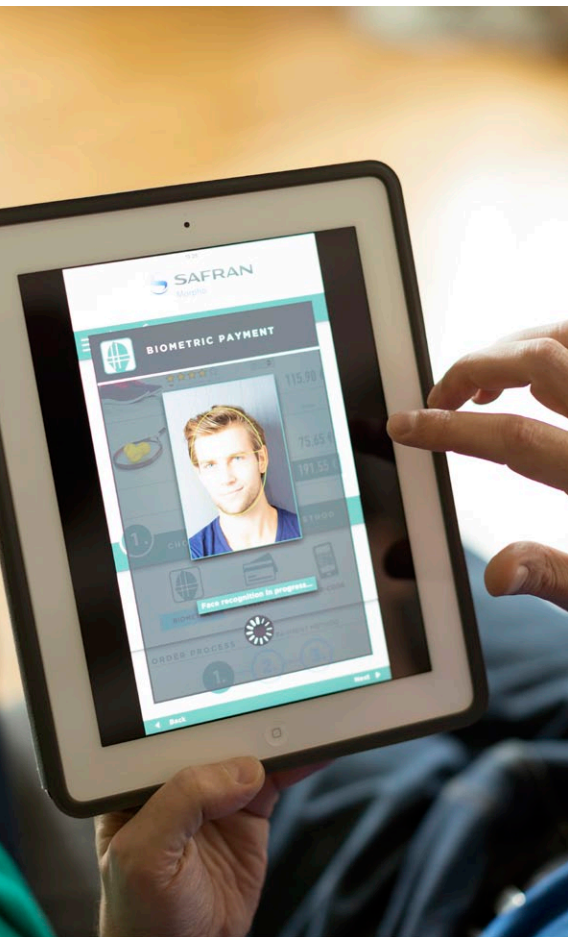
## IDENTITY

The set of characteristics by which a person is definitively recognizable or known (date and place of birth, full name, etc.).

# THE THREE CHALLENGES FOR DIGITAL IDENTITY

## DIGITAL IDENTITY

Information about individuals that enables them to access online services.




**Digital identity is an emerging but rapidly expanding market, spurred on by the digitization of world in which we live. To support this transformation, businesses and governments worldwide are stepping up their efforts to adapt services which earn the trust of users, fight fraud and simplify access to online services.**

### #fraud

Tackling the problem of identity theft in the digital world is an increasingly complex challenge. Many people do not even ensure the most basic protection of their digital identities, often relying on weak passwords to store private information or data. The proliferation of different digital identities online has made it even harder to protect them. Unaware of the risks and potential consequences, users tend to forego the essentials of password management, such as the importance of changing them regularly, making them complex and never writing them down! These inadequacies in data protection, compounded by often poorly protected storage infrastructures, make our digital identities easy and open targets for cyberattacks and large scale data theft.

### #convenience

Creating safe digital identities for the masses means first educating users about the importance of identity protection but also about developing solutions which support the need for convenience in today's connected world. Both the public and private sectors are progressively adopting biometrics as one solution, based on fingerprint, iris, and facial recognition. Contrary to complex passwords, biometric systems combine simplicity of use with a high level of security. To facilitate deployment of these solutions, governments are introducing regulation to promote best practices in electronic identification and trust services, with the aim to build trust in the digital world.

### #trust

General public awareness about online security may vary from one country to the next, but there is a strong trend in digital economies to educate and propose solutions to better protect consumers and their data. In addition to the geographical location of data storage facilities, users are also concerned about the solutions chosen by service providers for storing and encrypting their personal information. In a similar vein, online service providers need to be able to trust the identity of their customers. In the banking sector in particular, the level of trust has a direct impact on the type of services made available to consumers.

02

# FROM PHYSICAL TO DIGITAL IDENTITIES

**Passports, ID cards, driver's licenses – these and other official documents enable us to prove our identity in the physical world, whether it's for an administrative procedure or a transaction. To obtain these documents, you need to present an official record of who you are, such as your birth certificate. Obtaining these documents in different countries can be more or less complex, depending on local legislation.**

### #today

With the internet and smartphones now a ubiquitous part of everyday life, we are constantly asked to confirm our identity in the digital world. Whether we want to send an email, make a purchase or bank transaction, or just share our latest holiday photos, each service or application requires a specific user ID and password. But these many different accounts do not all offer the same level of security when it comes to protecting our digital identity.

### #tomorrow

Commercial providers such as Facebook and Google already allow users to access different services using a single sign-on (SSO). Meanwhile, several countries, including the UK, India, the Netherlands and Albania, have introduced pioneering government verification systems, allowing citizens to access certain operations requiring a high level of security online, such as passport applications, tax returns, loan applications, etc. These benchmark initiatives are just a few illustrations of the rapid expansion in digital trust services.

2.8 At the end of 2015, Safran had produced over BILLION ID DOCUMENTS worldwide


## Convergence of the physical and digital worlds

In 2015,
Facebook registered
**1.5** BILLION MONTHLY ACTIVE USERS[3]

**1.4** BILLION SMARTPHONES
were sold worldwide in 2015[4]

| | |
|---|---|
| 1975 | Safran delivers its first Automated Fingerprint Identification System (AFIS) to the FBI |
| 1986 | First smart card[1] |
| 1990 | Emergence of internet |
| 1995 | Introduction of the first online banking services in the US |
| 1998 | World's first electronic passport issued by Malaysia[2] |
| 2004 | Launch of Gmail and Facebook |
| 2006 | Safran delivers the first ICAO-compliant ePassport to the Netherlands (in use since 2005) |
| 2007 | Apple introduces the iPhone |
| 2013 | Launch of the iPhone 5s featuring a biometric fingerprint sensor |
| 2014 | Safran launches MorphoWave™, the first biometric solution featuring high-speed contactless fingerprint matching |
| 2015 | Safran rolls out the first mobile driver's license in the US |
| 2016 | Safran launches its selfie-check authentication solution for smartphones |

1_ Source: http://www.cartes-bancaires.com/spip.php?rubrique32
2_ https://hal.archives-ouvertes.fr/hal-01108892/document
3_ http://www.journaldunet.com/ebusiness/le-net/1125265-nombre-d-utilisateurs-de-facebook-dans-le-monde/
4_http://www.lefigaro.fr/secteur/high-tech/2016/01/28/32001-20160128ARTFIG00315-la-croissance-des-ventes-de-smartphones-a-ralenti-fin-2015.php

**What are the benefits of having a digital identity?**

Having a secure digital identity enables citizens to safely take advantage of the growing number of digital services provided by governments, banks and retailers from the comfort of their home, or on the move. Unlike their brick & mortar equivalents, online stores and agencies are available 24/7. As well as reducing costs for service providers and retailers, digital services translate into less time, hassle and cost for consumers.

03

# SAFRAN IDENTITY & SECURITY, A GLOBAL LEADER IN TRUSTED DIGITAL IDENTITY SOLUTIONS

**Safran has leveraged its extensive identity management and biometrics expertise to carve out a strong position in the digital identity market. In addition to our legacy markets, this unique expertise is attracting interest from new markets.**

### Safran's credentials in digital identity

Safran is a global leader in biometric identity solutions, providing a wide range of secure documents for more than 50 countries worldwide: biometric passports, identity cards, driver's licenses, etc. Safran also boasts extensive experience in ID registration and verification and large ID database management. These solutions are assessed and certified on a regular basis by independent authorities, guaranteeing Safran customers the highest levels of performance and security. At the same time, Safran's expertise in data privacy issues and protection enables us to develop "privacy by design" solutions that are fully compliant with local regulations.

### Leading the way in trusted mobile digital identity

Thanks to a unique blend of expertise in identity management, SIM cards and biometrics, Safran is the only provider to cover the entire mobile digital identity value chain – from identity registration, creation and authentication through to verification. Safran has leveraged this know-how on a wide range of programs and projects, including the Mobile Driver's License (mDL) application, the first ever state-issued digital driver's license in the United States, in Iowa. In addition, Safran supports its customers in their digital transformation strategy, helping them to develop new solutions, such as the eKYC (**e**lectronic **K**now **Y**our **C**ustomer) application, enabling new customers to securely open a bank account directly from their smartphone. We are also partnering with various international organizations to advance global digital identity standards and best practices. This includes work with the GSMA and FIDO alliance for secure and universal login solutions, for example Mobile Connect, enabling users to access different websites and applications without needing to remember dozens of passwords and usernames. With these types of applications users are authenticated through their mobile devices, and can easily log-in to any online service.

### Expanding market opportunities

The rapid growth of the sharing economy, illustrated by such commercial successes as AirBnB, Uber and eBay, to name a few, has spurred the need for companies to "know their customers and suppliers". Safran's trusted digital identity solutions address this need. Ultimately, any service that requires identity verification, such as online voting, eHealthcare, IoT and social media, can benefit from Safran solutions.

## TRUSTED DIGITAL IDENTITY

A person's digital identity is established on the basis of several, usually state-issued proofs of identity, whose authenticity must be verified. The stronger the proof, the more secure the identity is.

**450,000**

FALSE PASSPORTS

are currently in circulation in Europe, according to Interpol[6]

### Identity fraud: banks lead the battle

When it comes to digital identity, the stakes are particularly high for banks, who must counter three types of fraud:

- Identity theft: when someone tries to pass themselves off as a bank customer or as a new customer wanting to open an account.
- Insider fraud: to avoid insider theft and identity fraud.
- Customer fraud: when a customer rejects a transaction that they actually conducted. To prevent this type of fraud, banks must implement measures to ensure that transactions cannot be repudiated.

### How well do you know your customers?

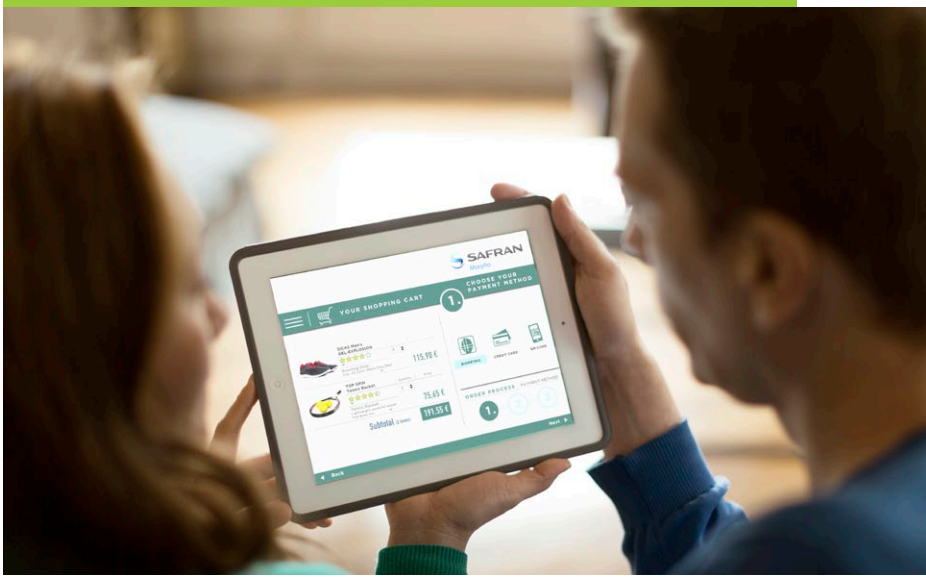
KYC ("know your customer") is a global anti-money laundering initiative launched in the 1990s, which recommends that banks ask potential new customers to provide several different forms of identity when opening a new account. To offset the extra hassle that this entails for customers – and give banks greater flexibility to offer products that match consumer preferences – banks have defined "levels of assurance", depending on how well they know their customer. The four levels of assurance range from basic to high value-added services, allowing customers to, for example:

**Level 1** Make physical payments

**Level 2** Access their accounts and make small payments online

**Level 3** Transfer money to third parties

**Level 4** Take out a mortgage online




5_ 2014 Annual Report by the Observatoire de la sécurité des cartes de paiement
6_ http://www.lefigaro.fr/actualitefrance/2015/12/22/01016-20151222ARTFIG00224-presde-120-000-personnes-sousdouble-identite-en-france.php

04

# THE THREE CORNERSTONES OF DIGITAL TRUST

**Protecting people's digital identities demands expertise across the entire trust value chain – from registration to deployment of online services. As a global leader in trusted digital identity solutions, Safran is one of the few companies to provide solutions addressing the full spectrum of requirements.**

## 1 registration

The first step is verifying the physical identity of an individual. This can be done online or face-to-face at a government agency. Depending on the case, a variety of documents are required (passport, driver's license, proof of residency, etc.,), together with personal details (e.g., full name, email address, etc.), all of which is then checked. If access to the person's digital identity involves biometric technology, their biometric data is recorded at this stage and then securely stored in accordance with national legislation. The data is then "deduplicated" to verify that the same person has not already previously registered.

***Aadhaar, the unique digital identity system in India***

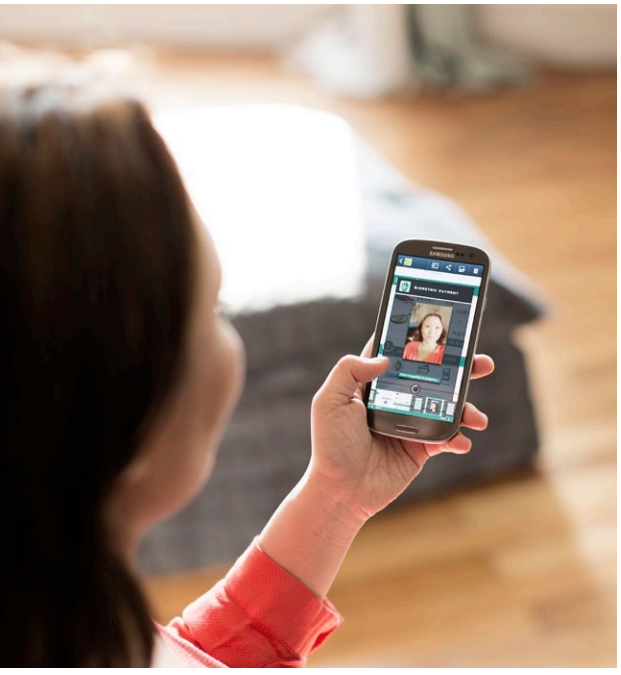
*Launched by the Unique Identification Authority of India (UIDAI) in 2009, India's Aadhaar program aims to provide all residents with a Unique Identity (UID) number, based on their biometric data. Safran supplied the technology for the system, which reached the unprecedented milestone of 1 billion digital identities in April 2016.*

## DIGITAL SIGNATURE

A digital signature guarantees that the user is actually the person signing the document. It also guarantees the authenticity and integrity of the document's content, meaning that it cannot be modified or repudiated. It is proof that the signatories consent to the method used. To preserve their confidentiality, integrity and long-term probative value, digitally signed documents can be stored in a digital vault. Digital signatures are used extensively in the banking, legal and real estate professions, as well as in industry, for example on maintenance and purchase orders.

**60**
MILLION DIGITAL SIGNATURES

guaranteed by Safran every year



## 2 authentication

Once a trusted digital identity has been generated, it needs a secure environment to be used. Drawing on our expertise in smart cards and biometrics, Safran has developed a complete and fully flexible range of secure authentication solutions for a multiple applications and use cases: One Time Password authentication, smart cards, smartphones, fingerprint scanners, video-capture facial recognition systems, etc. The choice of technology depends on the level of security needed. Sending an email, for example, is much less critical than when applying for a loan!

***Idensys in the Netherlands***

*Safran is leveraging its expertise to help develop a digital identity system in the Netherlands based on users performing selfie-based authentication ("selfie check") with their smartphones.*

## 3 applications

Safran offers a broad range of solutions enabling organizations to use trusted digital identities for other applications besides online accounts. Our portfolio includes secure transaction and data solutions based on digital signatures and archiving to ensure document integrity and authenticity over time.

***Morpho Cloudcard+***

*Morpho Cloudcard+ enables secure operations to be performed on mobile devices, through strong authentication, transaction authorization and the creation of digital signatures. The secure element is both embedded in the mobile device and in the cloud and can only be accessed through biometric verification or by entering a PIN. Cloudcard+ strikes the perfect balance needed for authentication in the mobile world: compatibility with all types of mobile devices, is simple to use, and provides greater security compared to SMS authentication solutions.*

05

# BIOMETRICS AND DIGITAL IDENTITY

**Biometrics refers to the use of the unique physical characteristics that identify an individual. Based on fingerprint, iris and facial recognition, biometrics is the most widely used and most accurate technique for identifying individuals. So how do biometrics and digital identity fit together?**

## Biometric technology combines convenience with security

In digital environments, checking the identity of a user is not an easy process, since it requires users to prove that they are who they say they are. There are many ways to do this, but biometric technology has the distinct advantage in that it cannot be transferred, forgotten or stolen, unlike a PIN or a card. As a result, biometric identification systems present a minimal risk of fraud. Another key benefit is that they are very convenient to use (requiring just a photograph of yourself - a selfie - or fingerprint scan), especially for mobile applications.

## Biometrics – a strong authentication factor

Strong authentication establishes trust in a user's identity, giving organizations the peace of mind that users are not fraudsters. The most effective solution for ensuring this high level of trust is to use two-factor authentication, combining several possible credentials: what the user has (smartphone or chip card), what they know (PIN or password), or what they are (biometric data). Based on two-factor authentication (smart card + password), EMV, the global standard for credit and debit payment cards based on chip card technology, is the most commonly used authentication solution, protecting close to 1.2 billion chip cards worldwide. Other equally effective strong authentication solutions are also available, such as integrating biometric technology into smartphones to reduce the risk of transaction repudiation as well as PIN theft or unauthorized use.

### Using your smartphone as your driver's license

As the primary proof of ID in the US, the driver's license shifted into the digital realm in 2015. Developed by MorphoTrust USA, the Mobile Driver's License (mDL) application lets drivers carry a digital version of their license on their smartphone and present it on the screen if requested. The mDL software includes security features that are linked and layered in the digital image on the screen. These features not only ensure a high level of security, they also enable the mDL to be quickly and reliably authenticated when presented for identification purposes and to protect against fraudulent reproduction. In addition to PIN and fingerprint-based security features already built into phones used in the pilot, the mDL app can be secured using SafranTrust facial recognition unlock technologies which require the user to take a selfie and use a personalized PIN.


### "Selfie checks" for better mobile security

To combat identity fraud and provide extra security for online transactions, Safran has developed a biometric authentication solution that is easy to deploy for service providers and ensures additional protection for consumers. Based on facial-recognition, Safran's Face Authenticatication solution or “selfie check”, offers a viable alternative to traditional user verification methods, such as a PIN or password, on mobile devices. The application's "liveness detection" feature requires that users move their heads slightly to prevent  a photo being used in an attempt to spoof the system. Delivering an universal form of authentication, superior security and ease of use, Safran's innovative biometric authentication software is well poised in the evolution to replace passwords. Safran’s "selfie check" solution is certified by FIDO* for compliance with the Alliance's specifications and interoperability with other FIDO-compliant products and services.

*The FIDO (Fast IDentity Online) Alliance was formed in July 2012 to address the lack of interoperability among strong authentication technologies, and remedy the problems users face with creating and remembering multiple usernames and passwords.

06

# MARKETS EMBRACING DIGITAL IDENTITY

## 1_ Governments

- **Objective:** Simplify and secure access to online government services by providing a trusted digital identity for all citizens, facilitating everyday procedures easier as well as reducing costs.

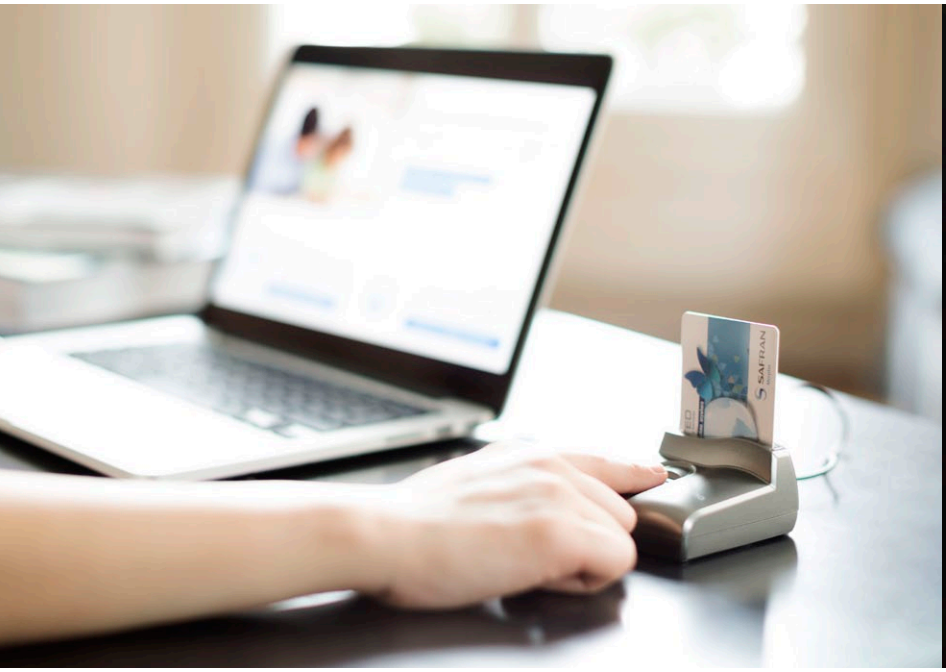
### Safran solutions

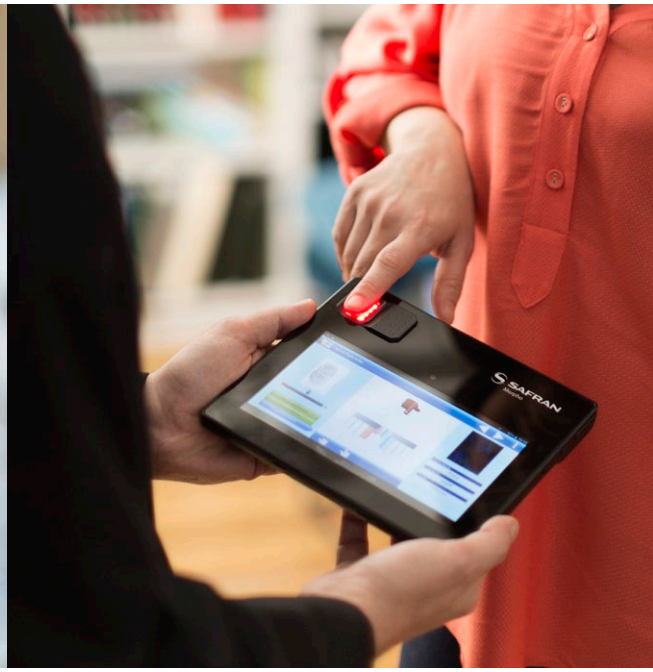
- **Physical identity registration** for an entire population, either via government agencies or teams in the field. In India, this solution was adopted by the government as part of its Aadhaar program.
- **Online identity registration.** The UK government selected this solution for its Identity Assurance Programme (IDAP, known publicly as Gov.UK Verify): users are able to choose from several certified companies, including Safran, to verify their identity before using a public service online.
- **Online authentication platforms** for countries which already use electronic documents and digital identity systems. In Albania, Safran developed the eAleat secure identity services platform, which citizens can access using their national e-ID card, also produced by Safran.

The Aadhaar project has helped the Indian government to fight fraud and corruption and save

1 BILLION DOLLARS A YEAR[8]

8 World Bank and http://www.planetbiometrics.com/article-details/i/4011/desc/indias-biometric-idshould-beemulated-world-bank/





A digital transaction costs

14 TIMES LESS THAN

a physical transaction[9]

Banco Itaú, a Safran customer, has registered biometric data for

30 MILLION CUSTOMERS

Biometric technology has helped Banco Itaú

REDUCE FRAUD BY 68%[10]

1/3 OF TRANSACTIONS USE BIOMETRICS, REDUCING TRANSACTION TIME BY MORE THAN 30%[11]

## 2_ Financial institutions

**Objective:** Reduce the cost of transactions and financial operations and at the same time offer differentiated products and services. The challenge lies in providing secure e-banking services that combine customer convenience with protection against identity theft.

### Safran solutions

- **Secure online bank transactions** thanks to multi-factor authentication (e.g., smartphone, biometrics, chip card), coupled with identity management solutions and trust services.
- **Biometric systems** to maximize banks' trust in user identity. In Brazil, Banco Itaú selected Safran to equip its ATMs with biometric sensors. Instead of using a chip card, customers simply scan their fingerprint to withdraw cash. As well as reducing the risk of card fraud, the system is easy to use.
- **Digital contracts for all sales channels** (bank branch, website and mobile, ATMs, call centers, etc.): end-to-end digital process for all contracts and account documents.

9_ Source: Forrester Research
10_Source : Executivos Financeiros
11_Source: Banco Itau

## 3_ Telecommunications

- **Objective:** Operators want to comply with new customer registration regulations, and find new growth opportunities by expanding mobile services. Using new skills and technologies with existing smartphones, they can deliver greater customer security and convenience.

## Safran solutions

- **Secure network connection** using SIM cards, which contain a unique "subscriber identity module" for each of the billions of mobile users worldwide. Safran is helping to define specifications for the standardization of next-generation SIM card technologies that provide remote management capability, and delivering GSMA compliant eSIMs and remote SIM provisioning.
- **User authentication for mobile devices.** Embedded Secure Elements (eSE) are tamper-proof chips, that can be used to secure ID credentials. Secure application management (for mobile payment, transport and eTicketing) can be integrated into eSE or NFC-enabled SIM cards. Our Mobile Connect solution delivers convenient and secure alternative to usernames and passwords, and includes unique biometric options.
- **Biometric authentication for mobile devices.** Our secure selfie check facial recognition technology is available for integration into mobile devices and mobile apps.
- **Storage of identity credentials in mobile devices:** user identity information (such as biometric data) is securely stored in the device's secure elements.
- **Quick, convenient and secure sign-up for mobile contracts, whether online or in person.** Depending on national legislation, government databases or identity documents can be accessed to enable quick and easy customer registration, take out mobile contracts or sign up for new digital services. In India, new customers can now present their Aadhaar eID number and benefit from almost immediate access to the operator's services.

Safran,
WORLD'S
2nd
LARGEST
supplier of SIM cards

MORE INFO

To discover more about our solutions please email **info@safrangroup.com**


SAMSUNG
Your Bank
MOBILE PAYMENT

# POWERED BY TRUST

**SAFRAN IDENTITY & SECURITY**
11, boulevard Gallieni - 92130 Issy-les-Moulineaux - FRANCE
Phone: +33 (0)1 58 11 25 00 - www.safran-identity-security.com
Société anonyme au capital de 159.876.075 euros - 440 305 282 RCS Nanterre

SAFRAN

Photos : Shutterstock - SAFRAN Morpho - 07/16 - Création : FK Agency