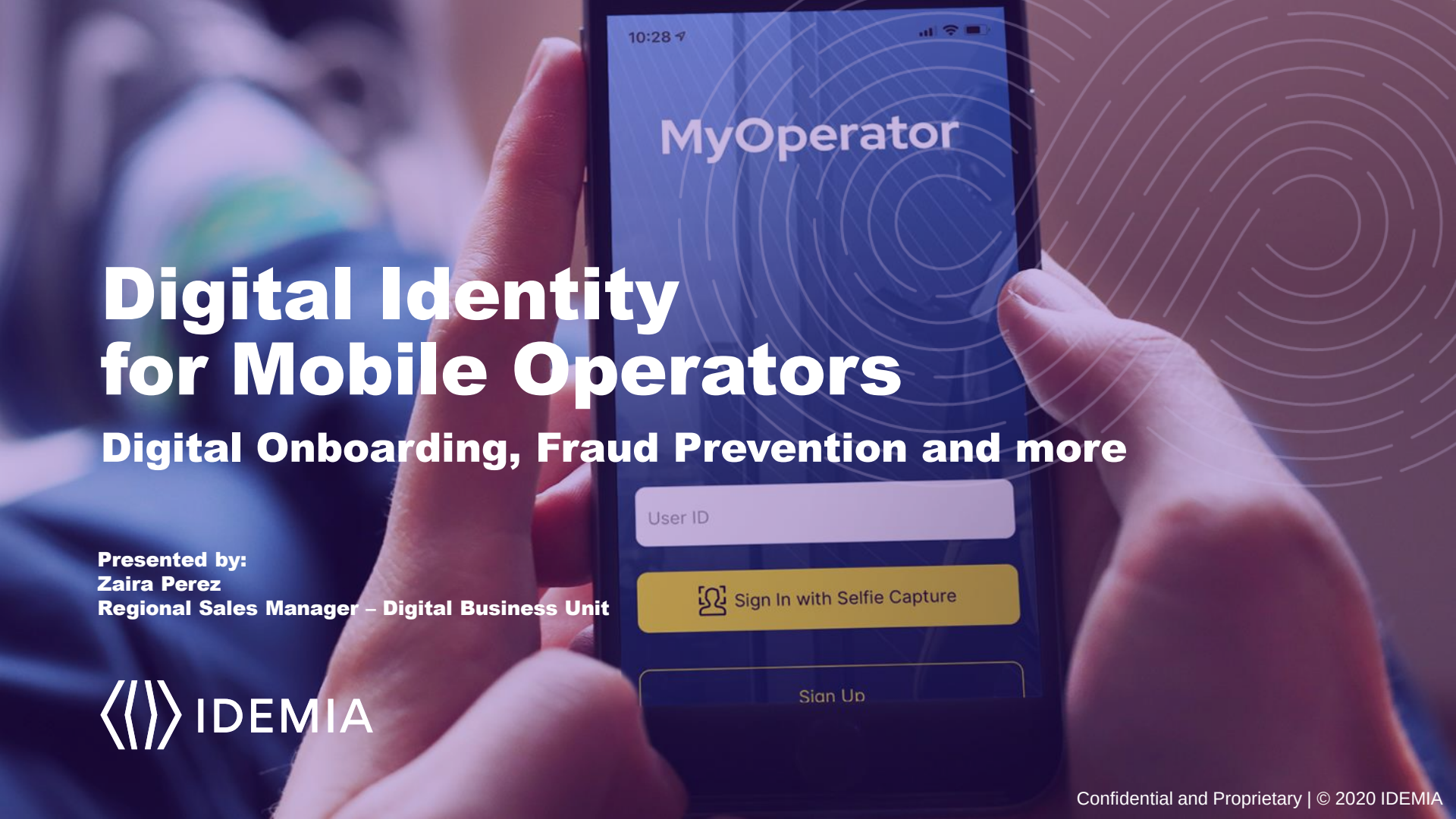


Digital Identity for Mobile Operators

Digital Onboarding, Fraud Prevention and more

Presented by:
Zaira Perez
Regional Sales Manager – Digital Business Unit

IDEMIA

Agenda

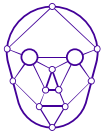
1. Digital Identity for Mobile Operators
2. Fraud Prevention
3. Digital Onboarding
4. eKYC + eSIM
5. Mobile Operators as Identity Providers
6. Demos

Digital Identity for Mobile Operators

Mobile operators need to be confident in the claimed identity of customers, especially when it comes to digital onboarding, fraud prevention, and authentication use cases.

Mobile digital identity will generate over **$7 billion** for mobile operators in 2024, a 800% growth rate from 2019.

Source: Juniper Research



Customer Onboarding

- Digital onboarding
- SIM/eSIM registration
- AML/KYC compliance

Fraud Prevention

- Prevent device fraud and loss
- Enhance internal security
- Prevent SIM swap fraud and account takeover (ATO)
- Prevent Mobile Financial services fraud

eSIM + eKYC

- Complete onboarding & activation journey for eSIM subscribers
- Anywhere, anytime in a secure, frictionless and seamless
- Reduced customer acquisition cost and fraud

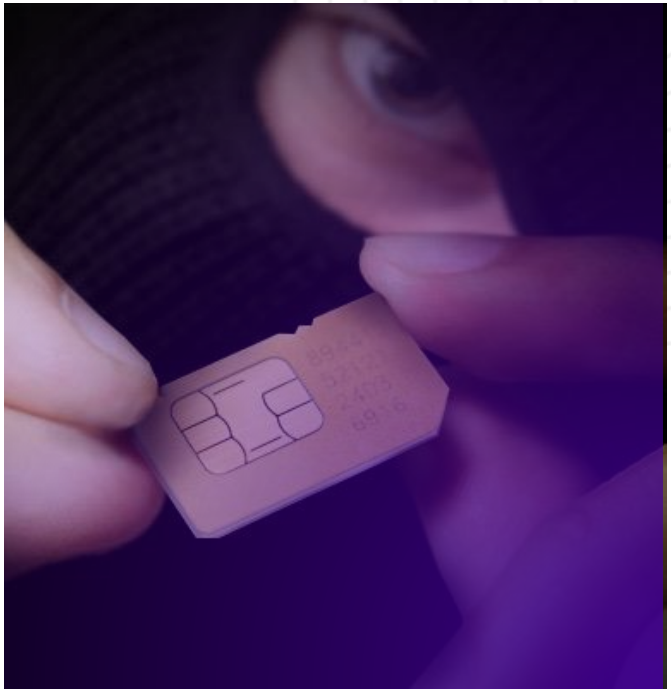
Identity Provider (IdP)

- With a database of secure, verified identities, MOs are in a strong position to become identity providers (IdP)
- Monetize identity attribute already captured through digital enrollment processes
- Increase brand awareness (ie. Sign In with MYID)

IDEMIA

Mobile Operators Are No Strangers to Fraud

Total fraud losses for MNOs is
$29 billion
(but is likely higher because not all fraud is reported)



Identity theft
occurs when personal information that can be used to identify someone is stolen

SIM registration
and account opening is the most common type of fraud for MNOs

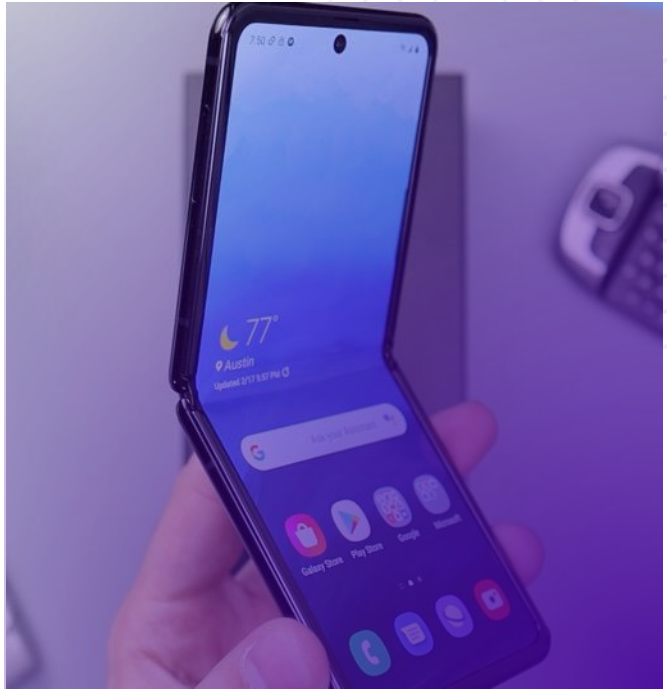
Data breaches have exposed
16 billion records since 2019

Sources: CFCA 2017 Survey, Neural Technologies, Javelin Research

IDEMIA

Today the Risks are Higher

In postpaid markets, both **subscription & device** are potential losses for MNOs



Remote onboarding with unsecured channels creates new opportunities for fraudsters

Phone prices are increasing, costing an average of $528 in the United States

Amplified by **COVID-19** and the push towards remote onboarding and alternative channels

IDEMIA

Fraud Blacklist

Customer enrollment
Branch, mobile or online

KYC

Fraudsters **Defaulter**

Customer database

Noms	Photos
Pierre Dupont	
Alain Michel	
Robert Smith	
...	

Biometric Matching

Customer Watch list database

Noms	Photos
Pierre Dupont	
Alain Michel	
Robert Smith	
...	

Picture and ID available in database

› Most regulations impose on mobile operators to acquire the applicant ID document during the KYC process.

Biometric Search Services

Output

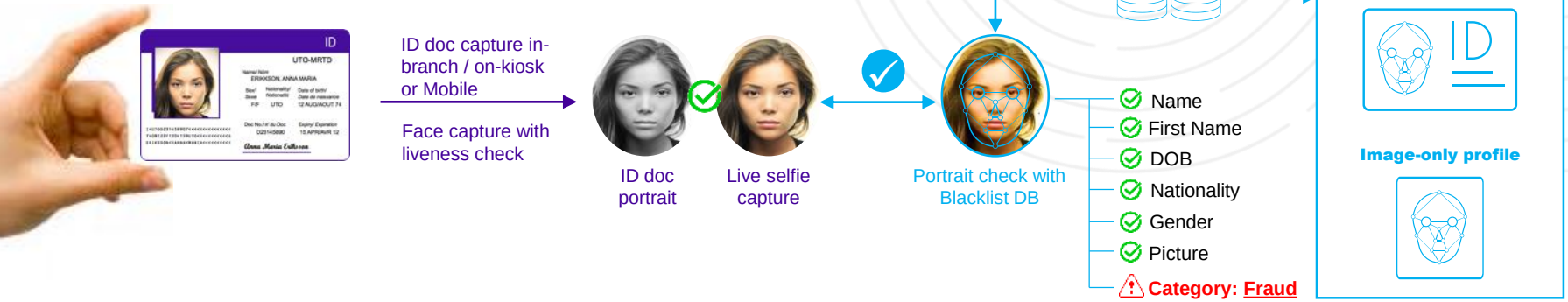
Identification of fraudsters and defaulters

Watch list Database offers

› Early risk detection
› Customer journey acceleration
› Massive drop of false positives
› Biometrics search service

IDEMIA

Biometric Screening Against Blacklist



Capture ID doc & selfie
Customer is asked to capture ID document and face selfie.

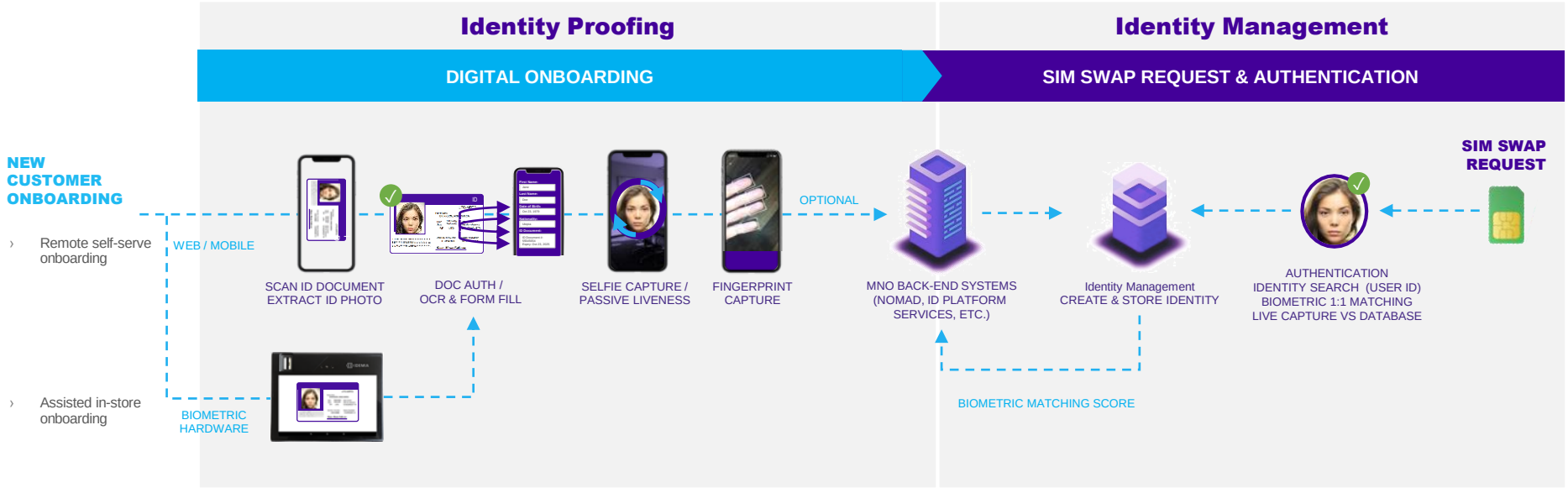
ID Verification
ID data including the portrait is extracted from the document.

Biometric Matching
ID document photo and the captured selfie are checked against the entire blacklist photo library.

Adjudication
Match is made. According to the scientific method used, the probability that the applicant is not the person in Blacklist library is in the range of 1 in 100,000,000.

IDEMIA

SIM Swap Fraud



IDEMIA

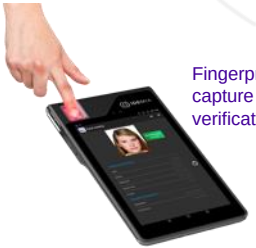
In-Store Onboarding with Biometric Hardware

Driver's license or national ID card capture with NFC

Passport capture with NFC

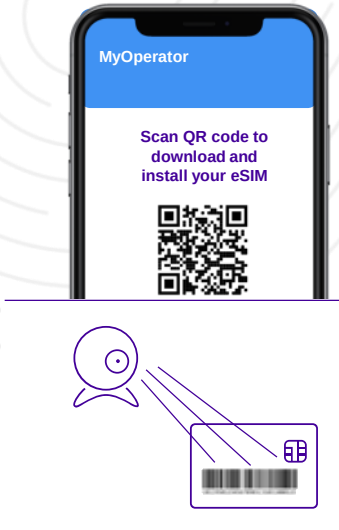
Driver's license or national ID card capture with MRZ scan

Face capture and verification



Fingerprint capture and verification

MyOperator
10GB
LTE



Plan Selection

Customer chooses a plan at the MNO retail store or kiosk.

In-Store ID Document Capture

Customer ID doc is captured in-store using IDEMIA's biometric-enhanced hardware terminals. Machine Readable Zone (MRZ) and NFC chip reading methods of data extraction are both supported.

Biometric Capture

Customer face or fingerprint can be captured and verified against the ID doc or root of trust (if access is available).

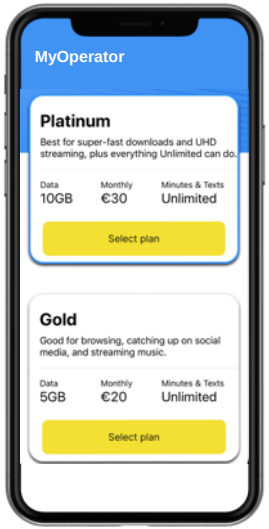
Activate eSIM or SIM card

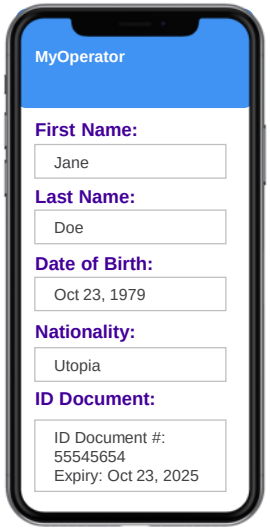
eSIM QR code is scanned, triggering a profile download onto the phone, or the ICCID barcode is scanned and physical SIM is activated.

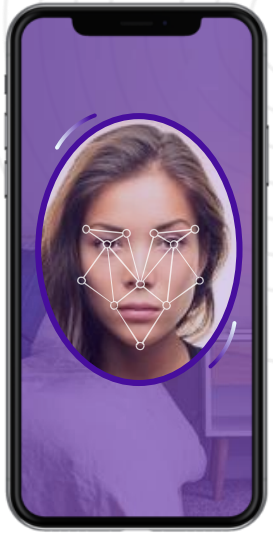
Activate Subscription

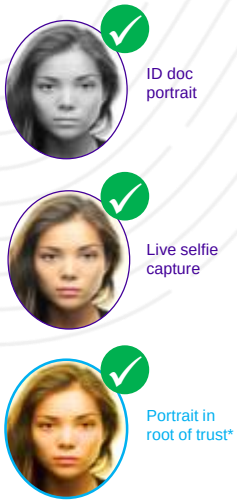
Subscription is activated on the MNO network and eSIM (or SIM) is installed onto the device.

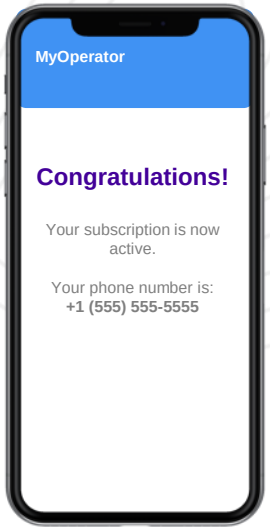
Remote Onboarding with a Mobile App











Plan Selection

Customer chooses a plan through the MNO app or mobile website.

ID Document Capture

Our SDK captures and extracts alphanumeric info and portrait, and verifies the document for authenticity.

Automatic Form Filling

Extracted data is used to populate registration forms, reducing data entry errors.

Selfie Check/ Liveness Detection

Capture a selfie and compare with the ID doc portrait, and optionally with a root of trust. Our industry-leading passive liveness detection ensures the customer's presence.

Activate Subscription

Activate subscription and download eSIM profile to device, or ship physical SIM.

* depending on RoT access availability

Remote Onboarding on the Web

Plan Selection

Customer chooses a plan through the MNO website.

ID Document Capture

Our SDK captures and extracts alphanumeric info and portrait, and verifies the document for authenticity.

Automatic Form Filling

Extracted data is used to populate registration forms, reducing data entry errors.

Selfie Check/ Liveness Detection

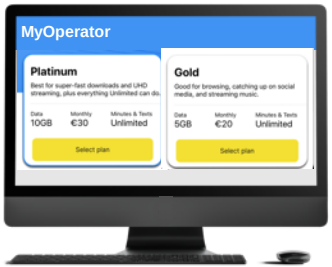
Capture a selfie and compare with the ID doc portrait, and optionally with a root of trust. Our industry-leading passive liveness detection ensures the customer's presence.

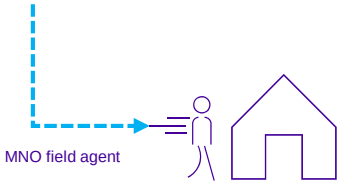
Activate Subscription

Activate subscription and download eSIM profile to device, or ship physical SIM.

* depending on RoT access availability

Field-Agent Digital Onboarding





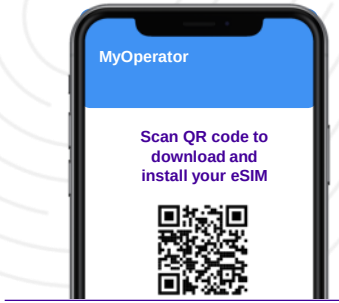
Driver's license or national ID card capture with NFC

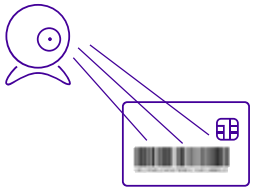
Passport capture with NFC

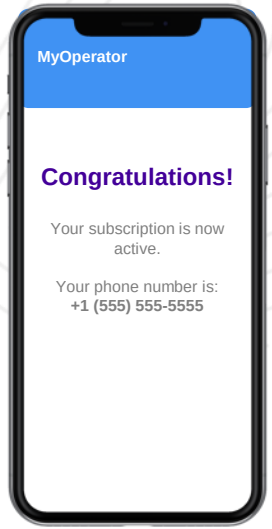
Driver's license or national ID card capture with MRZ scan

Face capture and verification

Fingerprint capture and verification







Plan Selection

Customer chooses a device and plan on the MNO website or mobile app

Contactless Delivery

MNO field agent shows up at home or office to deliver the device and perform the KYC process

ID Document Capture

Customer ID doc is captured using IDEMIA's biometric-enhanced hardware terminals. Machine Readable Zone (MRZ) and NFC chip reading methods of data extraction are both supported.

Biometric Capture

Customer face or fingerprint can be captured and verified against the ID doc or root of trust (if access is available).

Activate eSIM or SIM card

The eSIM QR code is scanned, triggering a profile download onto the phone, or the ICCID barcode is scanned and physical SIM is activated.

Activate Subscription

Subscription is activated on the MNO network and eSIM (or SIM) is installed onto the device.

Join us on

www.idemia.com