FINGERPRINTS

ACCESS ALL AREAS

AN INTRODUCTION TO BIOMETRICS AND ITS VALUE TO ACCESS CONTROL

"Biometrics are well established in smartphones and as the ***IoT continues to expand,*** *their benefits are gathering momentum across a broad spectrum of other industries. The future will see biometric authentication deployed in a range of new areas –* ***letting end users access what's theirs.*** *From offices to apartments, suitcases to cars and data, biometrics are* ***set to make our modern lives easier*** *while improving security and usability."*

Thomas Rex, SVP BL Smartcard & Embedded, Fingerprints

TABLE OF CONTENTS

01

Biometrics 101

BIOMETRICS 101

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

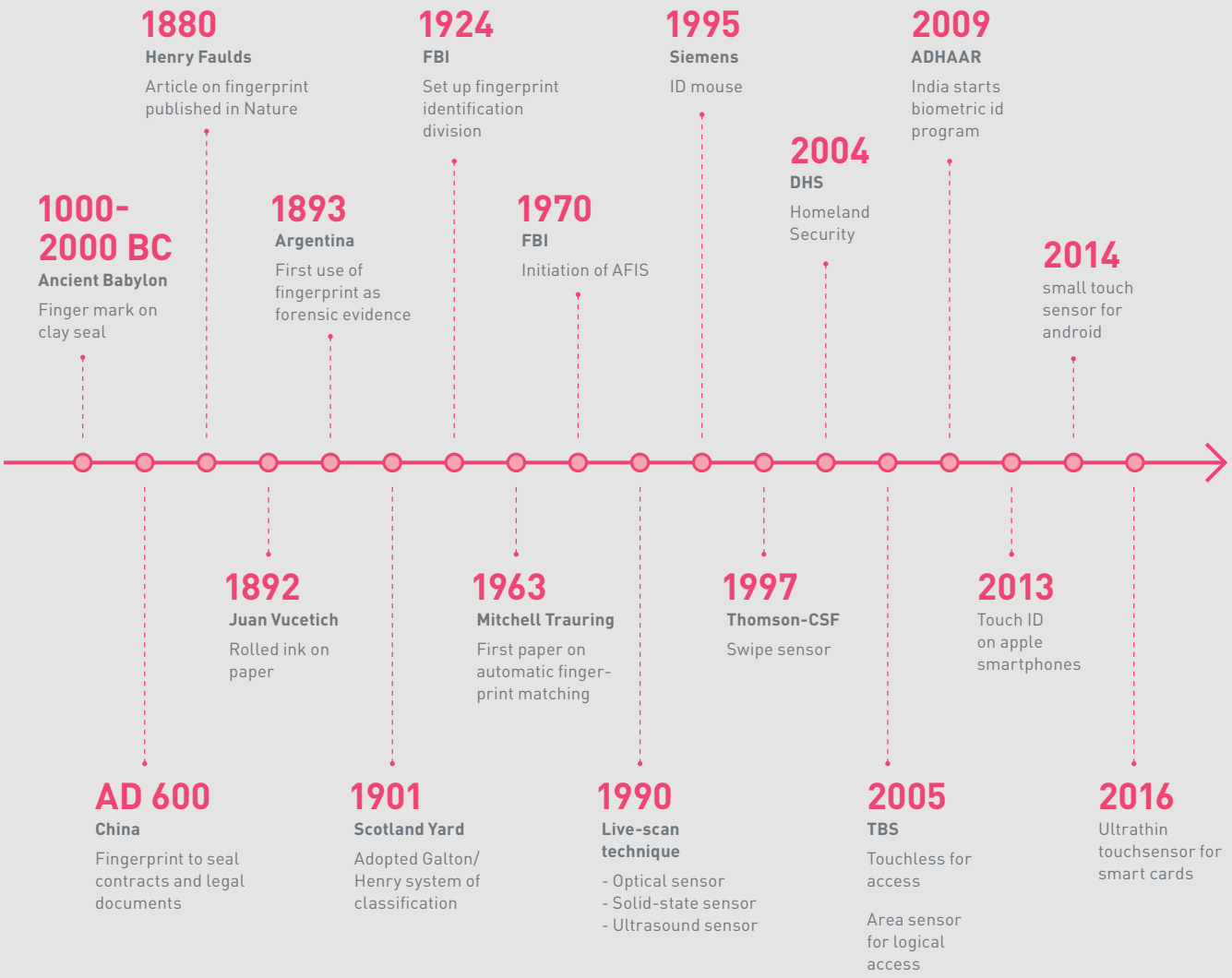
With so many activities needing fast, reliable and convenient authentication it is no surprise that identity verification has become a cornerstone of today's society, enabling secure interactions while preventing fraud and criminality.

BIOMETRICS – A POTTED HISTORY

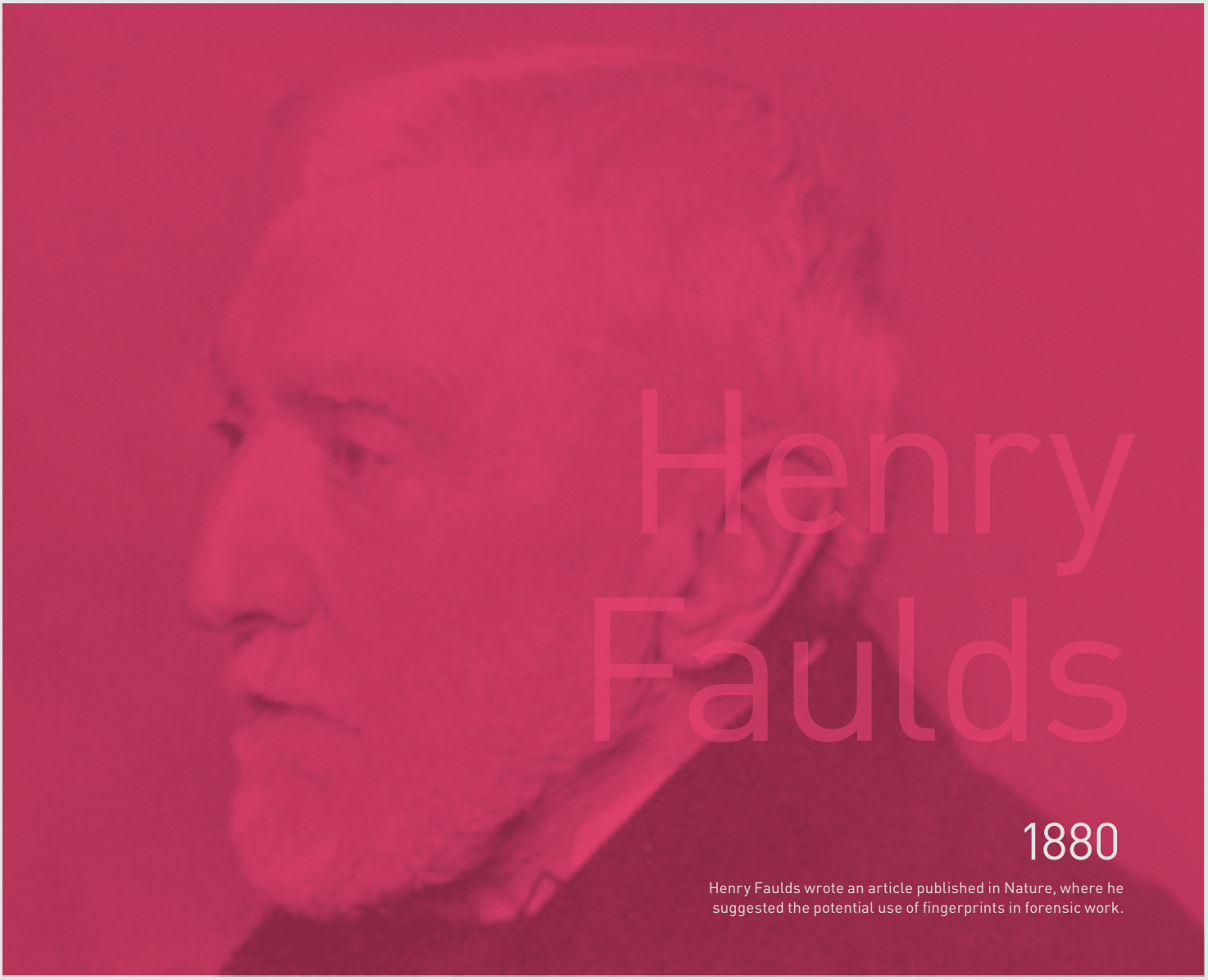
Using biometrics as an authentication method is not new as physical characteristics have always been used to identify people. There is evidence of fingerprints being used as a person's mark for Babylonian and Chinese business transactions as far back as 500 B.C. and 300 B.C. respectively. The late 1600s 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.

FINGERPRINT 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.**



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. 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?

When comparing biometric authentication with other authentication factors, several aspects come into play. Authentication based on knowledge factors (e.g. a password), is technically easy to implement but also relatively easy to break with computerized algorithms or with spyware in the user's device. Also, users tend to select simple and common passwords, even sharing them with others. This makes reliable authentication impossible.

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

POSITIVE

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

NEGATIVE

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

OTHER AUTHENTICATION

POSITIVE

KNOWLEDGE

- → Easy to implement

OWNERSHIP

- → Generally easier

NEGATIVE

KNOWLEDGE

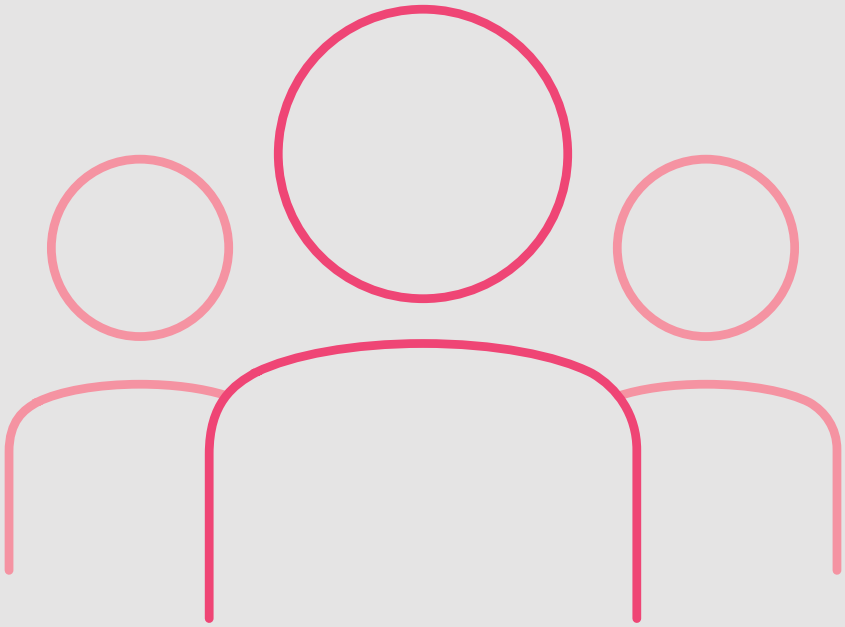
- → Easy to break computerized algorithms
- → Users tend to select simple and common passwords, even use the same one for office and for private and sometimes even share them with others. This makes reliable authentication impossible.

OWNERSHIP

- → Relies upon a physical token which are easy to loose or steal

These are key advantages making biometric authentication the preferred authentication factor in many applications. There are some drawbacks, though, including the convenience and social acceptability of some biometric methods. Also, depending on the type of biometric used, the cost, size and power requirements of the sensor and processing logic may be a potential drawback.

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

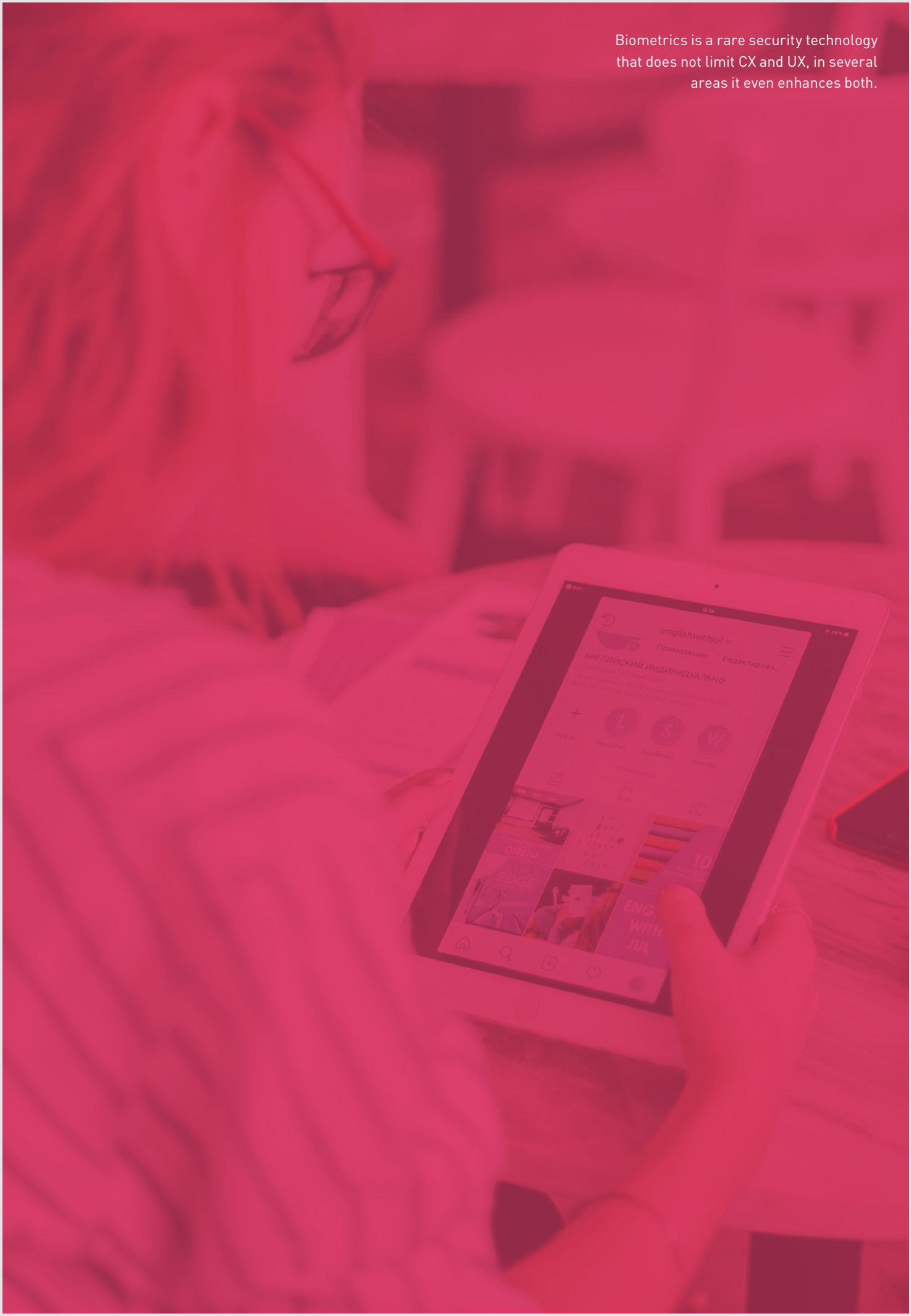


MARRYING SECURITY WITH CONVENIENCE

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 does not stop with 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.

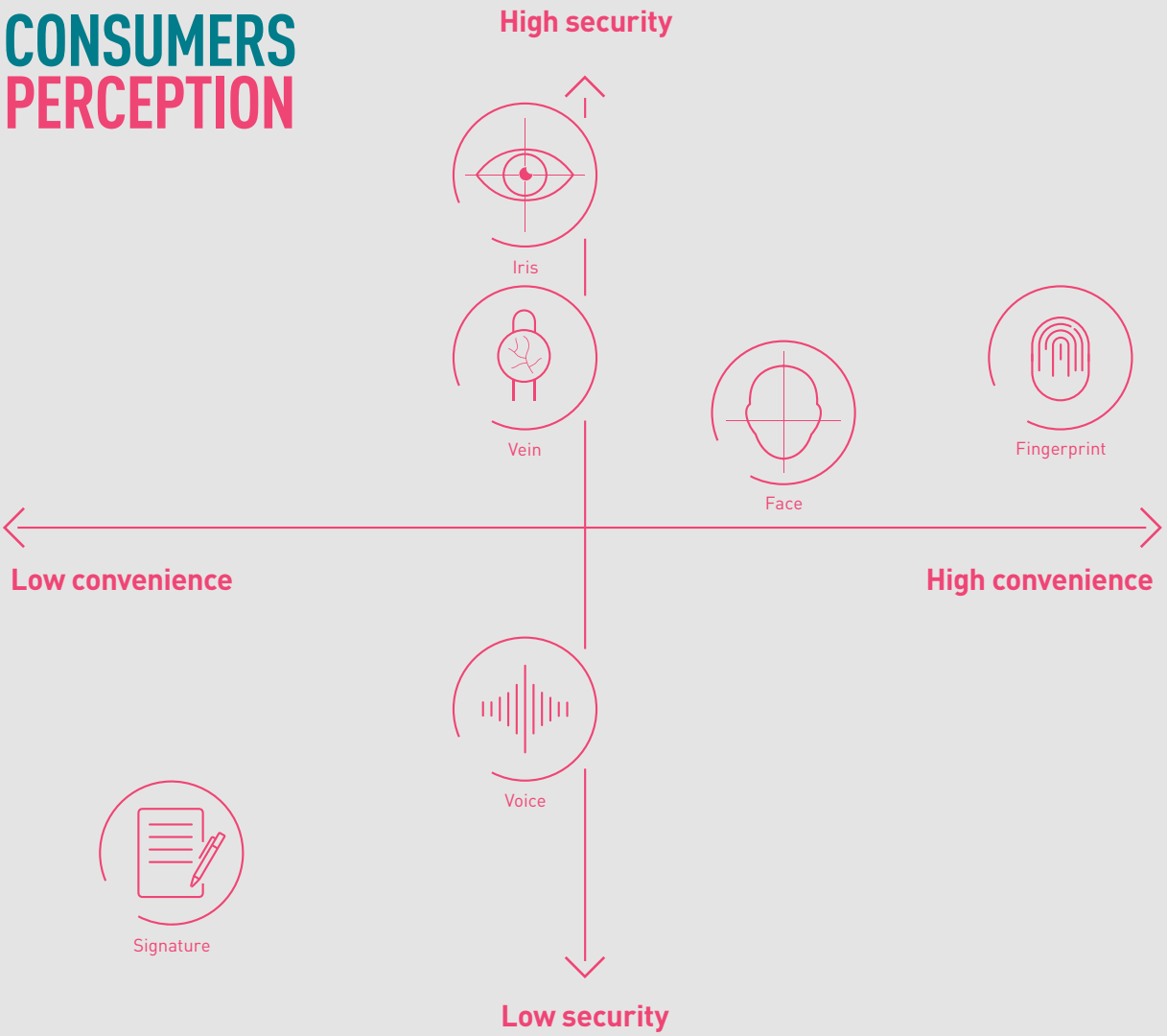
As an example of an anti-hacking measure used in today's modern consumer devices, a mathematical representation of the fingerprint is stored as a template, instead of the image itself. Storing the representation reduces hacking risks, since it cannot be used to re-create the original fingerprint image. 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.

Biometrics is a rare security technology that does not limit CX and UX, in several areas it even enhances both.



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.

CONSUMERS PERCEPTION



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

No system can be made 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.

FRR vs THE FAR

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.

But what kinds of biometric authentication are there, and **why has fingerprint risen to the top?**

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.

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

FINGERPRINT

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

Highly unique, easily collectable, measurable and usually permanent throughout a person's lifespan, there are also a number of standards already in place. This has made fingerprint the de facto modality to date, despite some finding it intrusive and challenges remaining when fingers are dirty or particularly dry/wet.

EYE

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

Similar to fingerprint, the characteristics of eyes are unique and permanent. In the past it has often been used in government use cases like border control, but with new advancements and simpler enrolment processes it is now being used in consumer devices like smartphones. It now also works in darker conditions and when wearing glasses.

FACE

Scrutiny of the many features of the face

Relatively low cost to implement with a camera or current smartphone technology, face recognition can be done over much larger distances than some other modalities. It can, however, be quite easy to spoof, requires good lighting and its low stability over time as the face changes can result in high failure rates. The latest 3D technology has improved security, but it comes with a high cost.

VOICE

Analysis of a person's voice print

While it is easy to implement at a low cost, there are major shortcomings. Voice prints change over time and require regular updates, they can also change due to factors like environment and illness, and voice prints can be easily recorded and spoofed. It is also worth considering the UX, as asking the user to speak can be both time consuming and inconvenient. Voice is perfect as a UI though, as it is a convenient and natural way of interacting with various devices.

VEIN RECOGNITION

Scrutiny of the vein pattern of fingers or hands

Vein is a highly secure method the vascular pattern lies under the skin. The scanners, however, can be quite large, expensive and require a lot of power. The matching process can also be quite slow as vein patterns are very complex making processing requirements very high.

BEHAVIORAL

Recognition of a person's gait or gestures

Accurate measurement of gait parameters requires sophisticated equipment, including several video cameras and load transducers which makes it costly and complicated to implement. Gestures can also be interpreted but is still in its infancy and security and spoofing concerns are yet to be addressed. Interestingly, it can also be used in the background as a second or third factor to increase security for use cases like online transactions, or in the future of shop & go stores.

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	●	●	●	○	○	●

● High ◐ Medium ○ Low

So, it is fair to say that companies looking to implement biometric authentication have several options, depending on their needs.

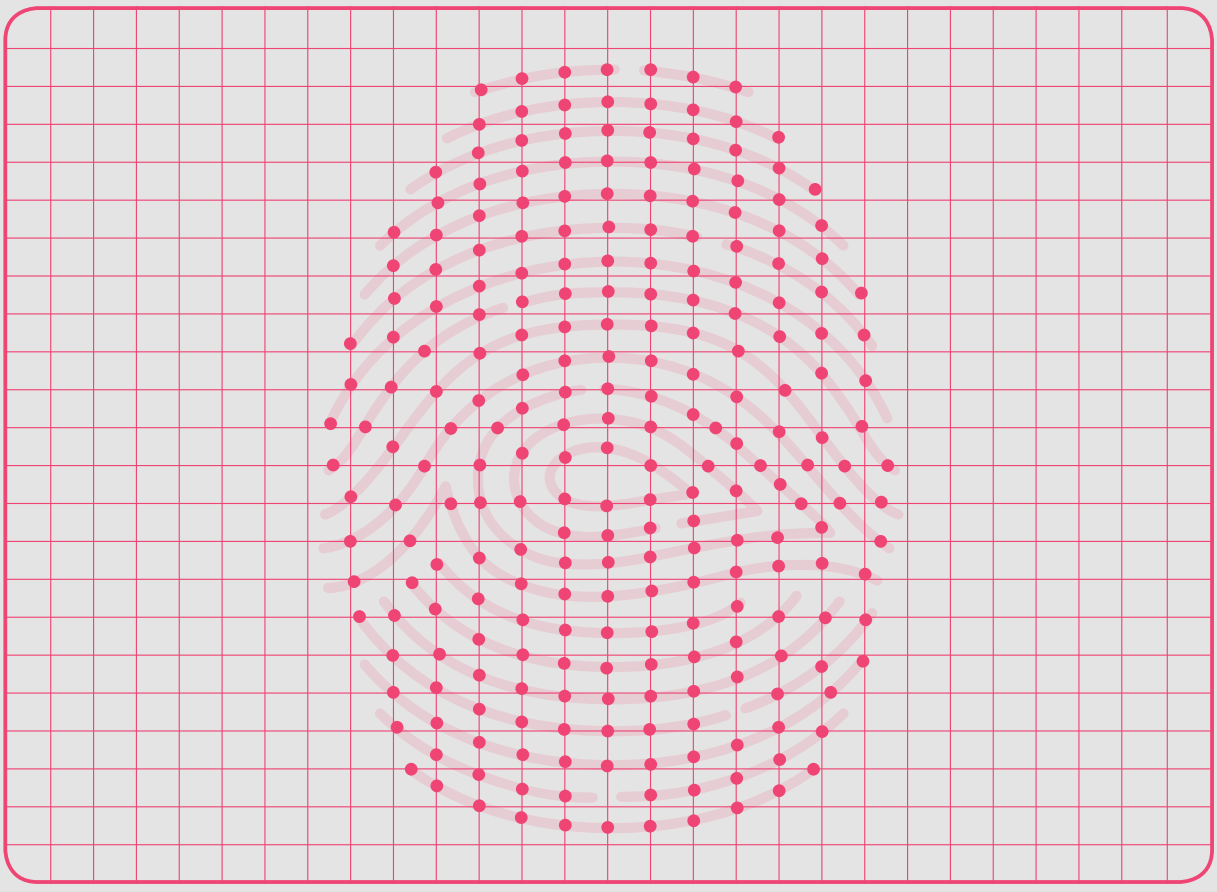
Fingerprint has risen to the top of the pile because of its position in the nexus between security and convenience. It is now a very stable technology that consumers are familiar with which makes it the ideal candidate to unify authentication across multiple device form factors.

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. With the ability to produce very small sensors, it is essential the enrollment and verification are done carefully with high quality software. This technology is hitting 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.

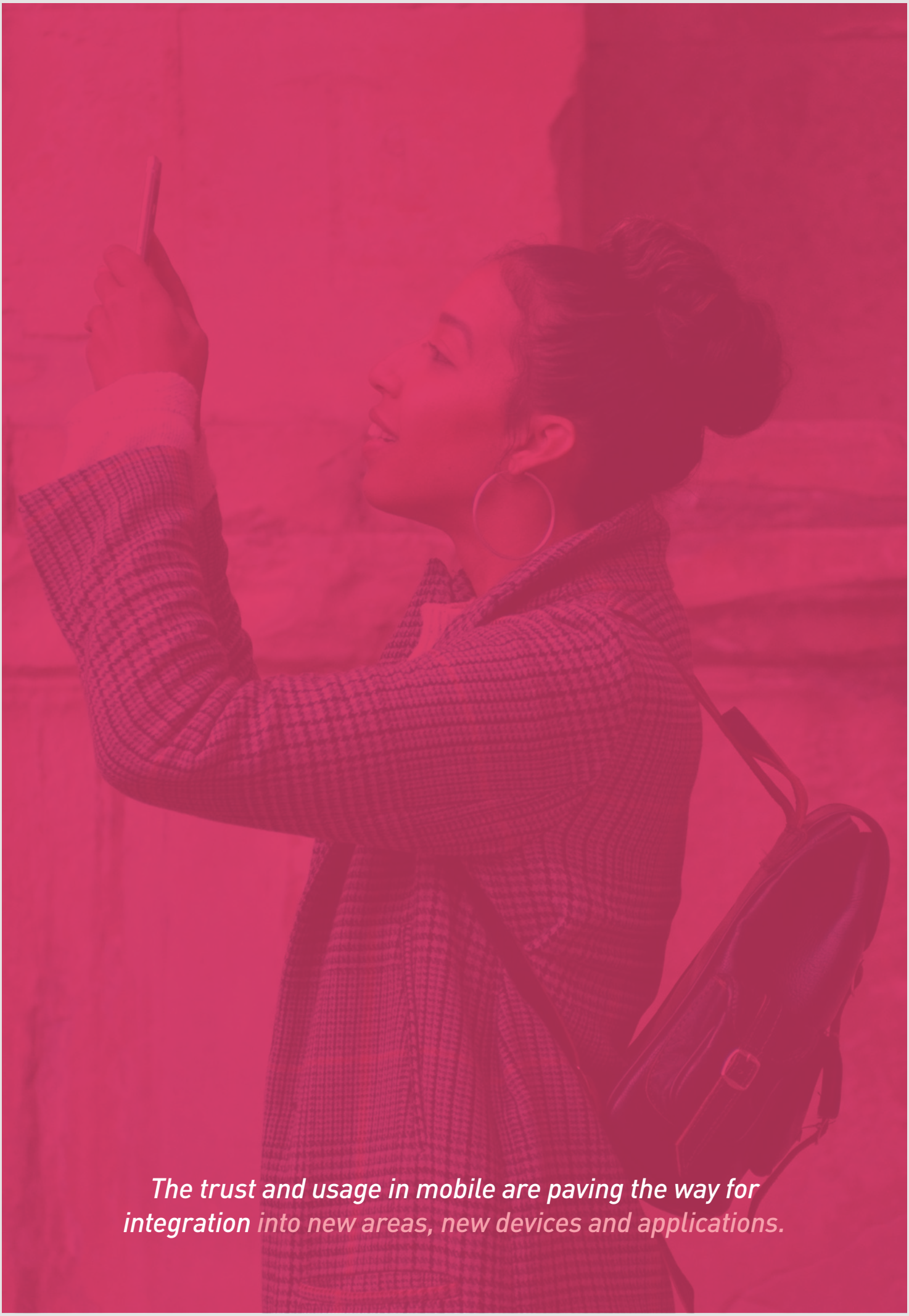
Limited adoption as they often have high power requirements, are not able to capture fine details, can be quite large, can't create 3D images and are sensitive to "wear and tear".

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

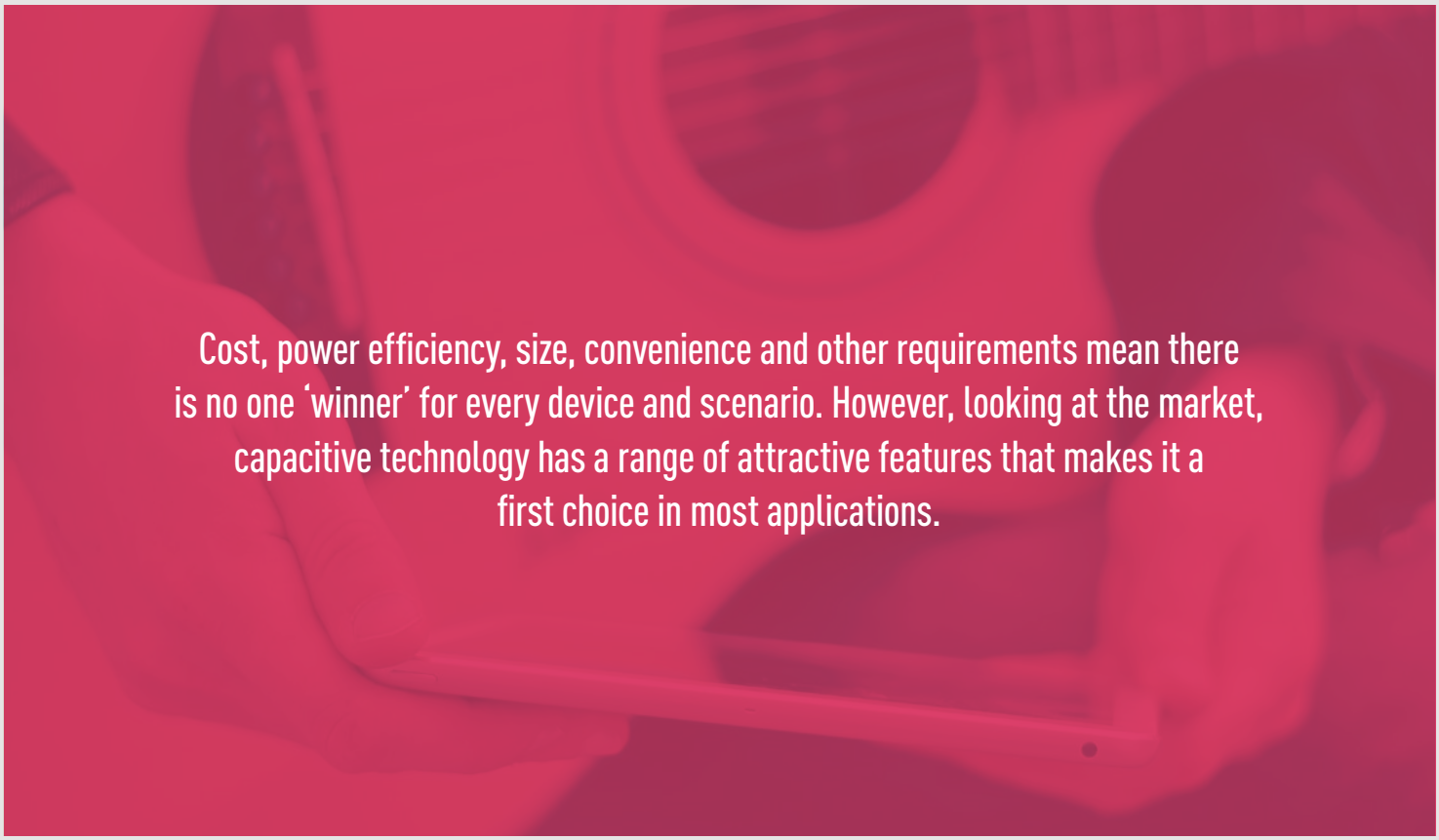
They provide more biometric information than most other fingerprint sensors and are good at reading wet and damaged fingers, but not dry fingers. They can be slow, expensive, power hungry, bulky and require a lot of processing power.

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



Cost, power efficiency, size, convenience and other requirements mean there is no one 'winner' for every device and scenario. However, looking at the market, capacitive technology has a range of attractive features that makes it a first choice in most applications.

FINGERPRINT TECHNOLOGY COMPARISON

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

High Medium Low

03

The success of fingerprint in mobile

THE SUCCESS OF FINGERPRINT IN MOBILE

Mobile devices are central to our daily lives. They are a hub for various services including travel, payments, emails and banking, as well as accessing and opening doors, cars and more. Each new use case involves increasingly sensitive information.

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.

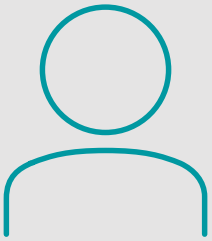
All of this has seen biometrics rise to the top as one of the best authentication solutions to raise mobile security hand in hand with convenience.

FINGERPRINTS HAS ACHIEVED HUGE SUCCESS IN MOBILE

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

>70%

of smartphones shipped have biometrics



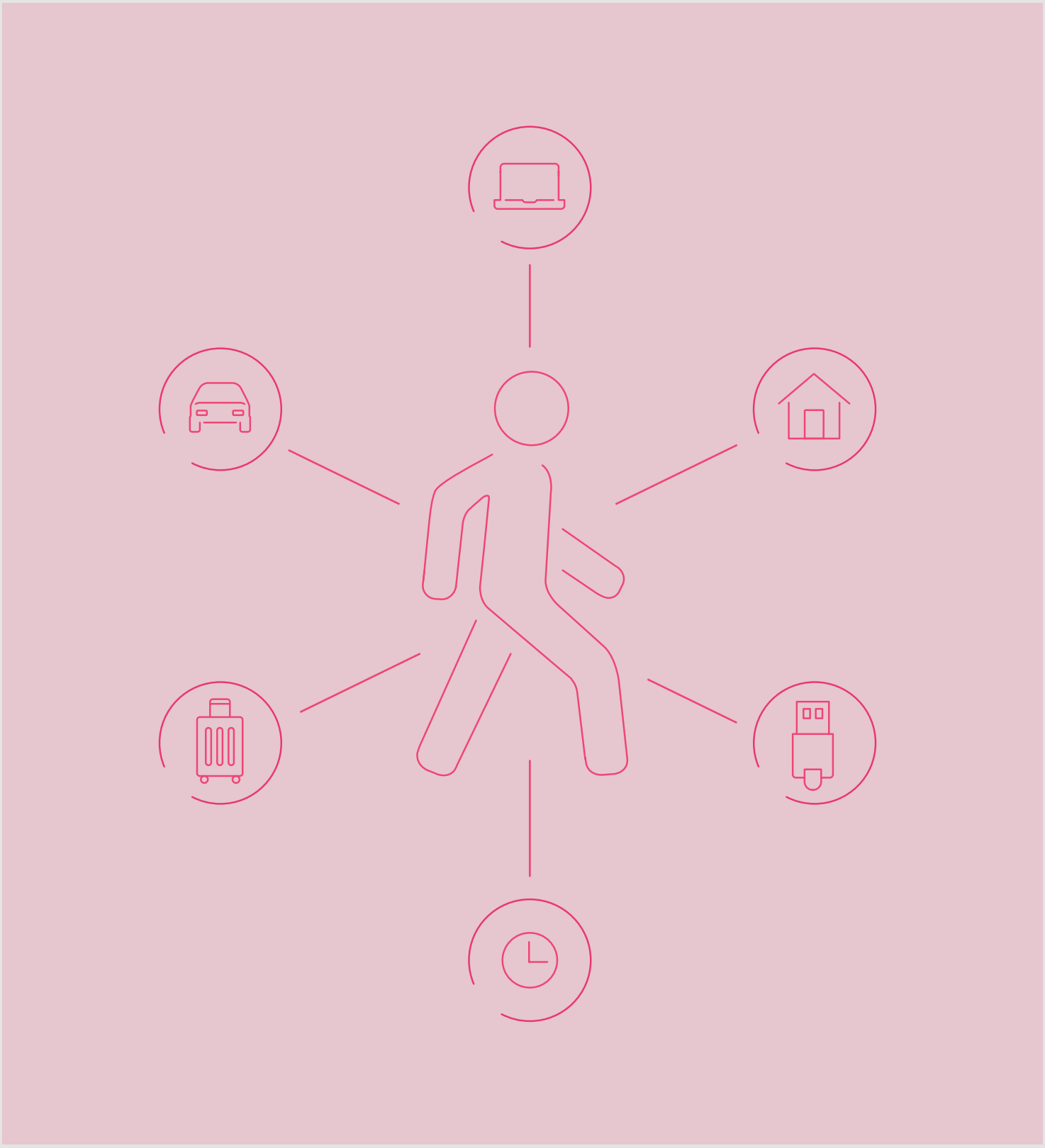
82%

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

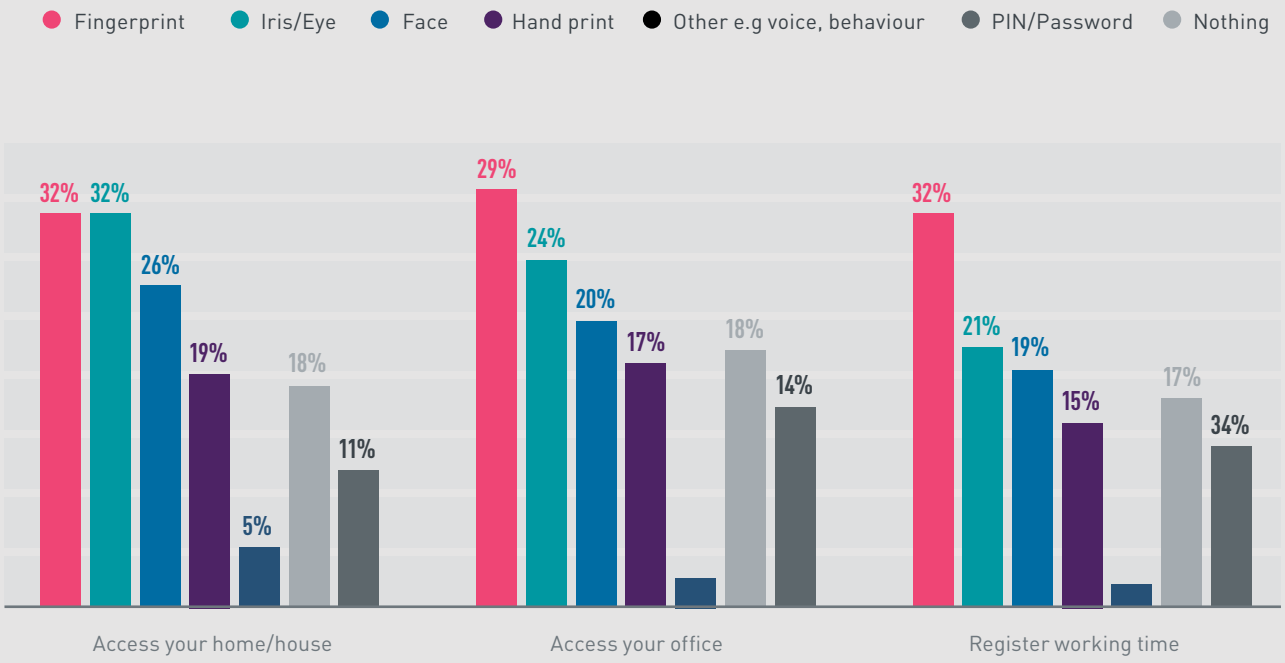
Fingerprint sensors are also expected to remain the number one authentication option, despite the other solutions – like iris scanners and facial recognition – that have been grabbing headlines.

Source: Fingerprints consumer research 2017

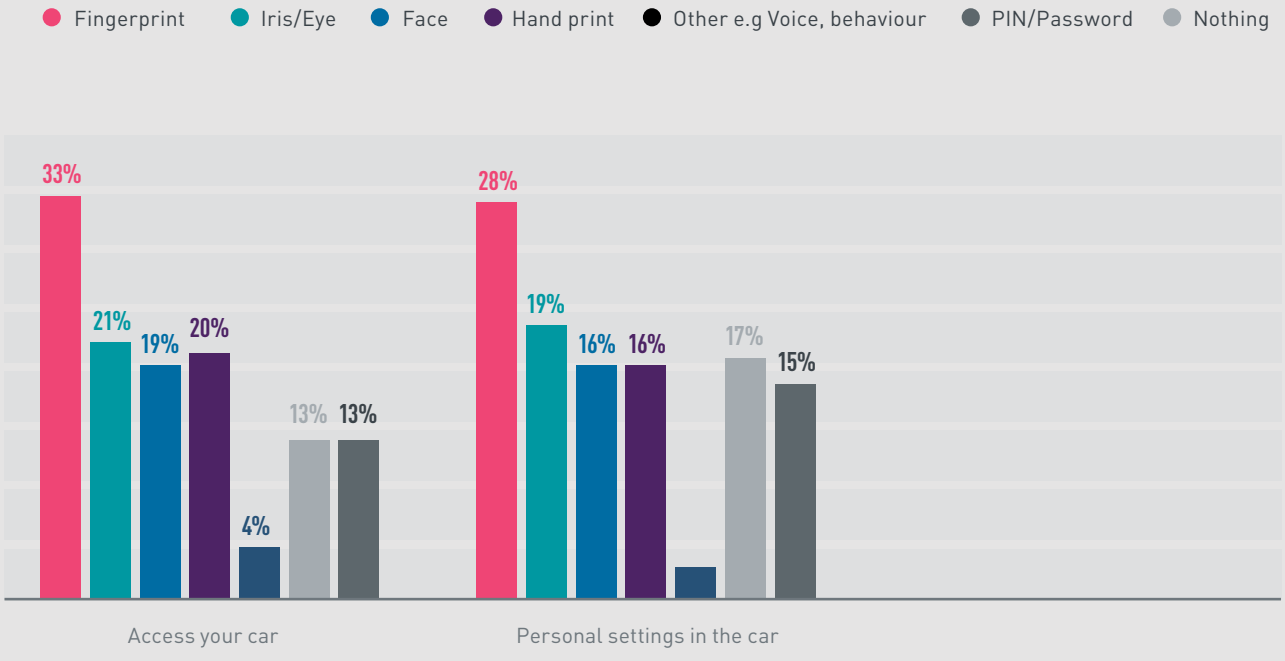
As the world becomes increasingly connected – consumers have also rated additional areas where they expect to see biometrics easing their daily lives.



Consumers want biometrics to access their things.



As this is considered convenient – no need to bring key or remember pin or password higher security and is a modern way forward.



Source: Fingerprints consumer research 2017

"BY 2020, THE IOT WILL REDEFINE THE CONCEPT OF "IDENTITY MANAGEMENT" TO INCLUDE WHAT PEOPLE **OWN, SHARE,** AND **USE".**

GARTNER


OWN
SHARE
&USE

chapter 04

04

Make things genius – use cases for access

MAKE THINGS GENIUS – USE CASES FOR ACCESS

The overall access control market is expected to grow from USD 7.5 billion in 2018 to USD 12.1 billion by 2024.*

IoT is changing the world around us, and so the way we access buildings, devices, applications, information and services must change also. As the number of connected devices grows, the need for seamless authentication is essential to remove the hassle of PINs, passwords, physical keys and tokens. Moreover with biometrics, you can ensure that access is granted to the correct person. This completely removes the threat of stolen PINs, ID cards and keys. With the range of devices and applications needing robust authentication becoming almost unlimited, and fragmented, we have identified a brief-selection of potential use cases on the next page.

* marketsandmarkets.com

DOOR LOCKS

Mini smart door locks – Improves the design of the home, provides the twin benefits of an improved aesthetic, with top-level security and convenience.

Digital door locks – A high-security fingerprint sensor discreetly placed on a handle. This design is more ergonomic and user friendly, providing a new way of entering a physical location.

Touch door locks – Designed for demanding weather conditions, the reader is installed on the outside of the door, with an indoor lock controlling unit. It works with mechanical lock bodies and is powered with standard batteries.

Once enrolled, it is not possible for someone to reverse engineer the fingerprint image from stored data.

CAR ACCESS AND SETTINGS

Connected Cars – Users can open their car, as well as personalize their settings with both touch and touchless authenticators enabling the benefits of physical and digital access.

TOKENS, DONGLES AND CRYPTO WALLETS FOR SIMPLE, STRONGER AUTHENTICATION

FIDO2 - Biometric secure token – The fingerprint module prevents any misuses of the token from people other than the authorized user and losing the key will cause no security risk at all. The embedded security chip is designed and developed to encrypt, store and protect fingerprint data.

Cryptocurrency wallets – Cryptocurrency owners can benefit from the increased levels of security and accessibility enabled by biometric-enabled cold/offline wallets. As a result, users can overcome many of the problems experienced in the secure storage of cryptocurrencies in recent years.

PROTECT AND ACCESS PERSONAL BELONGINGS

Smart suitcase – With a single touch, users can open suitcases within one second - no more keys or pins - making journeys elegant, easy, and even more fun!

LAPTOPS AND NOTEBOOKS

Usage of biometrics in new chrome – With just a touch of a button, users can both unlock computers alongside accessing apps and services.

REMOTE CONTROLS

Access and personalize the entertainment experience – Smart controller for devices and apps, a smart fingerprint button that turns your hand into a human remote control. By simply touching the button users can create shortcuts and control over 20 functions. The button automatically recognizes which part of the hand you are using to touch it and is an easy, fun way to control and interact with devices and apps.

AND MANY MORE!

"**The last five years have seen a rapid increase,** not only in adoption, but also in the range **of market sectors and targeted consumer activities.** Adoption of biometric technologies should continue to accelerate and expand across all user domains and market sectors".

Source: Current Biometric Adoption and Trends, Rachel German and K. Suzanne Barber, The University of Texas at Austin. September 2017.

chapter 05

05

The benefits of biometrics for access control

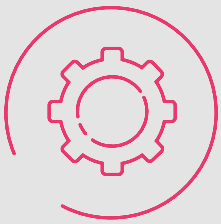
THE BENEFITS OF BIOMETRICS FOR ACCESS CONTROL

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.

HIGHLIGTED 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

ABOUT US

TRUSTED COMPANY

- → Fingerprints sensors authenticate devices billions of times per day
- → Hundreds of millions of sensors shipped yearly
- → Integrated in over 400 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

THE HISTORICAL MILESTONE OF

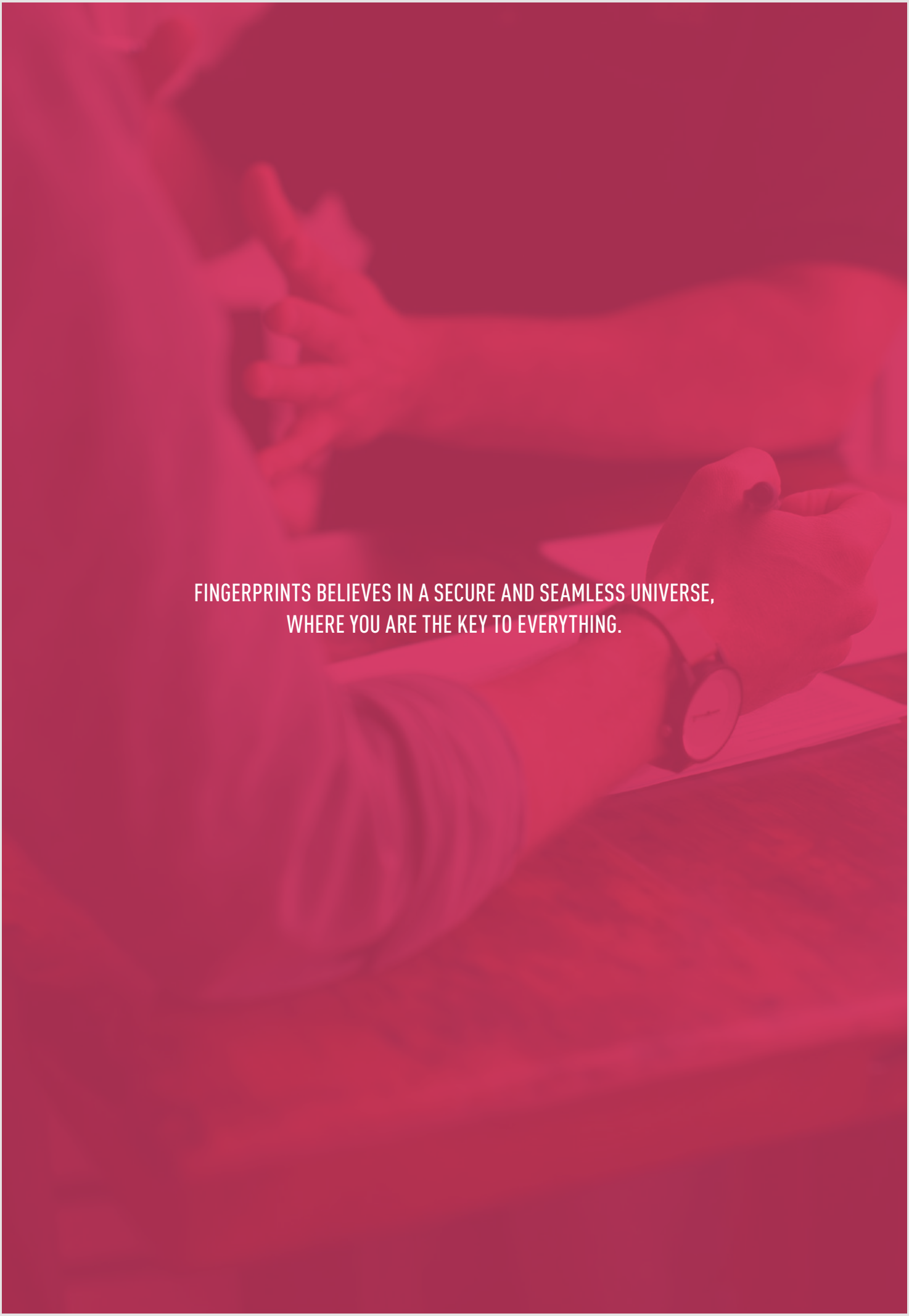
1 BILLION SENSORS

SHIPPED WAS REACHED IN ***MAY 2019***

OUR PRODUCTS EXIST IN MORE THAN

100+

DIFFERENT ACCESS ***DEVICES AND APPLICATIONS***



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** for more information about our touch and touchless solutions for access control.

FINGERPRINTS