



Gemalto's trusted digital ID technology for Mobile Network Operators

gemalto 
security to be free

Table of Contents

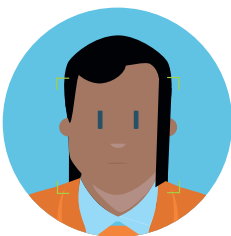
- 1. Capture devices & solutions.....4
- 2. Document verification solutions.....7
- 3. Biometric solutions.....10
- 4. Digitalization & use of ID.....13
- 5. Gemalto: Your trusted partner in digital identities.....15



The average person already owns multiple digital identities, which are used to access a range of different services. Yet as more and more important services move online, it's critical that digital identities reflect real, verifiable identities.

In response, companies across the globe are increasingly adopting trusted digital IDs as a secure way to verify their customers identities. As opposed to a person's declared identity, a trusted digital identity uses verification steps to prove that a person is who they say they are.

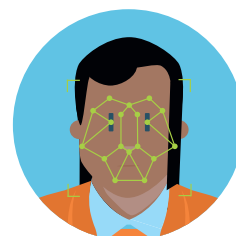
The creation of a digital ID consists of three general phases: 1) capture ID documents or biometric information, 2) verify the authenticity of these documents or check of biometric attributes, and 3) digitalize the identity for later usage. Here we present Gemalto's portfolio of technology for capturing, verifying, and digitalizing identities. These technologies and combined solutions can easily be deployed by MNOs to begin offering more advanced customer identity verification.



Capture



Verify
(ID docs & biometrics)



Digitalize



1. Capture devices and solutions

For the majority of MNOs, the days of “manually” checking the IDs of new mobile subscribers are coming to an end. The need to allow remote online sign-ups and a decreasing tolerance for slow processes in stores point towards the need for more efficient, flexible and secure identity capture methods. This includes a move towards collecting biometric information.

Gemalto's Secure Software Development Kit (for mobile devices) and our range of document readers and biometric readers make it possible for MNOs to set up an identity capture solution that can be deployed across all their sales channels.

1.1 Gemalto's Trusted Digital Identity SDK

If an MNO seeks to allow remote sign-ups, then a user's own device (such as a mobile phone or personal

computer) can be used to capture their identity attributes. Gemalto's Trusted Digital Identity SDK provides all the steps needed for customers to create a trusted digital ID from their smartphone.

Gemalto's Secure SDK is easily and transparently integrated with the MNO's mobile app and can be used on Apple or Android. The resulting application assists the subscriber in taking a picture of their ID document and taking a selfie. It controls the camera and displays the video stream on screen, while checking that the image quality is acceptable and that lightspots are not disturbing ID verification or facial recognition. Importantly, it also prompts the user to move to detect liveness. Quality control tips guide the user along the way. The image is automatically post-processed and prepared for analysis.

1.2 Gemalto Document Readers

To enable further verification of an ID document's security features or to capture identity attributes with an even higher degree of fidelity, dedicated equipment is needed. Gemalto's document readers address the need for security and speed simultaneously. Thanks to sophisticated checks (for example under ultra violet light)

our document readers can be used to detect numerous fake documents.

With options built for stationary use (desktop readers) at the point of sale as well as mobile use (tablet readers), these solutions can be easily adapted to different needs and priorities.

Our range of document readers cater to different security and mobility needs



White light

Picture ID verification under visible light



Invisible light

Identity document verification using ultra-violet & infrared scanners



Electronic

Electronic document verification of contact- or contactless documents

SUCCESS STORY

Gemalto's advanced document verification solution for a major MNO in North America

The challenge

A major MNO faced a problem in which falsified ID documents were being used for new phone activations, resulting in huge losses each year.

Gemalto's solution

The operator chose Gemalto's High Security solution to reduce retail fraud, automate data capture and improve customer service, using full page document readers.

Results

- > ID Authentication can handle the IDs specified by customer. ID Authentication enables speedy processing of the IDs presented by the customer. It's precise, while also accommodating minute variations in legitimate IDs, keeping false rejects to a minimum.
- > Data capture reduces data entry errors. Greater efficiency means less time doing data input, more time spent upselling features and services.

- > Reliable and convenient full page document reader
- > Reads and authenticates multiple document types:
 - Optical read of all ICAO 9303 travel documents
 - Passports, Visa, ID cards, driving licenses
 - RFID enabled, 1d and 2d barcodes
- > Visible, Infra-red and UV image capture
- > Fast and accurate document processing
- > Easy operation and maintenance
- > Maximum flexibility in systems integration



1.3 Gemalto biometric tablets & readers

Gemalto's biometric readers enable the collection of biometric information, such as fingerprints, at the MNO's point of sale. Gemalto's fingerprint scanners are certified and ensure high quality in the capture of biometric attributes. They are in use across the globe for secure identification at national borders, healthcare offices and law enforcement stations. Our biometric tablets have also been deployed in contexts where mobility and flexibility was key, such as for voter registration in remote areas.

A selection of Gemalto's biometric capture devices



Biometric tablet
Fingerprint & Facial



Fingerprint

1.4 Gemalto kiosks for self-service enrollment

Escalating standards for speed and convenience are leading many MNOs to allow customers to purchase SIM cards and mobile plans remotely and on-the-spot. To enable this convenience while adhering to security regulations like Know Your Customer, this remote process

needs to capture both ID documents as well as biometric information. Gemalto's kiosks make it possible to provide fully self-serviced enrollment capabilities in places like malls. These kiosks help reduce lines at points of sale and enable access to services anywhere.

Gemalto kiosks provide flexible ID verification solutions for swift and secure onboarding in unattended locations

- > Self-service at points of sale help avoid long lines
- > Improved user experience through touch screen
- > Highly customizable components including:

- Contact / Contactless reader
- Fingerprint reader
- Numeric PAD
- Web Cam
- Receipt printer
- Payment terminal
- Utility bill scanner



SUCCESS STORY

Fly to Gate

The challenge

To reduce bottlenecks at security checkpoints in airports. In collaboration with IER, Gemalto set about creating a multimodal biometric checking and document verification system.

Gemalto's solution

An identity token is created by matching a passenger's biometric information (face or fingerprint) to their travel reservation and ID.

Results

- > Processing time is reduced by up to 80%, vastly improving the passenger experience.
- > 87 automated control e-gate are being implemented across Paris-Charles de Gaulle and Paris-Orly.

87 automated
control e-gates

2. Document verification solutions

Identity fraud is significantly impacting the business of MNOs year after year, and the use of forged documents by fraudsters is one of the most commonly used tactics. Gemalto's document verification solutions significantly reduce this type of fraud with sophisticated technology for checking the authenticity of identity documents. With our range of capture devices, Gemalto offers three different levels of document verification, ranging from white light verification, to advanced verification under invisible light, up to electronic verification of the ID document's chip. Checks include verifications of visual patterns, color

bands, electronic chips and other security elements.

The document presented can also be referenced against a pre-defined Template Database containing a global list of reference identity documents such as passports, identity cards, residence permits and driving licenses. Gemalto's ID Verification Template database contains documents from over 180 countries and is constantly updated with new templates from identity documents around the world, as well as with new verification checks based on evolving fraud cases detected in the field.



2.1 Gemalto Document Verification under white light

This is Gemalto's fundamental verification offer, designed primarily for online verification via multi-function A4 scanners, smartphones and other consumer devices.

A comprehensive set of visual verification actions are performed in white-ambient light to ensure the integrity of the identity document. Verification can be performed either in store or remotely.

Gemalto ID Verification Template Database

Gemalto ID Verification offers document verification capabilities against a pre-defined Template Database containing a global list of reference identity documents such as passports, identity cards, residence permits and driving licenses.

ID Verification Template database contains documents from over 180 countries and is constantly updated with

new templates from identity documents around the world, as well as with new verification checks based on evolving fraud cases detected in the field.

Documents accepted for verification



100% e-passport coverage



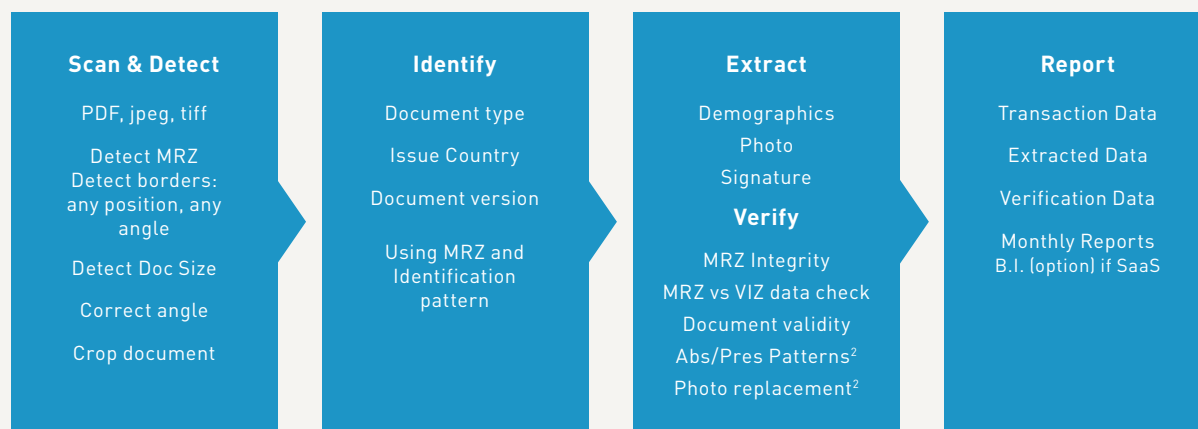
100% of European identity cards



A worldwide coverage of passports, id documents, driving licenses and residence permits

White light verifications include but are not limited to:

- > Identification of document (country, type, version)
- > Integrity verification of documents MRZ (special machine readable zone - 2 or 3 line code)
- > MRZ vs Visual Inspection Zone (VIZ) Consistency
- > Format validation of VIZ fields in accordance with ICAO standards
- > Check of document validity (non-expired documents)
- > Extraction of demographics and photo
- > Verification of visual security features and patterns over white-ambient light, photo replacement



*Specifications above are not exhaustive.

SUCCESS STORY

Orange France

The challenge

In 2015, ORANGE's invoicing and fraud/debt-recovery departments embarked on a project to improve ID verification systems in order to reduce fraud and the resulting financial consequences.

100%
of fraud reduction
measured in some stores



Gemalto's solution

They selected Gemalto's automatic, real-time ID Verification solution to help reduce the financial burden of ID fraud, and to ensure that all verification processes were in place across all stores.

Results

- > The solution successfully performs hundreds of daily real-time verifications.
- > After Gemalto's ID Verification solution was introduced, the fraud rates were slashed by up to 100% in some stores.
- > Thousands of sales staff are requesting real-time ID Verification across all ORANGE stores.

Advanced Document Verification enables enhanced verification of different identity document security features that exist in different light spectrums: white, infra-red, and ultra-violet.

2.3 Gemalto electronic ID verification

Numerous protection mechanisms are in place to avoid malicious extraction of data from the chip. The communication channel between the chip and the reader is protected and transmitted data is encrypted. Before data can be read from a chip, the reader needs to provide a key derived from the **Machine Readable Zone** on the ID or main page of the passport. Once the information on the chip is read, it can be compared to the information printed on the document. It is extremely complex and expensive to falsify the information printed on the ID document's chip, which is why electronic verification is seen as the leading-edge of verification.

AutoFill by Gemalto was designed to quickly extract data from a captured image of a particular identification document and auto-populate fields in an existing database, CRM or custom application. It can be used, for example, on a mobile device to capture data from different identity documents & utility bills. Data is then

- > All Document Verifications under White light
(as mentioned in previous chapter)
- > Presence and absence of pattern and color band
- > UV Dull paper
- > Ink check
- > Photo replacement
- > Luminance
- > Digital Watermarks



AutoFill by Gemalto significantly reduces the onboarding and transaction time, as well as eliminates the possibility of human error in the transaction and registration process. It can be used as a stand alone solution or in combination with one of the verification offers.



3. Biometric solutions

Gemalto's biometric verification services include solutions for fingerprint verification and facial recognition, as well as for iris and palm verification. In response to the foremost market needs, we focus on fingerprint and facial recognition.

We have more than 200 biometric deployments in 80 countries, serving strong biometric authentication and identification programs for governments and businesses. Acquiring Cogent Systems enabled us to leap ahead in the arena of trusted digital identities and build upon

Cogent's 27 years of biometric technology expertise. Our comprehensive suite of biometric verification technology can be adapted to suit varying security and flexibility needs.

200 biometric deployments
in 80 countries

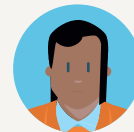
Live Capture



Reference



Comparison



3.1 Gemalto Cogent Facial Verification Solution (LFIS)

Gemalto Facial Recognition performs a comparison between the photo printed on an identity document (or contained on the chip if it is an electronic document) vs a live capture of a face (front-facing or selfie). By using top-end facial verification algorithms in combination with a constant QA process of the document photo (detection of hotspots over the picture), this technology reduces the number of false positives and maximizes the detection of fraud attempts. Throughout Gemalto's years of supplying biometric verification projects, this solution has been adapted to reliably perform in adverse conditions such as reduced lighting.

Results are provided in seconds by matching the facial biometrics of a selfie to the face image on the ID document and indicating if they match. In this process, the face image is captured then sent to the Face Verification service for analysis in the backend.

Gemalto Cogent Live Face Identification System (LFIS) is a top performing algorithm for facial recognition according to the National Institute of Standards & Technology.

- > Cogent Face Recognition is typically used for identifying wanted people on a blacklist using high resolution cameras and sending alerts to a console/mobile in real-time.
- > Cogent Facial Recognition integrates latest facial recognition technologies, such as fast face tracking and set-to-set matching.

3.2 Gemalto's Liveness Detection Solution

Gemalto liveness detection prevents fraudsters from using static images/figures such as printed photos, photos broadcasted from a screen, an animated video, 3D "hard" masks, head sculptures and other mechanisms used to fake identities. The solution ensures that there is indeed a live person in front of the camera by enabling two separate authentication factors (facial recognition + liveness detection). This offers a higher level of assurance that a person possesses a valid ID, that they match the photo on the ID and that they are a live person.

HOW LIVENESS DETECTION WORKS

The Liveness Detection feature prompts the user to execute a movement and evaluates the user's response. As Liveness Detection requires analysis on a video stream, Gemalto has

selected a local solution to avoid transmission of heavy video files in the network.

Example of online attack



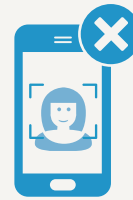
Bob is willing to steal Ann's identity



He has access to her ID Card and takes a picture



He presents a picture of Ann to fool the face matching algorithm



The liveness fails

Both a facial recognition scan and a liveness check take no more than five seconds. This not only helps increase customer

conversions, it can also significantly minimize fraud. All without impacting customer experience.

3.3 Gemalto's Fingerprint Verification Solution (AFIS)

Gemalto Automated Fingerprint Identification System provides true, integrated multimodal fingerprint identification. It is a scalable and customizable solution that allows you to perform a range of tasks for processing, editing, searching, retrieving, and storing fingerprints and more. It is designed to integrate easily with industry-standard biometric recording workstations/devices as well as with third party systems. GTO's AFIS technologies have been used in more than 80 countries

from national biometric civil identification projects to border control and criminal records systems.

AFIS performs at top levels in terms of accuracy, speed, flexibility, and scalability. Superior algorithms and a comprehensive set of powerful tools analyze and enhance the quality of prints, increasing the probability of a hit. While transactions are processed in the background, users can concurrently perform multiple tasks swiftly and precisely.



Gemalto Assurance Hub (GAH)

Third party checks can be conducted via Gemalto Assurance Hub (GAH), which helps a fraud department assess the risk undertaken when an end user subscribes to the company's services. This tool analyzes the data linked to the user, e.g. payment history with the MNO, geographic criteria, the user's typical IP address, the device the user uses to access the

service, and so on. Data from other parties, such as a credit bureau, can also be called on in the case of certain users. Depending on the score generated by the risk engine, the user will receive different authentication messages when accessing a service (fingerprint only or password + selfie, for example).



4. Digitalization & use of ID

After capture and verification is completed, the user's identity is trusted and verified, allowing them to subscribe to MNO services. When allowed by law and usually after explicit user consent, MNOs may save the digital ID of a user.

This trusted digital identity also simplifies future access or login to MNO services — a user may simply be asked to present his fingerprint or selfie. In the case where an MNO wants to position as identity provider, this Trusted Digital ID may even allow a user to access third party services, such as:

- > 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

Gemalto's solutions can be connected to third parties to retrieve additional ID attributes and perform checks, further enriching the trusted digital identity. Advanced interfacing is possible with external systems, criminal history systems, Livescans, mobile devices, web-based solutions, and other information systems.

4.1 Gemalto Mobile ID

Gemalto's Mobile ID solution powers the entire life-cycle management of mobile identities, from user registration to verification of mobile digital signatures, and connection to the certification authority and e-Government portals.

The future-proof Mobile ID platform is compliant with all GSMA Mobile Connect requirements and enables user-friendly and secure mobile services to improve the lives of consumers. This is our go-to solution to help MNOs become Trusted Identity providers.

Mobile eID is an electronic identity wherein the user identity is based on Public Key Infrastructure (PKI) and the keys are typically generated and stored in a tamper-resistant environment (in this case, the SIM). The Mobile ID SIM app allows citizens to confirm their identity and sign documents directly from their mobile phone, by entering a unique user-selectable PIN code.

This solution provides MNOs and government agencies with total flexibility in terms of integration with new service providers and as is entirely scalable regarding additional services.



SUCCESS STORY

Mobile ID Moldavia

The challenge

Moldova's Governance e-Transformation Agenda aims to digitize all public services by 2020. As a part of the agenda, the Moldovan government is collaborating with mobile network operators to start the The Mobile ID program. Gemalto set about to create a Mobile ID solution to allow citizens to confirm their identity and sign documents directly from their mobile phone, by entering a unique user-selectable PIN code.

Gemalto's solution

Gemalto's Mobile ID solution is responsible for the entire life-cycle management of mobile identities. This solution provides telecom operators and government agencies with total flexibility in terms of integration

with new service providers. As such, it is entirely scalable in terms of additional services. The future-proof Mobile ID platform is compliant with all GSMA Mobile Connect requirements and enables user friendly and secure mobile services that improve the lives of the Moldovan people.

Results

Today, more than 34,000 registered users utilize secure mobile digital signatures for eLicencing, tax declarations, criminal records requests and more. In 2013, the government of Moldova received a Government Global Mobile Award from the GSMA for embracing mobile technologies to improve government initiatives.



65%

Citizens' openness to using e-services via computer and/or mobile phone.



33%

The share of people who have accessed a government institution web page at least one time.



67%

The level of satisfaction of those citizens who offered marks from 3 to 6 (on a scale of 3-6).



5. Our core expertise: Digital identity

5.1 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 to them meet the need for greater security and convenience simultaneously. Our technology serves as the basis for 150+ eGovernment

 **150+** eGovernment programs

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. Serving as a trusted partner to MNOs over many years,

5.2 Accompanying your 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

we have supplied state-of-the-art products and services, compliant with the latest GSMA specifications. We provide SIM cards and managed services to more than 700 million subscribers and have already deployed more than 1000 solutions. 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 more than 450 MNOs, we seek to help MNOs provide the best possible experience to billions of people.

 **450**
MNO
customers

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.

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>