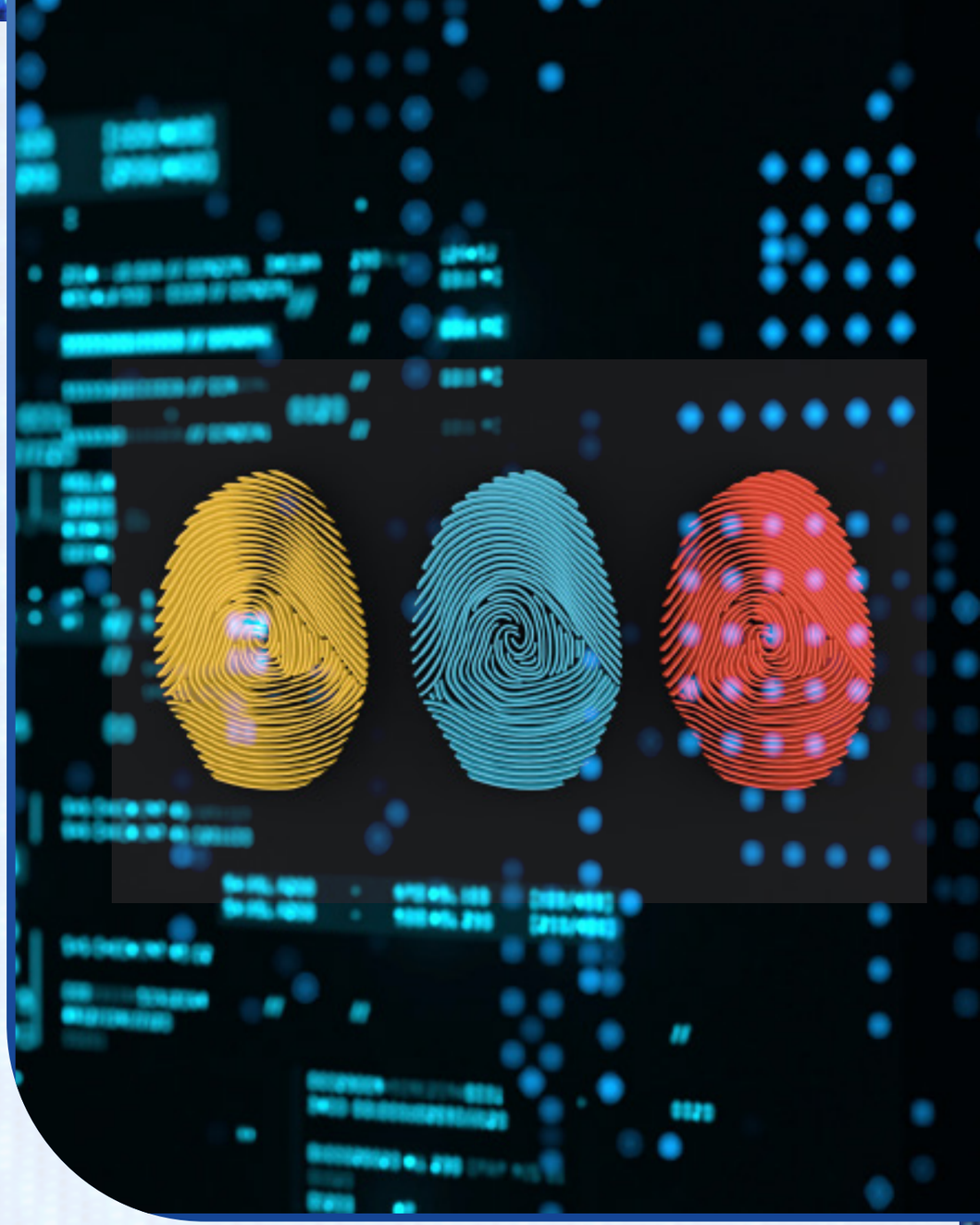
A Definitive Guide **to Fingerprint Technology**

EBOOK

Fingerprint technology is a mature, proven method for user authentication across a range of industries, use cases and environments. Selecting the right fingerprint technology often comes down to the level of **security** and **match accuracy** required, **capabilities** and **features** needed and **usability** to achieve both adoption and productivity. This eBook provides an overview of common fingerprint technologies available in the market today, aiming to help you make an informed decision in selecting an optimal fingerprint biometric system for your environment and needs.



HID

Why Fingerprints?

Commonly referred to as “something you are,” biometrics are unique human attributes, such as a fingerprint, face, palm print, voice and iris, that can be used to accurately establish the identity of one person from another.

Among the different modalities, the fingerprint is one of the most widely used methods for biometric authentication due to its speed, ease of use, high level of accuracy and cost-effective nature.

Fingerprints possess the functional components of being:

- **Universal:** it’s an attribute that (nearly) everyone has
- **Unique:** everyone’s fingerprint is unique and distinguishable
- **Permanent:** it’s reasonably stable, permanent and invariable over time
- **Collectable:** the prints can be acquired, measured and processed with ease
- **Defendable:** the prints can be defended from abuse, misuse, theft, imitation and substitution
- **Performant:** the feature, when combined with recognition techniques, performs with accuracy, speed, scale and ease of use
- **Adoptable:** the fingerprint has the highest adoption rate for biometric authentication

The Three Elements of Fingerprint Biometric Systems

A fingerprint biometric system consists of several components which work together to make an effective solution.

It begins with the fingerprint sensor, which is designed to capture and preprocess fingerprint data. A biometric algorithm is used to extract fingerprint minutiae data such as ridge endings, ridge bifurcation, ridge islands, the direction minutiae is pointing and measurements. A presentation attack detection (PAD) technique can also be used during the time of capture to ensure that the fingerprint is from a real, live person.

If the conditions are met, then the digital print dataset is stored as a record, called a template, in a cryptographically secure storage enclave. During the matching process, the presentation of the fingerprint is rechecked for liveness, and the template is retrieved from secure storage to perform the match.

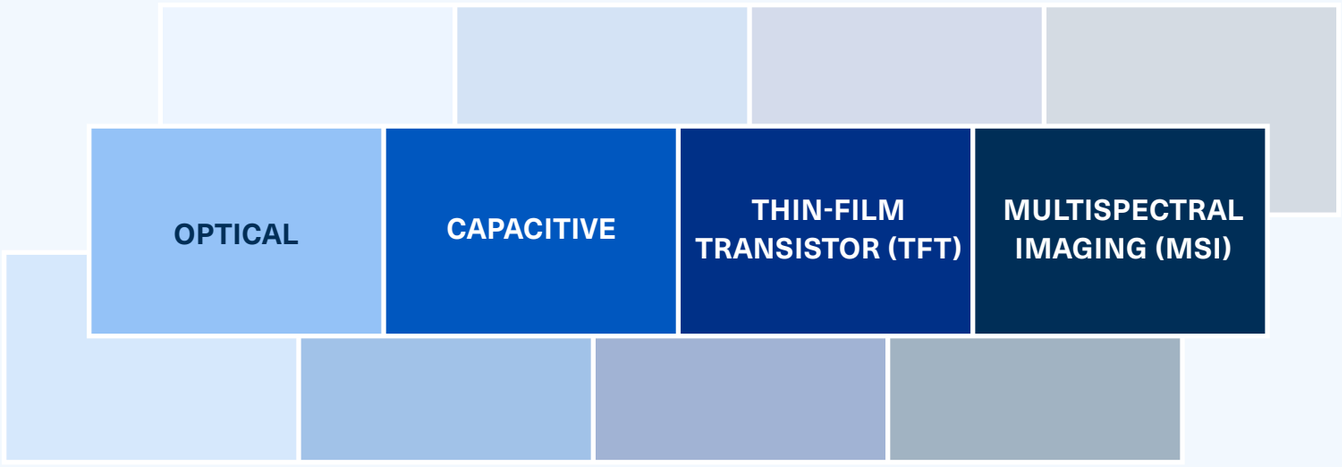
What separates an optimal biometric authentication system from a low-performing system? There are three important factors to consider:

1. How well the capture works for a range of fingers, skin types and print conditions across different environmental conditions such as temperature, humidity, light, surface oils, dust and dirt.
2. How effective PAD works to identify and reject fake finger attempts.
3. How well the system can accurately match legitimate users while rejecting illegitimate users.

Successful Biometric Implementations Require **3 Critical Components**

Fingerprint Sensing Technologies

There are different types of fingerprint readers in the market, but the prevailing ones are: optical, capacitive, thin-film transistor (TFT) and multispectral imaging (MSI). The basic idea behind each technology is to capture finger images, measure the physical differences of the images and establish an individual's identity. However, each technology has specific properties to perform fingerprint capture, presentation attack detection and matching for biometric authentication.



HID

Optical

Optical is the most mature sensor type for capturing and matching fingerprints. Optical readers use a light source, such as an LED, to shine a bright light over a fingerprint, take a digital photo and use algorithms to identify unique patterns on the print surface by analyzing the lightest and darkest areas of the print image.

The optical fingerprint sensors have a finite resolution. The higher the resolution, the finer the details that the sensor can detect about a finger, increasing the level of accuracy. Additionally, a thin silicon coating can be added to improve usability.

KEY BENEFITS:

- Most mature sensor technology
- A compact size to fit in most desktop environments or shared workstations
- Performs well in capture and matching, working quickly with a high degree of accuracy
- Offers a cost-effective price point for all types of use cases

Small form factor and cost-effective, optical fingerprint readers are ideal for desktop environments or shared workstations.

HID

Slim, power-efficient and relatively inexpensive, capacitive fingerprint readers are suitable for many high-traffic supervised environments such as border crossing, point-of-sale (POS) terminals and multi-user applications.

Capacitive

The capacitive method involves the use of small electric fields between the plates of an array of capacitors. A sensing element, or pixel, is made up of two capacitive plates with a small electric voltage between them, which generates an electrical field that extends above the sensor and gets altered by the finger presence.

When a fingerprint ridge is close to the capacitive plates, the electrical field will be blocked, reducing the field strength at that pixel. When a fingerprint valley is close to the capacitive plates, the electrical field is unaffected.

The capacitive fingerprint sensor measures the field strength for both ridges and valleys, resulting in differences in the electrical charge at the plate, and the data is combined to generate a grayscale fingerprint image. Advanced capacitive readers are less prone to fake finger attempts than their optical counterparts.

KEY BENEFITS:

- Compact and thin design best fits where space is limited
- Power-efficient and well-suited to battery-operated devices
- Less affected by lighting conditions for both indoor and outdoor environments
- Defendable and less prone to fake finger attempts

Thin-Film Transistor (TFT)

The TFT reader offers high-resolution image quality even under direct lighting while also being lightweight, slim and easy to carry, an ideal choice for in-the-field identification.

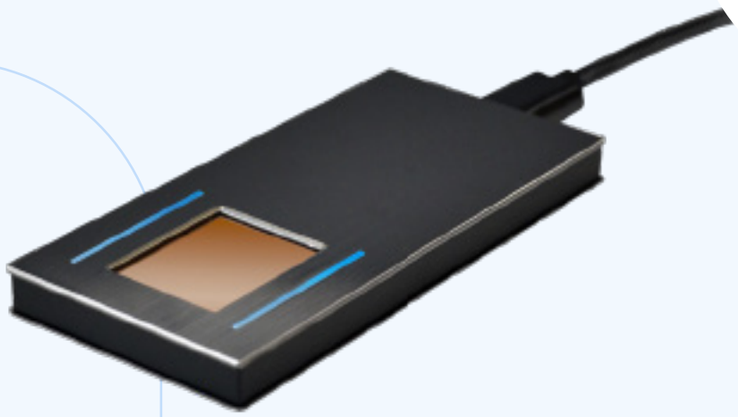
TFT fingerprint sensor can accurately recognize the smallest fingerprint features with ultra-high resolution. It provides exceptional accuracy for advanced biometric and security requirements.

In the area of fingerprint capture, TFT technology is used either as a larger-size matrix capacitive proximity detector (capacitive fingerprint sensor) or a larger-area matrix light detector (optical fingerprint sensor).

KEY BENEFITS:

- Ultra slim and lightweight, ideal for in-the-field mobile identification
- Low power consumption, ideal for in-the-field use
- Cost-effective price point for many use cases
- Optimal for mobile biometrics for law enforcement

TFT-based fingerprint readers are ultra slim and lightweight, ideal for in-the-field mobile identification.

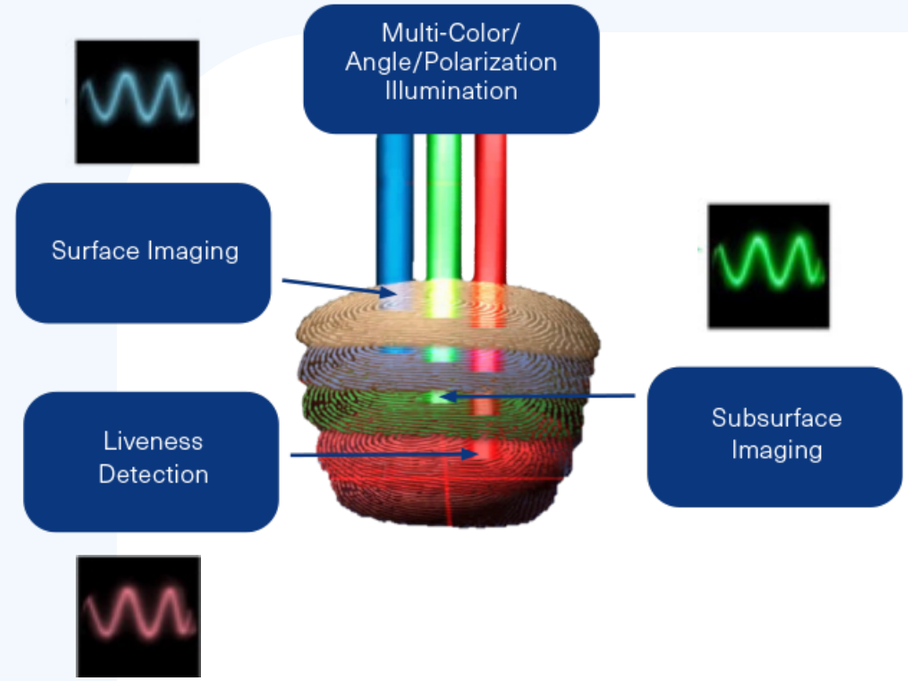


Multispectral Imaging (MSI)

MSI is an HID-patented technology that uses multiple colors of light projected into the finger from different angles to collect both surface and subsurface biometric data. This unique feature enables MSI readers to capture difficult fingers (e.g., dry, dirty, damaged, oily, wet and aged) in harsh environments (e.g., heat, cold, rain and snow), and deliver the highest level of accuracy.

HID's exclusive MSI fingerprint readers are **ISO 30107-3 PAD Level 2** compliant for advanced anti-spoofing against fraud.

Moreover, the technology offers sophisticated endpoint security. This feature prohibits cyber criminals from gaining unauthorized access to networks by turning fingerprint readers into secure endpoints.



KEY BENEFITS:

- Reads both surface and subsurface finger data for the highest level of matching accuracy
- Captures the most difficult fingerprints of diverse demographics
- Performs in challenging environments
- Conforms with ISO 30107-3 PAD Level 2 standards, reliably detecting spoofs
- Delivers endpoint security, protecting systems and networks behind the firewall

MSI readers use multiple colors of light at different angles to collect both the surface and subsurface fingerprint data for anti-spoofing against fraud and matching accuracy.

iBeta QUALITY ASSURANCE
TESTED
LEVEL 2
ISO 30107-3
Presentation Attack Detection
COMPLIANT

HID

Key Considerations for Selecting the Right Fingerprint Technology

The key considerations and requirements for selecting fingerprint technology are a balance between the total cost of ownership, security, suitability and usability. Below we explore some of these:

SECURITY

- ☑ Is the industry highly regulated such as financial services, healthcare, government entities or law enforcement?
- ☑ Are advanced capturing and biometric authentication specifications mandatory?
- ☑ Is there a need to ensure anti-spoofing?
- ☑ Is there a need to have endpoint security so networks, systems and data behind the firewall won't be impacted in the case of the fingerprint device being hacked?

SUITABILITY

- ☑ Will the technology be embedded in devices that require low power, battery-operated capability and portability?
- ☑ Will the technology need to fit into small spaces or be used in difficult elements or environments, indoor or outdoor?
- ☑ Is durability from unpredictable weather and lighting conditions a factor?
- ☑ What applications will the technology be used for, such as mission-critical border control or more common commercial use?

USABILITY

- ☑ Does the technology perform capture and matching with ease and consistency?
- ☑ Does the technology need to handle high volumes of fingerprint captures and matches?
- ☑ Is matching quick and accurate to enable user productivity instead of friction frustration?
- ☑ Will the device be used by multiple people in a shared workstation setting?
- ☑ Can the reader handle all types of fingerprints and diversified demographics for the mass population?

Based on these criteria, organizations can decide what kind of fingerprint capture technology best fits their deployment.
For example, for a shared environment with limited space, such as healthcare clinician's terminals, a slim and durable capacitive sensor would be a good fit. For more demanding use cases in highly-regulated, mission-critical environments that can't risk an identity misstep, such as banking or border crossing, organizations should consider more advanced technologies such as multispectral imaging (MSI) readers.

Key Use Cases for Fingerprint Biometrics

As industries continually evolve their identity and access strategies, they face unprecedented threats from fraud, account takeover and impersonation. Fingerprint biometrics continues to provide the most accurate, efficient and secure method for enrollment, user authentication and identity verification.

The use cases for fingerprint biometrics are widespread. One of the most common ones across industries is access control. For properties like government facilities, healthcare locations and corporate offices, biometric access control provides a valuable layer of protection.

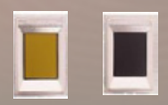
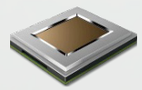
But fingerprint biometrics offers more than that. In this table, we highlight the **key use cases by industry** in which fingerprint biometrics is a proven solution to address real-world challenges.

BANKING & FINANCE	HEALTHCARE	RETAIL	LAW ENFORCEMENT	GOVERNMENT
• Biometric ATM • Customer Onboarding (eKYC) • Customer/Employee Authentication • Compliance (AML/KYC) • Fraud Prevention	• Chain of Custody • Compliance (HIPAA/EPCS) • Employee Authentication • Medical Fraud Prevention • Patient ID	• Age Verification • Loss Prevention • POS Security • Self-Service Checkout • Time and Attendance	• Background Checks • Criminal Booking • Crime Investigation • Inmate Management • Mobile Identification	• Benefits Distribution • Border Security • Citizen ID • Employee Authentication • Voter Registration

HID

Comprehensive Fingerprint Reader and Module Offerings

One solution does not fit all. Businesses can narrow their choices to the best fingerprint technology by matching their intended use cases with the key considerations. Whatever your use case is, our product lineup ensures that we have a solution to meet your needs and requirements.

OPTICAL	CAPACITIVE	TFT	MSI
DigitalPersona	EikonTouch & TouchChip	Nomad 30	Lumidigm
 DigitalPersona 4500 & 5300 Readers	 EikonTouch 510 & 710 Readers	 Nomad 30 Pocket Reader	 Lumidigm M-Series & V-Series Readers
 DigitalPersona 4500, 5200, 5300 Modules	 TouchChip OEM Modules	 Nomad 30 Module	 Lumidigm M-Series & V-Series Modules

iBeta LEVEL 1 ISO 30107-3 Presentation Attack Detection TESTED COMPLIANT

iBeta LEVEL 2 ISO 30107-3 Presentation Attack Detection TESTED COMPLIANT

HID

EXPLORE HID'S BIOMETRIC EXPERTISE:

- **Learn more about HID's fingerprint technologies and offerings >>**
- **Explore HID's comprehensive biometric portfolio >>**
- **Read HID's biometric blog posts >>**
- **Follow us on LinkedIn >>**

hidglobal.com

North America: +1 512 776 9000
Toll Free: 1 800 237 7769
Europe, Middle East, Africa: +353 (91) 414060
Asia Pacific: +852 3160 9800
Latin America: +52 55 9171-1108

For more global phone numbers click here

2026-05-01-bio-definitive-guide-fingerprint-technology-eb-en
PLT-07165

Part of ASSA ABLOY