​​​**Enabling swift and secure multi-channel Trusted Digital Identities**

To ensure their position in a future landscape, MNOs, OEMs and service providers need to claim new territory in the digital market, cut operational costs, and attract new customers. This can be achieved by establishing seamless and entirely digital customer journeys. A Trusted digital identity is the key to securing these journeys and to opening up a wealth of access for customers to security-sensitive services.

**​What is aTrusted Digital Iden​tity?**

To begin with, a digital ID is the technological link between a real entity such as a person and its digital equivalent entities. It includes a collection of electronically captured and stored identity attributes including biographic and biometric data.

People own many digital identities that consist of an email address and a password to access different online services. In some cases, such as engaging with media or entertainment, we may access social media using a pseudonym to reveal less about our identity. But when it comes to certain areas, like government services and banking, it’s critical that you are who you claim to be: IDs need to be trusted.

**A Trusted Digital Identity is created when the information provided has been verified, or checked for authenticity.**

A trusted digital ID consist of a set of verified attributes (like verified ID documents or biometrics), thus providing a certifiable link between an individual an​d their digital identity. These attributes may also include verification with third parties such as Government databases, social identity, credit card number or mobile records.

​For MNOs, OEMs and other enterprises, trusted digital IDs mean smoother digital workflows, faster customer acquisition processes and consistent customer data. Operating costs are reduced and the customer experience enhanced. Moreover, a Trusted Digital Identity can serve as a gateway for subscribers to access multiple security-sensitive services such as mobile money, eGov and online banking, allowing MNOs to take a lead in these fast growing sectors.

This is where Thales' Trusted Digital Identity Services Platform comes into play, a one-stop services platform to digitalize mobile subscriber enrollment.

It orchestrates everything needed by Telecom Operators to digitalize customer enrollment, including the capture, verification and authentication of customer credentials and biometrics.  Drawing on Thales' in-depth experience and expertise in these fields, as well as complementary services from trusted partners worldwide, the platform enables [streamlined enrollment](https://www.thalesgroup.com/en/markets/digital-identity-and-security/mobile/id-security/id-verification), both in-store and online.

As a result, Telecom Operators, OEMs and other enterprises can accelerate their digitalization strategies, launch new services, fight fraud and meet regulations.

​​**How to create a Trusted Digital Identity?​**

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.​ ​​

**1. Capture**

​

In-store or remotely, identity attributes are captured. Those attributes are ID documents such as passports, driving licenses, ID cards and also biometrics such as faces. The hardware needed can range from a mobile phone to specialized high end scanners.

**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.

**3. ​Digitalize**

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. ​

​ ​ ​

**1. How to capture ID documents and biometrics?​**

**Capture ID do​cuments**

The subscriber's ID 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.

**Capture biometr​ics**

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 or fingerprint.​

​​​​

​​**2. How to verify ID documents and biometrics?** ​

**Verif​​y identity**

After it has been captured, the system verifies the authenticity of an ID document with dedicated software. Different methods can be used to check security 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 different levels of document verification: standard, based on ID picture from visible light, advanced with security features existing in white, infra-red and ultra violet and chip-based with electronic document verification.

**​​Verify bi​​ometrics**

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 serv​ices that require identification — and in particular when verification needs to be conducted remotely.

**3. How is a digital ID created​?**

**Digitalize**

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 seamlessly access the MNO’s services or third party services.