




FINGERPRINTS

# ACCESS ALL THE RIGHT AREAS

AN INTRODUCTION TO BIOMETRICS AND ITS VALUE TO ACCESS CONTROL



*"Growing innovation of integrating biometrics is seeing the tech add even more value to our home and working lives. Just look around at our increasingly connected world. The unique balance of convenience and security offered by biometrics can bring trust to access control use cases in our devices, homes and offices"*

**Michel Roig**, Senior VP Business Line Payments & Access, Fingerprints

# TABLE OF CONTENTS

<b>CHAPTER 1</b>	<b>04</b>
Biometrics 101	
<b>CHAPTER 2</b>	<b>14</b>
What makes fingerprint the king?	
<b>CHAPTER 3</b>	<b>23</b>
The success of fingerprint in mobile	
<b>CHAPTER 4</b>	<b>31</b>
Smarter access; at home, at work	
<b>CHAPTER 5</b>	<b>34</b>
The benefits of biometrics for access control	
<b>ABOUT US</b>	<b>36</b>
About us	

# 01



# BIOMETRICS 101

In today's connected world we are required to prove who we are many times each day, and this can take a lot of valuable time. Locks need to be opened, devices need to be accessed and secure purchases need to be made – but it is essential that only authorized people can perform these tasks.

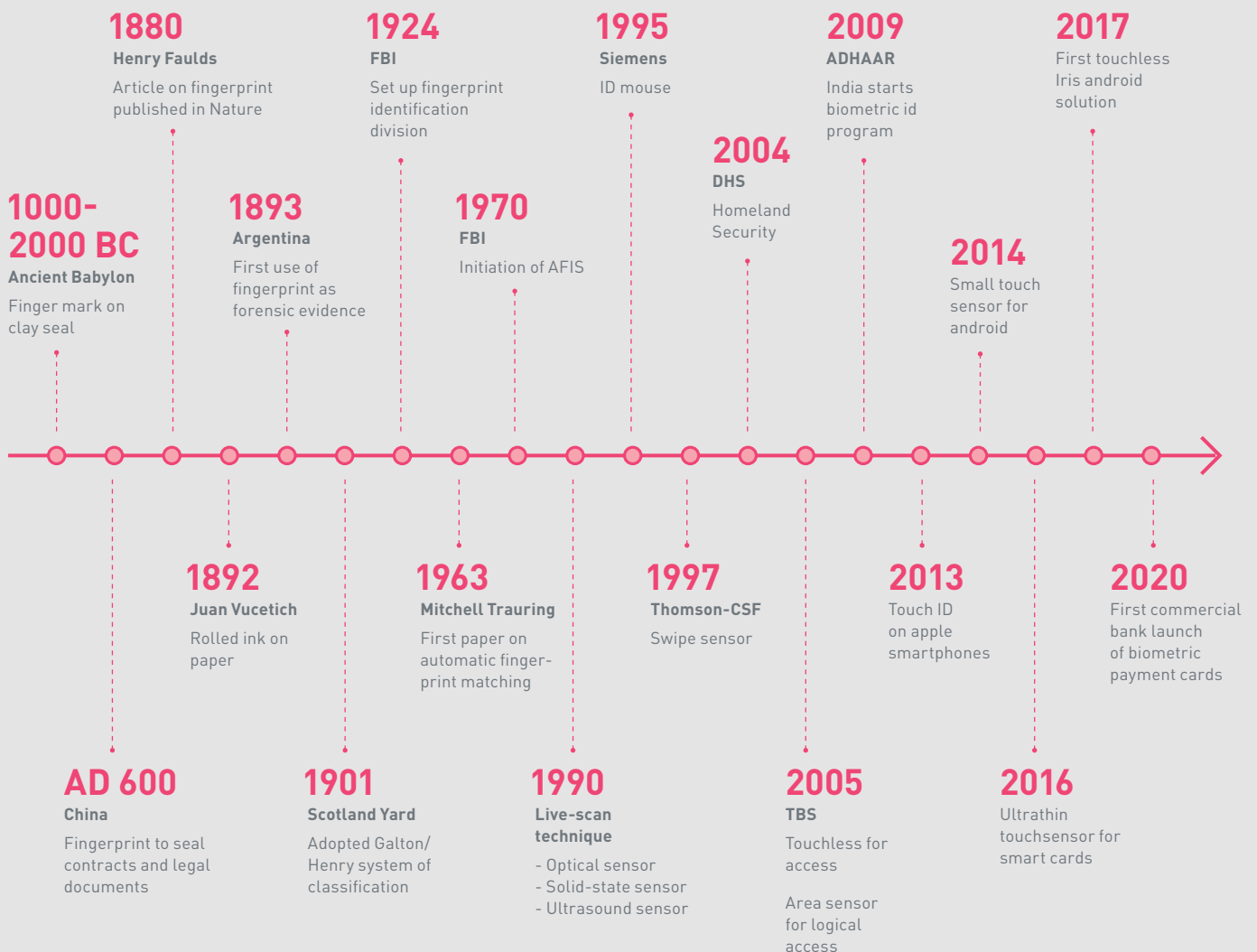
With so many activities needing fast, reliable and convenient authentication, it is no surprise that identity verification has become a cornerstone of today's society, enabling secure and seamless interactions while preventing fraud and criminality.

## BIOMETRICS – A POTTED HISTORY

Using biometrics as an authentication method is not new as physical characteristics have always been used to identify people. There is evidence of fingerprints being used as a person's mark for Babylonian and Chinese business transactions as far back as 500 B.C. and 300 B.C. respectively. The late 1600s saw a number of observations made into the details of fingerprints and in 1788 German anatomist and doctor J. C. A. Mayer became the first to declare the uniqueness of friction ridge skin.

In the 1800s a Parisian anthropologist called Alphonse Bertillon developed a method to identify criminals. 'Bertillonage' required numerous, precise measurements of a human's anatomy, body shape and markings. The late 1800s saw Sir Francis Galton publish a detailed study in which he presented a new classification system for fingerprints and the 'minutiae' that he defined are still in use. In 1896, the 'Henry Method' was developed by Azizul Haque in India to classify and store fingerprints so that searching could be performed easily and efficiently.

## BIOMETRIC RECOGNITION MILESTONES



Automated processes for biometric recognition have only become possible in the last few decades with the advancements in integrated circuits and computer processing. Today there is a **broad variety of biometric technologies** available, with **fingerprint** recognition being the **most widely used**.

# THE FUTURE



The Future: The connected world of the cloud, smart homes, and smart cities needs new identification and authentication solutions. This is opening up a billion new possibilities for our biometric technologies.

# WHAT IS NEEDED TO AUTHENTICATE?

Authentication factors give us the means to verify identity or confirm authorization to perform a task and can be grouped into three basic categories: something the user knows, something the user has, or something the user is.



## **INHERENCE**

Something the user is or does, for example a fingerprint, signature, voice etc. Biometric authentication leverages various inherence factors to validate the identity of a user.



## **OWNERSHIP**

Something the user has, for example an ID-card, security token, mobile phone, physical key etc.



## **KNOWLEDGE**

Something the user knows and hopefully remembers, such as a password, PIN-code, answer to a security question etc.

Authentication often includes at least two, preferably three of the above categories. This is then referred to as two-factor and multi-factor authentication (MFA). It is of course also possible to use several factors from the same category, such as a PIN-code and a security question, but that will not give the same extended level of security as “true” multi-factor authentication.



## IS BIOMETRIC BEST?

Choosing authentication methods is always a balancing act between several different factors such as size, cost, power and processing requirements convenience and, perhaps most importantly, security. Where knowledge-based factors such as PIN or password are easy to implement, they can be hacked through data breaches, spyware, algorithms or even social engineering techniques like shoulder surfing. Also, users tend to select simple and common passwords, even sharing them with others or storing them in an unsecure way. This makes reliable authentication impossible, especially if they are expected to use a growing list of increasingly complex usernames and passwords as their use of connected technology grows.

Authentication based on ownership factors is generally safer but relies upon a physical token like a key, card or phone which are easy to steal, lose or even simply leave at home. Manufacturing these devices also costs money.

### BIOMETRICS

### OTHER AUTHENTICATION

#### POSITIVE

- Unique to each person
- Always with you
- Does not change over time

#### POSITIVE

- KNOWLEDGE**
- Easy to implement
- OWNERSHIP**
- Generally easier



#### NEGATIVE

- Social acceptability of some biometric methods.
- The cost, size and power requirements of the sensor and processing logic

#### NEGATIVE

- KNOWLEDGE**
- Easy to break computerized algorithms
- Users tend to select simple and common passwords, even use the same one for office and for private and sometimes even share them with others. This makes reliable authentication impossible.
- OWNERSHIP**
- Relies upon a physical token which are easy to steal



When biometric authentication is correctly implemented, the information needed is **unique to each person**, is always with them, and normally does not change over time.

Security is obviously one of the most fundamental factors to discuss when comparing biometric authentication systems. As always, there is a tradeoff between high security and user convenience which needs to be considered. Assessing a system's security is not limited to how well the biometric identifier can be read and matched. We also must include possible illegal access to the processing engine – hacking – and if it can be fooled by someone simulating the biometric identifier – spoofing.

As an example of an anti-hacking measure used in today's modern consumer devices, a mathematical representation of the fingerprint is stored as a template, instead of the image itself. Storing the representation reduces hacking risks, since it cannot be used to re-create the original fingerprint image. Furthermore, the template is not stored just anywhere on the device. In mobile devices the template is stored, and the algorithms involved in the authentication process are run, in a Trusted Execution Environment (TEE). This further enhances security as it keeps the biometric data, as well as the processes, away from potential hackers and viruses.

Spoofing involves the forgery of faces, voices, fingerprints etc. in an attempt to authenticate fraudulently. Many advanced technologies have been developed to minimize the risk of spoofing. In fingerprint recognition, for example, spoofing risks can be reduced by increasing the image quality and by using sophisticated matching algorithms. Additional security can be achieved by various anti-spoofing schemes and use of more than one biometric identifier to authenticate the user.

*No system can be made totally secure – with unlimited time (and money) you can hack and spoof anything. Advanced biometric techniques however make such malicious attacks extremely expensive and time consuming.*

Biometrics is a unique security technology that means there is no trade-off between security and convenience.



## FRR vs THE FAR

### FALSE REJECTION RATE

Often used to gauge the convenience of biometric sensors, this tells you how often the sensor will wrongfully reject the valid biometric in the matching algorithm.

### FALSE ACCEPTANCE RATE

Frequently used in assessing the security of biometric systems, this tells you how often the sensor will statistically provide a positive match without the right biometric data.

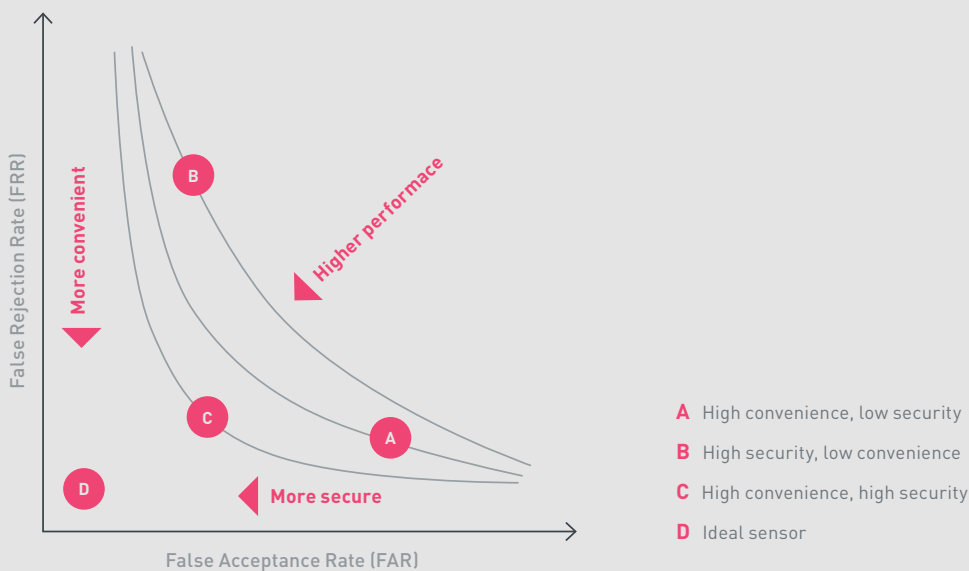
Plotting the FRR versus the FAR for various types of biometric authentication systems gives an insight into the trade-offs between security and convenience. The ideal sensor has minimal FAR as well as FRR, but in reality, biometric authentication systems are somewhere on a curve where you either have high convenience (low FRR) but lower security (high FAR) or vice versa.

Convenience is also related to other attributes of the sensor, such as how intuitive it is to use, how quickly it wakes up/how the user wakes it up, as well as how the sensor is incorporated in the end-product, though that is more a consequence of size and design flexibility of the sensor.

$$\text{FAR} = \frac{\text{TOTAL FALSE ACCEPTANCES}}{\text{TOTAL FALSE ATTEMPTS}}$$

$$\text{FRR} = \frac{\text{TOTAL FALSE REJECTIONS}}{\text{TOTAL TRUE ATTEMPTS}}$$

### TRADE-OFF BETWEEN SECURITY AND CONVENIENCE



# 02

What makes fingerprint the king?





# WHAT MAKES FINGERPRINT THE KING?

Humans have many biometric identifiers, or modalities, that can be captured and analyzed by biometric systems. Behavioral identifiers are measurable traits that are acquired over time and can be analyzed to confirm identity by using pattern recognition techniques. Physiological modalities are something you are, rather than something you do or know.

But what kinds of biometric authentication are there,  
and **WHY HAS FINGERPRINT RISEN TO THE TOP?**

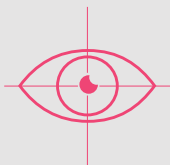
EXAMPLES OF <b>PHYSIOLOGICAL IDENTIFIERS</b>	EXAMPLES OF <b>BEHAVIORAL IDENTIFIERS</b>
Fingerprint, handprint, footprint Iris and retina of the eye Face, ear Vein and vascular patterns	Voice Signature Gestures Gait



## FINGERPRINT

**Analysis of the unique ridges and patterns of skin on our fingertips**

The de facto modality to date and often the first thought when people are asked to name a biometric authentication method.



## EYE

**Examination of the iris, retina or scleral vein patterns of the eye**

Previously a preserve of governments, now smartphone technology is making it available for widescale consumer use.



## FACE

**Scrutiny of the many features of the face**

Widely available in many of today's smartphones, but requires good lighting, simpler 2D solutions are easily spoofed and become unreliable with ageing faces.



## VOICE

**Analysis of a person's voice print**

Although cheap, it is difficult to accommodate regular changes that come with age, illness or location and they are very easy to spoof.



## VEIN RECOGNITION

**Scrutiny of the vein pattern of fingers or hands**

A secure but sometimes slow method with high processor requirements, which often make scanners large, costly and power hungry.



## BEHAVIORAL

**Recognition of a person's gait or gestures**

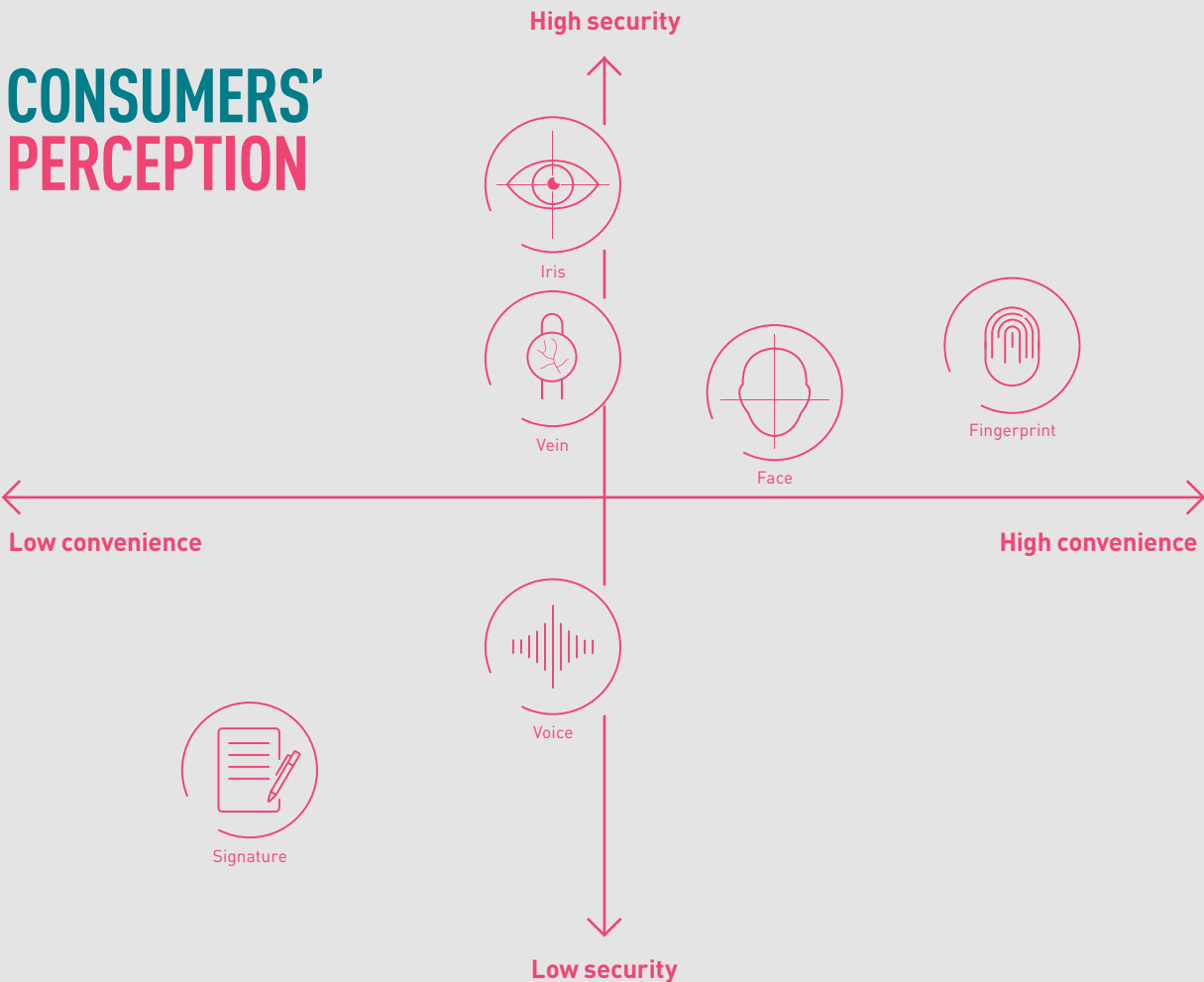
Comes with accuracy concerns and is relatively new and expensive as it requires additional complex equipment and analytics to be integrated with a video surveillance camera.

## COMPARING BIOMETRIC MODALITIES

		FINGERPRINT	IRIS	FACE (2D)	FACE (3D)	VEIN	VOICE
SECURITY	Uniqueness						
	Hard to copy/spoof						
CONVENIENCE	Speed						
	Accuracy						
SCALABILITY	Cost efficient						
	Easy to integrate						

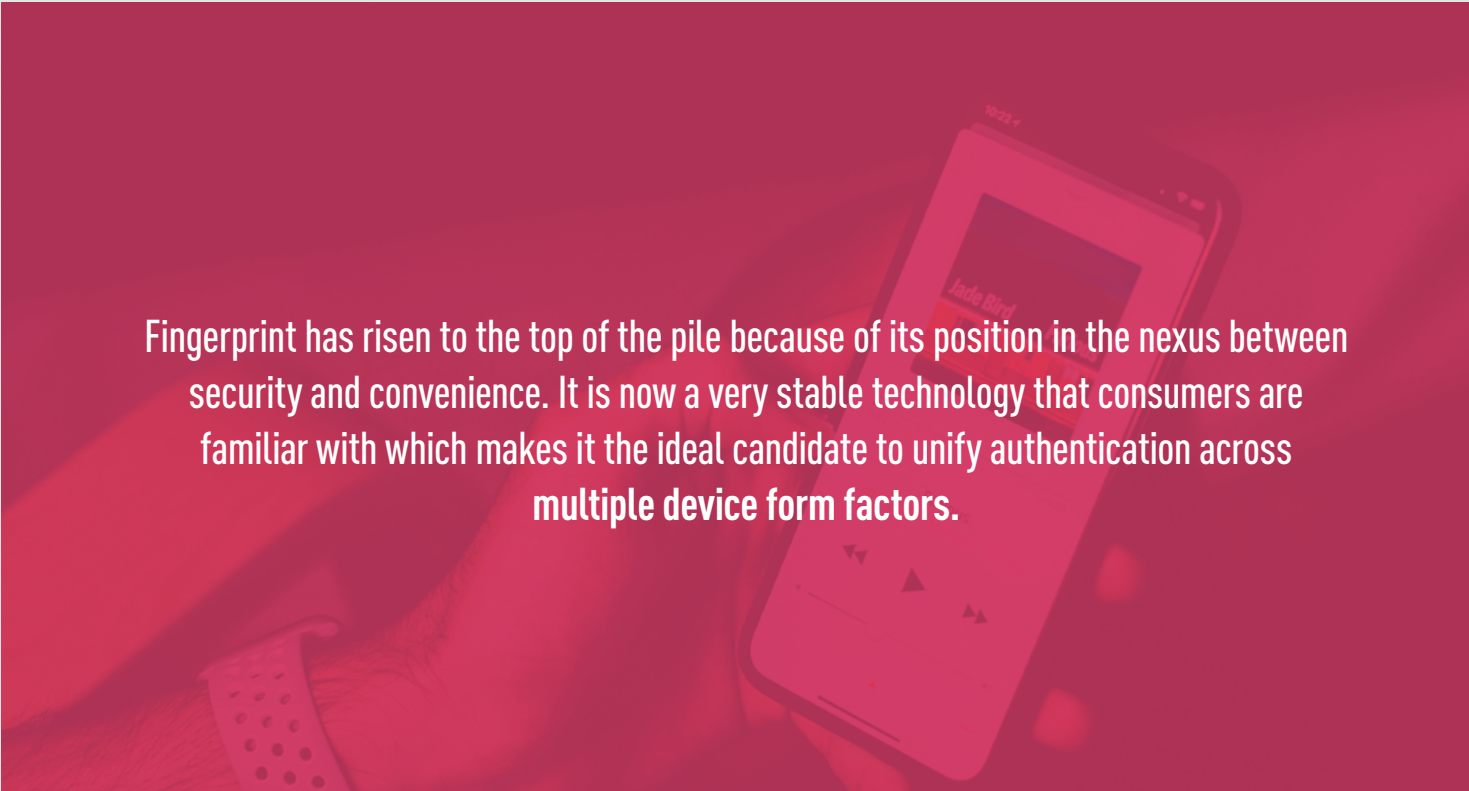


So, it is fair to say that there are several options when it comes to choosing which biometric modality to use, and it all depends on the unique authentication needs of the implementation.



Source: Fingerprints™ market research 2017 in collaboration with Kantar TNS, 4,000 online consumers in UK, USA, China, India.





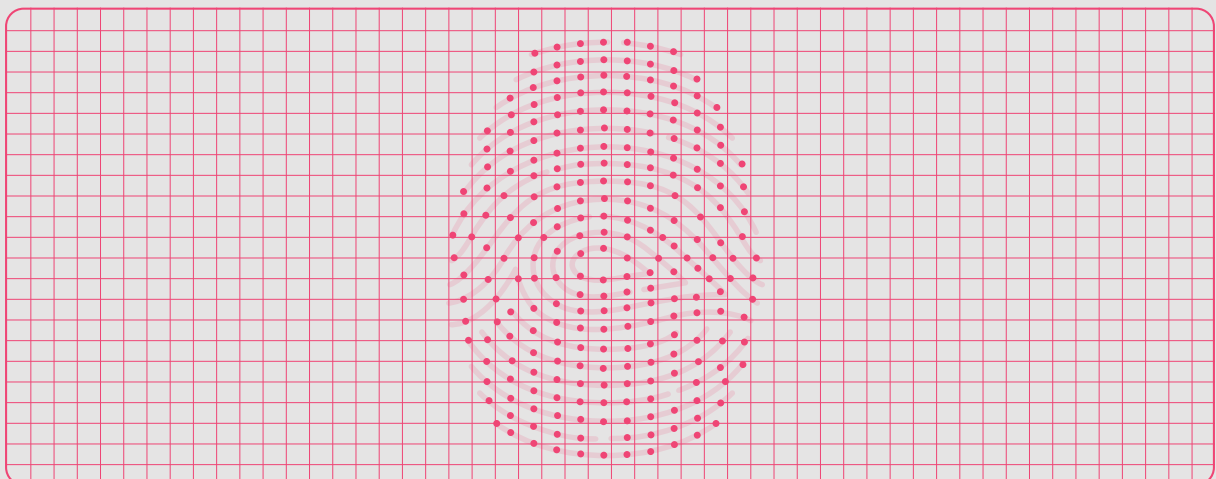
Fingerprint has risen to the top of the pile because of its position in the nexus between security and convenience. It is now a very stable technology that consumers are familiar with which makes it the ideal candidate to unify authentication across **multiple device form factors.**

## A CLOSER LOOK AT FINGERPRINT

Unfortunately, though, it is not simply a case of choosing 'fingerprint' as there are several different types of fingerprint sensors which each lend themselves to different use cases and scenarios.

## WHAT IS A FINGERPRINT SENSOR?

A fingerprint sensor is an electronic device used to register a digital image of the fingerprint pattern. It is often integrated into another device, such as smartphone, laptop, payment card or door lock. The sensor captures the relevant fingerprint features for further processing within the device.



**CAPACITIVE** - Generates the fingerprint image by passing a small electrical current across the surface of the finger.

Excellent image quality allows small sensors that have very low power consumption to be produced at a low cost. They also boost 3D anti-spoofing measures, perform fast image capture, are durable and easy to integrate. This technology hits the sweet spot making it the most common and popular fingerprint sensor in high volume consumer devices like smartphones.

**OPTICAL** - A camera is used to capture an image of the fingerprint.

As the first electronic fingerprint sensor to have been launched, they are now cheap to produce and can also be integrated into the screen, opening up new use cases like in-display sensors on smartphones. But they are also prone to spoofing, do not work well in sunlight, are sensitive to contamination by their environment and often wear with age.

**THERMAL** - Create fingerprint images using temperature measurements.

Limited adoption as they often have high power requirements, are not able to capture fine details, can be quite large, can't create 3D images and are sensitive to "wear and tear".

**ULTRASONIC** - Creates visual images of the fingerprint by bouncing high-frequency sound waves off the epidermal skin layer.





























They provide more biometric information than most other fingerprint sensors and are good at reading wet and damaged fingers, but not dry fingers. They can be slow, expensive, power hungry, bulky and require a lot of processing power.

**PRESSURE SENSITIVE** - Create an image when the ridges and valleys of a finger apply different levels of pressure to the surface.

Pressure sensitive sensors can be small and are one of the few sensor categories, beside capacitive, that can be integrated in smaller devices such as mobile phones and tablets. However, existing sensors are temperature sensitive and less suitable for use where the environmental conditions are harsh or rapidly changing.

The sheer diversity of the cost, power efficiency, size, convenience and other requirements mean there is no one ‘biometric silver bullet’ that suits every requirement. However, the closest we can come to this is through **ACTIVE CAPACITIVE TECHNOLOGY**, which is the first choice in most applications.

## FINGERPRINT TECHNOLOGY COMPARISON

	ACTIVE CAPACITIVE	ULTRASONIC	OPTICAL	ACTIVE THERMAL
Cost efficiency				
Design flexibility				
Technology maturity				
Security				
Convenience				
Power efficiency				
Mobile device adoption				

 High  Medium  Low

A man in a suit is shown from the chest up, adjusting his glasses with his right hand while holding a smartphone in his left hand. The background is a blurred crowd of people, suggesting a public event or conference. The entire image is overlaid with a semi-transparent red filter.

*The trust and usage in mobile are paving the way for integration into new areas, new devices and applications.*

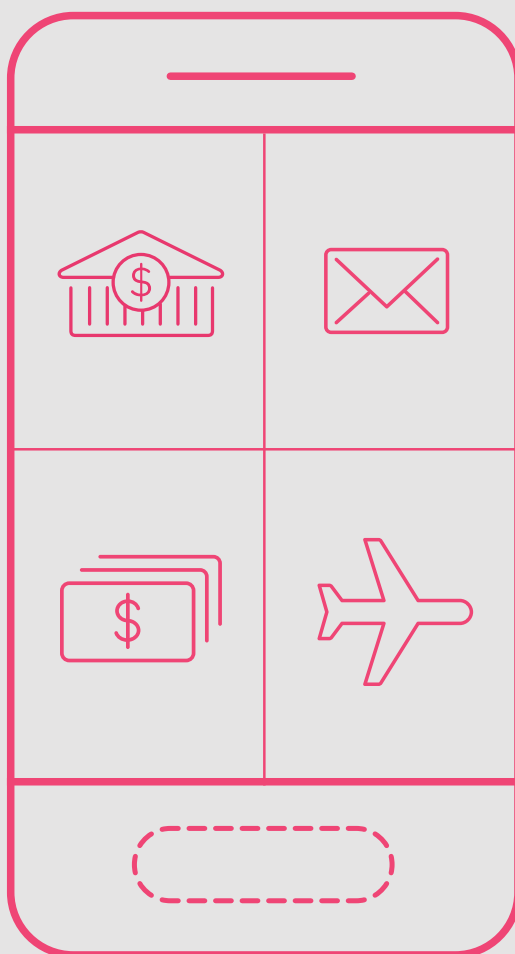
# 03

The success of fingerprint in mobile



# THE SUCCESS OF FINGERPRINT IN MOBILE

After a decade of integration, mobile is the most mature market for consumer biometrics. Biometrics has now become the preferred method for mobile authentication, and its use has gone far beyond device unlocking to become an integral part of many of the use cases seen with today's typical smartphone user.



What's more, when you combine human error and laziness with today's complex password requirements (Warning: password must be at least 12 characters long and contain a capital letter, a number, a special character, and cannot contain a word, name, or a place) we have a recipe for disaster.

All of this has seen biometrics rise to the top as one of the best authentication solutions to raise mobile security hand in hand with convenience.

## FINGERPRINTS HAS ACHIEVED HUGE SUCCESS IN MOBILE

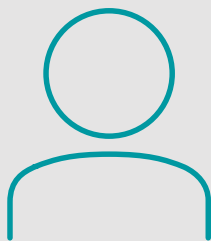


Fingerprint has replaced PINs and passwords as the most popular way to authenticate on mobile



**>80%**

of smartphones shipped have biometrics



**82%**

of consumers that have access to biometrics on their smartphone use it\*

Fingerprint sensors are also expected to remain the number one authentication option, despite solutions like iris and facial recognition grabbing headlines.

\*Source: Fingerprints™ market research 2017 in collaboration with Kantar TNS, 4,000 online consumers in UK, USA, China, India.

# 04

Smarter access: at home, at work





# SMARTER ACCESS; AT HOME, AT WORK

Protecting our domestic and professional lives is essential.

Over the years, the Internet of Things (IoT) has made our world smarter and more connected, bringing with it new levels of convenience. Connectivity, however, brings new security challenges.

Biometric authentication can bring an end to the frustration, stress and insecurity of misplaced physical keys, cumbersome and forgettable passwords, and unhygienic PIN codes. With biometric technology, you are the key to everything.

## UNLOCKING THE NEXT GENERATION OF SMART HOME

Over the years, IoT solutions have been making our homes smarter. Energy meters, multimedia, lighting and security systems...connected devices are transforming our domestic lives.

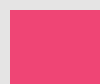
Research estimates that consumers are driving this trend as the smart home market is expected to grow from \$78.3 billion in 2020 to \$135 billion by 2025.\*

## CONSUMERS WANT BIOMETRICS TO ACCESS THEIR THINGS



27%

to access their home/ house



22%

to log in and personalize their entertainment system settings



21%

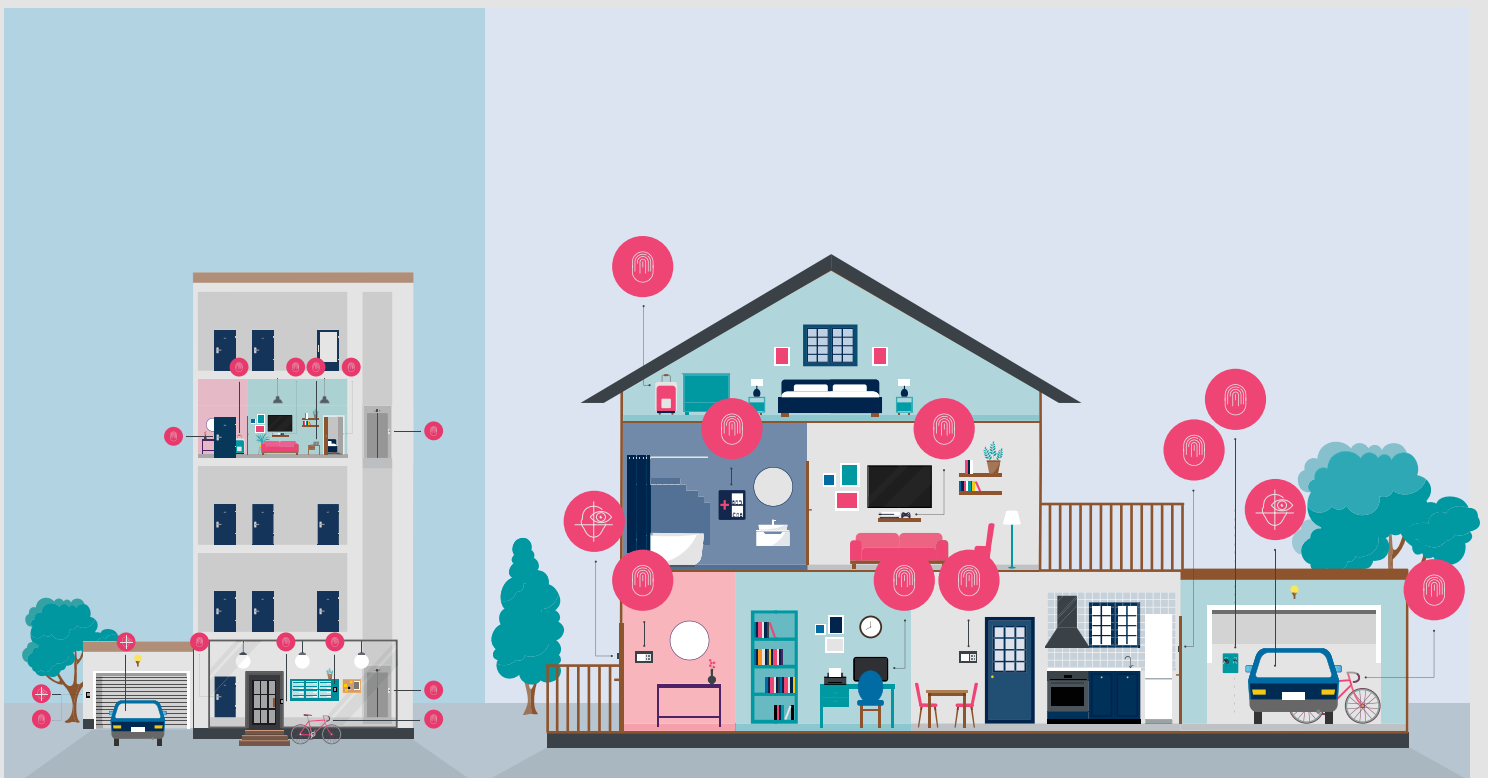
turning on/off alarm



20%

to access and personalize their car

\*Source: Research and Markets 2020, *Smart Home Market with COVID-19 Impact Analysis by Product (Lighting Control, Security & Access Control, HVAC Control, Entertainment, Home Healthcare), Software & Services (Proactive, Behavioural), and Region - Global Forecast to 2025.*



## IT ALL STARTS WITH HOW YOU ENTER

**Biometric control of door locks** – embedding a fingerprint sensor within a door, handle, frame or elsewhere to grant entry.



## MANAGING YOUR HOME SYSTEMS

**Home alarms and electronics such as remote controls and multimedia systems** – all controlled, and personal settings accessed, with a single touch.



## CAR ACCESS AND SETTINGS

**Unlock your car and it automatically adjusts to your personalized settings** – getting your journey off to a seamless start.



## PROTECTING YOUR VALUABLES

**Kitchen appliances, safes, medicine cabinets, suitcases and bike locks** – protecting and securing belongings and (hazardous) areas.



## KEEP YOUR PC PERSONAL

**Biometrics in PCs and peripherals** – users can unlock computers and access data, apps and services.

## WHY BIOMETRICS MAKES A SMART HOME SMARTER

**LOCK...LOCK...WHO'S THERE?** - With biometric door locks, you become the key. PINs and passwords can be hacked, locks can be picked and keys can be lost or stolen. Biometric sensors within devices and locks adds a trusted layer of security, making our homes safer without compromising convenience.

**KEEP IT PERSONAL** - Using biometrics allows you to log in and automatically adjust to the personalized settings of your smart home systems, letting you enjoy your smart home quicker.

**SECURING SAFER SPACES** - Hazardous areas such as medicine cabinets and kitchen drawers and cupboards can be set up to only allow authenticated users to access them with biometric locks and providing parents and care workers with added peace of mind.

**IMPROVING SECURITY MANAGEMENT** - In multi tenanted building where people use not just the front door, washing rooms bike halls, mail rooms and communal spaces, biometric locks help security managers control which tenants have access to which area dependent on their individual requirements.

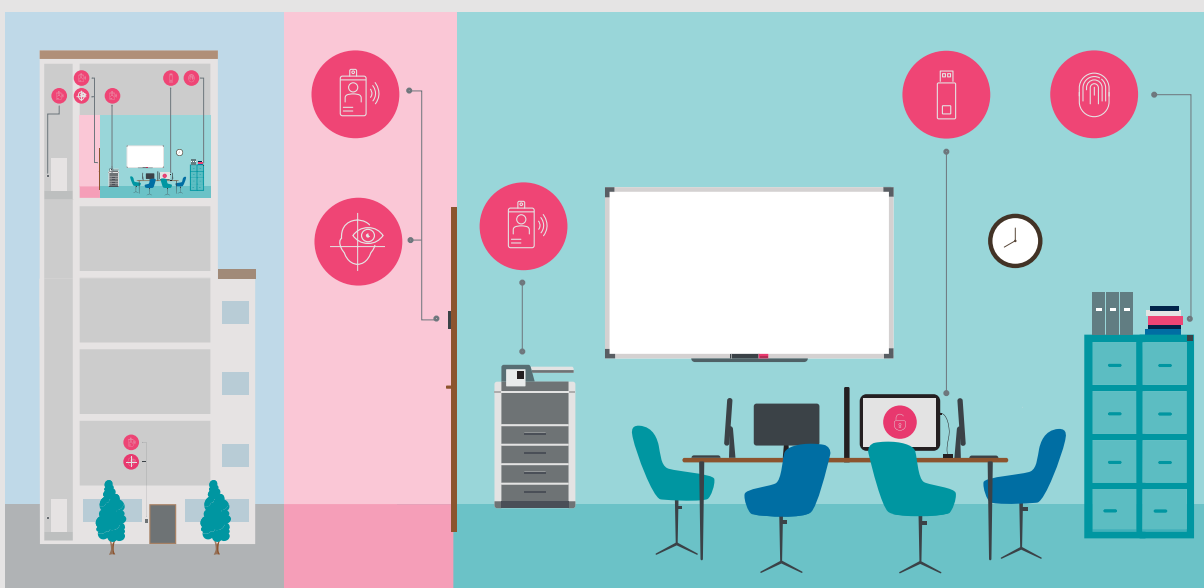
**DEFINE YOUR DESIGN** - A range of shapes and colors seamlessly integrate into any door lock design.

**ACCESS, EVERY TIME** - Discreet, slim and durable and works from any angle in less than 500ms up to 10 million times.

## BIOMETRICS IS THE KEY TO SMARTER WORKING

Protecting the workplace is a significant issue for many organizations, and over the last few decades new technologies have changed our offices. Flexibility is also key. Working from anywhere must be seamless, smooth and secure both for employer and employee to support increased remote working and the gig economy.

This has brought with it increased security and privacy demands. Businesses cannot rely on legacy security systems to secure both physical and digital office spaces, especially as 60% of hacking incidents involve the use of stolen credentials. The future of office security lies in biometrics.



### ENTER WORK & ACCESS THE RIGHT AREA

**Office doors, alarms & safes** – can be accessed and controlled with biometric solutions.



### KEEP YOUR PC PERSONAL

**PCs and peripherals** – to access devices and corporate apps and services.



### ENTER AND UNLOCK DIGITAL SPACES

**Access secure data environments** – such as the company server, encrypted USB storage devices and ensure secure and seamless connection to VPNs, controlled access servers and applications.



### WORKPLACE PERSONALIZATION

**Your settings** – or personal employee accounts can be enabled easily when using shared devices, such as printer system or “hot desk” computer.

## IN FOCUS – BIOMETRIC ACCESS CARDS

A range of different biometric form factors are already helping workplaces become smarter, managing access control, time and attendance, and much more. We're seeing one form factor gain significant momentum – the biometric access card.

Biometric access cards can be thought of as a multi-function key that can combine features such as an ID badge, access key, time and attendance and alarm control.

The benefits of biometric access cards are within easy reach for many organizations as they can be integrated into the existing access control system.

## BIOMETRICS... IN AN ACCESS CARD?



- 1. PRIVACY** Fingerprint data is stored in the card. Users control their own data. 100% GDPR compliant.
- 2. POWER** Ultra-low power consumption, even when active.
- 3. FLEXIBLE** Manage access rights and combine access with time tracking, alarm systems, ID badge and more. Works with existing contactless technologies.
- 4. PERFORMANCE** Small, thin and robust sensor. Authenticate from any angle in less than half a second.

## WHAT ARE THE OPPORTUNITIES?

### CARD MANUFACTURERS

- ➔ Bring innovation
- ➔ Increase market share
- ➔ Add features and functionality to existing card
- ➔ Offer a hygienic access solution
- ➔ Privacy compliant

### ENTERPRISES

- ➔ Secure & Convenient physical and digital access
- ➔ Hygienic and contactless, no tap on pin pads
- ➔ Enhanced privacy as data stored on device, card is personal
- ➔ Combine access with ID badge, time and attendance, alarm...
- ➔ Works with your existing infrastructure
- ➔ Reduce IT, admin and fraud cost
- ➔ Reduce concern and stress among staff

**BIOMETRICS -**

**PROVIDING A**

***WORRYLESS,***

**SECURE**

**WORK AND HOME**

**ENVIRONMENT**

# 05

The benefits of biometrics for access control



# THE BENEFITS OF BIOMETRICS FOR ACCESS CONTROL

Compared to other forms of authentication, biometrics provide choice, security and an intuitive user experience, bringing a range of benefits to device manufacturers, service providers and consumers alike. In addition you are always sure it is the right person that is granted access.

## HIGHLIGHTED BENEFITS



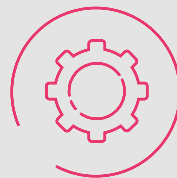
### EFFICIENCY

Low power consumption  
– 1,8 volt power



### SECURITY

Optimized features to maximize  
secure authentication



### FUNCTIONALITY

High image quality with  
optimized biometric  
performance



### CONVENIENCE

Enduring speed (<400ms) and  
minimizing false rejections  
(FRR 3%)



### RELIABILITY

ESD protection: +-15kv



### DURABILITY

Waterproof coating IP67,  
+10M touches



### HYGIENE

Enabling a contactless experience  
for a safer authentication



### PRIVACY

Offers enhanced privacy  
if local storage



# ABOUT US

## **TRUSTED COMPANY**

- Fingerprints solutions authenticate users billions of times per day
- Hundreds of millions of sensors shipped yearly
- Integrated in over 500 smartphone models

## **OUTSTANDING PERFORMANCE**

- Unrivalled low power consumption
- High image quality – optimized biometric performance for small sensors

## **ENHANCING DESIGN OPPORTUNITIES**

- Our small sensors and modules enable brands to be as creative as they like
- Ready for cost-effective, high volume production
- Largest fingerprint biometric supplier to door lock makers globally

THE HISTORICAL MILESTONE OF

# 1 BILLION SENSORS

SHIPPED WAS REACHED IN MAY 2019

**#1 GLOBAL  
BIOMETRIC  
SOLUTION PROVIDER  
IN DOOR LOCKS**

OUR PRODUCTS EXIST IN MORE THAN

# 100+

DIFFERENT ACCESS *DEVICES AND APPLICATIONS*

A photograph of a person's hands holding a pen over a document, with a watch on the wrist. The image is overlaid with a red gradient. The text is centered in the middle of the image.

FINGERPRINTS BELIEVES IN A SECURE AND SEAMLESS UNIVERSE,  
WHERE YOU ARE THE KEY TO EVERYTHING.

Fingerprint Cards AB (Fingerprints) – the world’s leading biometrics company, with its roots in Sweden.

We believe in a secure and seamless universe, where you are the key to everything. Our solutions are found in hundreds of millions of devices and applications, and are used billions of times every day, providing safe and convenient identification and authentication with a human touch. For more information visit our website, read our blog, and follow us on Twitter.

Fingerprints is listed on Nasdaq Stockholm (FING B).

Visit [www.fingerprints.com/solutions/access](http://www.fingerprints.com/solutions/access) for more information about our touch and touchless solutions for access control.

