



Thales Trusted Digital ID
FINGERPRINT SCANNERS
For Mobile Network Operators

Meeting new regulations

Identity fraud is increasing in most countries, often resulting in the use of mobile subscriptions to perpetrate criminal acts or even terrorism. To protect citizens and fight the effects of such frauds, many governments are planning or have already implemented new regulations that oblige Mobile Network Operators (MNOs) to strengthen identity verification during subscriber enrolment. As part of this process, several countries now require subscribers' fingerprints to be captured and/or verified. This is particularly the case in countries where few people have an identity document, or such credentials are not sufficiently secure to ensure robust verification.

Cutting the cost of fraud

Strengthening identity verification of subscribers also helps MNOs to fight fraud that directly impacts services such as sponsored devices and postpaid subscriptions. Significant annual cost savings can therefore be achieved.



Thales' biometric technologies

Thales has more than 200 biometric deployments in 80 countries, supporting strong biometric authentication and identification programmes for governments and businesses. Acquiring Cogent Systems enabled us to leap ahead in the field of trusted digital identities and build on Cogent's 27 years of biometric technology expertise. Our comprehensive suite of biometric verification solutions can be adapted easily to suit varying requirements for security and flexibility.



Thales' core expertise: digital identity

At Thales, we work with some of the world's largest businesses and governments, providing flexible technological solutions that help meet the need for greater security and convenience simultaneously. Our technology serves as the basis for over 150 eGovernment programmes. Digital identity remains at the core of our expertise, as we enable hundreds of our partners to implement advanced authentication and security solutions.

Serving as a trusted partner to MNOs over many years, we have supplied state-of-the-art products and services, compliant with the latest GSMA specifications. We provide



SIM cards and manage services to more than 700 million subscribers and have already

deployed more than 1000 solutions. Our products comply with the most demanding international standards, such as those defined by the U.S. Department of Commerce, the FBI, Interpol and the American National Standards Institute.

By merging our expertise in digital identity with long-standing partnerships with more than 450 MNOs, we seek to help operators provide the best possible experience to billions of people.

Comply with regulations and fight fraud with Thales fingerprint scanners

Thales fingerprint scanners enable the collection of fingerprints (from 1 to 10 fingers) at the MNO's point of sale. These fingerprints can then be verified against either a government fingerprint database (where available), or an MNO's database. Where possible, they can even be compared with the fingerprints stored inside the chip of a secure identity document.

In an unattended environment, attacking a fingerprint-based biometric system by presenting fake fingers to the sensor represents a serious threat. A forger, using relatively simple methods, could copy a fingerprint from

Anti-spoofing technology
(Liveness Finger Detection - LFD)

a smooth surface and transfer it to a material like silicone gel, slipping it over the finger to fool the scanner. Thales' patented, built-in HW-based Liveness Finger Detection (LFD) technology resists spoofing attacks with all known materials, significantly increasing security in unattended applications. A patented illumination system inside the scanner detects if the finger placed on the prism/scanner is human skin, or if artificial materials are involved. In the event of a spoofing attempt, the system returns the message: "FAKE FINGER DETECTED".

Thales fingerprint scanners are certified and ensure high quality capture of biometric attributes. They are in use across the globe for secure identification at national borders, healthcare offices, law enforcement stations and MNOs.

DactyID20

A compact single finger scanner offering a superior built-in fake finger detection system. This versatile scanner can be used for verification or authentication, especially for unattended applications such as kiosks, online login and many others.

Key benefits

- Easy integration: multi-OS support (Windows, Linux and Android), MultiScan SDK, OEM module also available
- Ease of use: acquisition driven by a software interface explaining which scanner to place and the result of acquisition
- Fake finger detection: patented technology for Liveness Detection
- Software latent fingerprint and halo removal: no need to clean the prism after every acquisition
- Competitive price and low maintenance costs: no consumables needed (e.g. silicon membranes, cleaning kits)
- High quality: designed in Italy for outstanding quality and reliability
- Smart Card: Smart Card reader model available
- FBI PIV: FBI PIV certified – FAP20
- iBeta tested: ISO 30107-3 Biometric Presentation Attack Detection Standard Level 1 compliant



Available in three versions:



DactyID20

Desktop version



DactyID20_SC

Desktop version with
Smart Card reader
included



FSM20

OEM/Module for
integration into third
party equipment
such as kiosks

Certification

In August 2020 DactyID20 became the first PIV FAP20 certified scanner that is compliant with ISO 30107-3

Thales anti-spoofing capability was tested by iBeta to the ISO 30107-3 Biometric Presentation Attack Detection Standard and was found to be compliant with Level 1.



The iBeta laboratory is accredited by NIST NVLAP as an independent test lab.

At the end of test the number of fake fingers classified as real (APCER rate) was zero (0%). Moreover, the number of real fingers classified as fake was also equal to zero (0.03%).

DactyScan84

A compact 10-print and rolls biometric Livescan, in full compliance with the "10-print capture scanner & software user group requirements". Suitable for all applications that require 4-slaps and rolled acquisition.

DactyScan84 is a heavy-duty scanner enabling several applications, including:

- Civil identification and authentication
- Access control
- e-ID documents, e-Passport and visa issuance
- Border control
- Criminal background check

10-prints and rolled acquisition

With up to 27 frames per second for 4-slaps and up to 25 frames per second for rolled prints acquisition, the Multifinger Scanner DactyScan84 is unique in terms of acquisition speed. An ergonomic design combined with an easy-to-integrate SDK architecture makes the Multifinger Scanner DactyScan84 the perfect choice for system integrators and solution providers.

A user interface based on 12 three-colour LEDs facilitates the acquisition procedure by indicating the fingerprint(s) to be acquired and providing quality feedback. This eliminates the need for skilled operators, increasing workflow efficiency.

The Multifinger Scanner DactyScan84 is available as an OEM module, for system integrators requiring a compact 10-print Livescan that can be physically integrated into embedded solutions.

Spoofing and Liveness Detection

As an option, Multifinger Scanner DactyScan84 can be upgraded with a leading-edge SW solution that detects fake fingers made with a variety of different materials.



Active scanning window

Flat four fingers up to 3,2" x 3,0"

Two flat thumbs up to 3,2" x 3,0"

Rolled finger up to 1,6" x 1,6" - 500 dpi

Supported Operating Systems

Microsoft Windows up to Win10 in 32-bit and 64-bit configuration; Linux Ubuntu and Fedora distributions in 32-bit and 64-bit configuration; Android.

Certification

The Multifinger Scanner DactyScan84 is a 3.2" x 3.0" 10-prints and rolls Livescan at 500 dpi certified by the FBI according to FBI IAFIS IQS App. F. as a Livescan System as well as for Identification Flats.