



FINGERPRINTS

TOUCH, TAP, TRUST

MOBILIZING BIOMETRICS FOR PAYMENT CARDS

“It has taken time and incredible expertise to bring fingerprint sensors to payment cards. 2019 and beyond will see biometric cards rolled out by banks and financial institutions around the world, benefiting their business, merchants and consumers. Issuers need to understand the technology itself to make informed decisions, so that they give customers a card that enhances the buying experience, rather than hindering it.”

Thomas Rex, SVP Business Line Smartcards at Fingerprints

TABLE OF CONTENTS

CHAPTER 1	04
Biometrics 101	
CHAPTER 2	14
What makes fingerprint the king?	
CHAPTER 3	24
The success of fingerprint in mobile	
CHAPTER 4	28
Scaling down – adapting mobile tech for payment cards	
CHAPTER 5	32
Payment cards - The next use case	
CHAPTER 6	37
What’s next? Questions to ask your card partner	
ABOUT US	42
About us and our partners	

01



BIOMETRICS 101

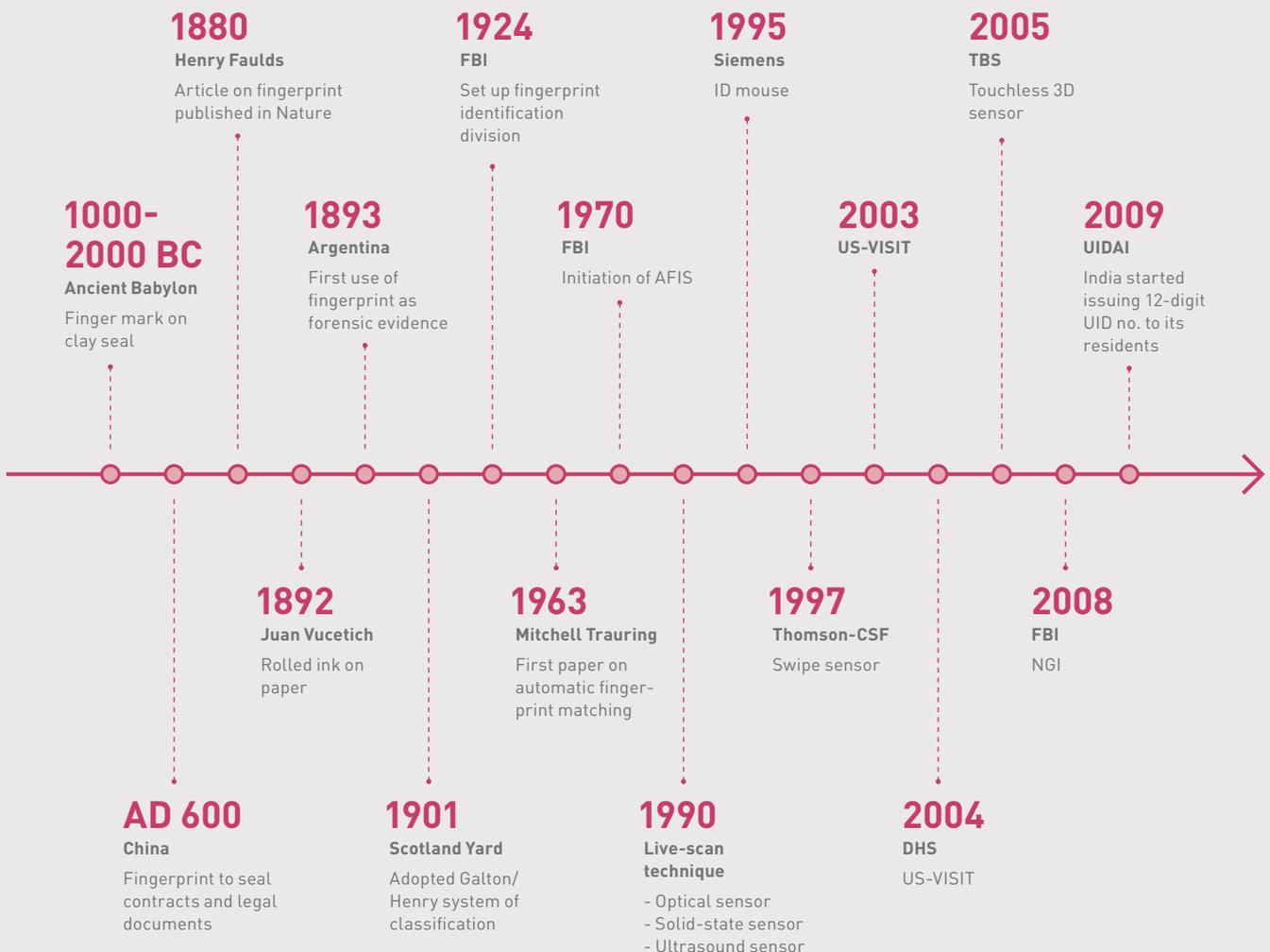
We constantly need to prove who we are. Locks need to be opened, devices need to be accessed and purchases need to be made – but it is essential that only authorized people can perform these tasks. With so many activities needing fast, reliable and convenient authentication it is no surprise that identity verification has become a cornerstone of today's society, enabling secure interactions while preventing fraud and criminality.

BIOMETRICS – A POTTED HISTORY

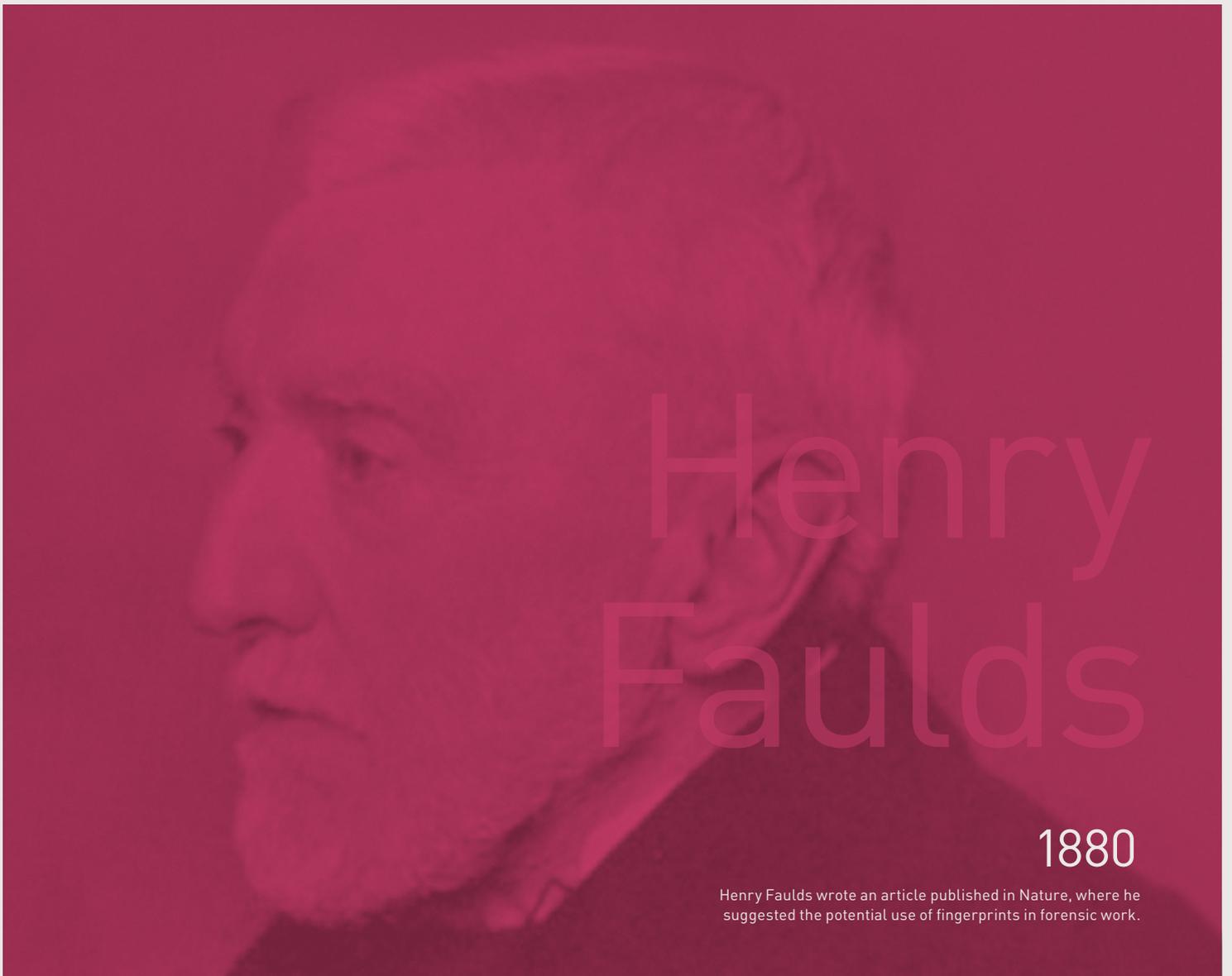
But using biometrics as an authentication method is not new as physical characteristics have always been used to identify people. There is evidence of fingerprints being used as a person's mark for Babylonian and Chinese business transactions as far back as 500 B.C. and 300 B.C. respectively. The late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



Henry Faulds

1880

Henry Faulds wrote an article published in *Nature*, where he suggested the potential use of fingerprints in forensic work.

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?

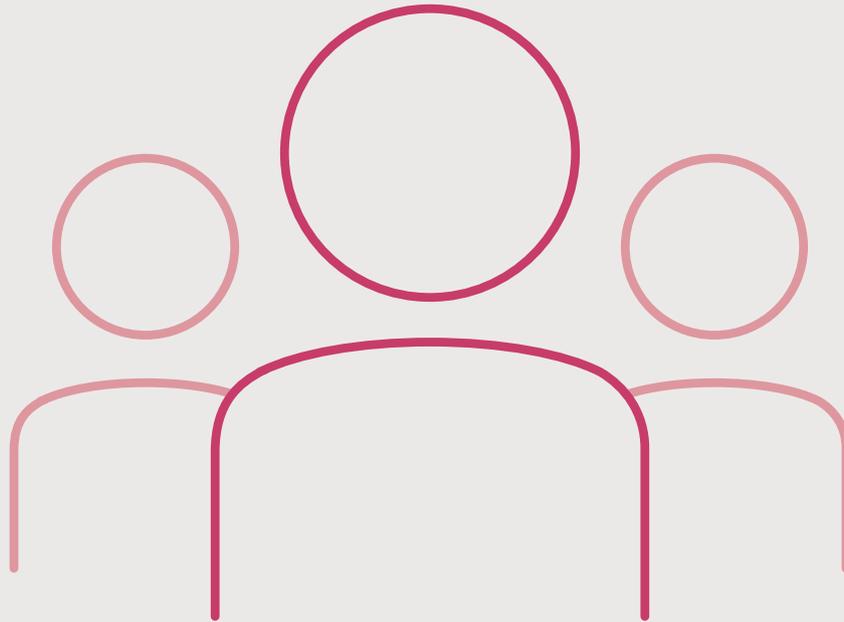
When comparing biometric authentication with other authentication factors, several aspects come into play. Authentication based on knowledge factors (e.g. a password), is technically easy to implement but also relatively easy to break with computerized algorithms or with spyware in the user's device. 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	OTHER AUTHENTICATION
<p>+ POSITIVE</p> <ul style="list-style-type: none"> → Unique to each person → Always with you → Does not change over time 	<p>+ POSITIVE</p> <p>KNOWLEDGE</p> <ul style="list-style-type: none"> → Easy to implement <p>OWNERSHIP</p> <ul style="list-style-type: none"> → Generally easier
<p>- NEGATIVE</p> <ul style="list-style-type: none"> → Social acceptability of some biometric methods. → The cost, size and power requirements of the sensor and processing logic 	<p>- NEGATIVE</p> <p>KNOWLEDGE</p> <ul style="list-style-type: none"> → 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. <p>OWNERSHIP</p> <ul style="list-style-type: none"> → 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.

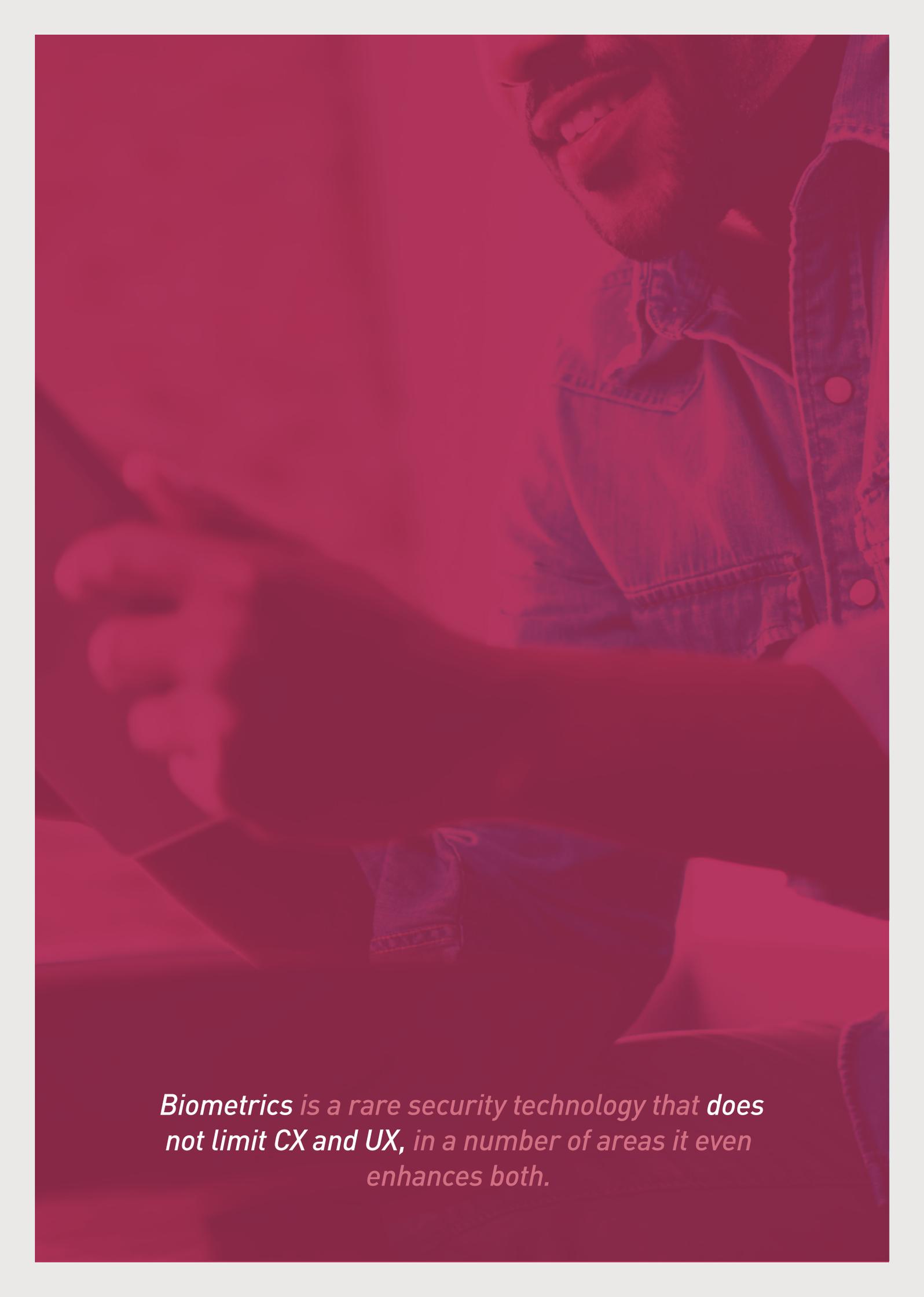
With correctly implemented biometric authentication the information needed is unique to each person, is always with them, and normally does not change over time.



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 have to include possible illegal access to the processing engine – hacking – and if it can be fooled by someone simulating the biometric identifier – spoofing.

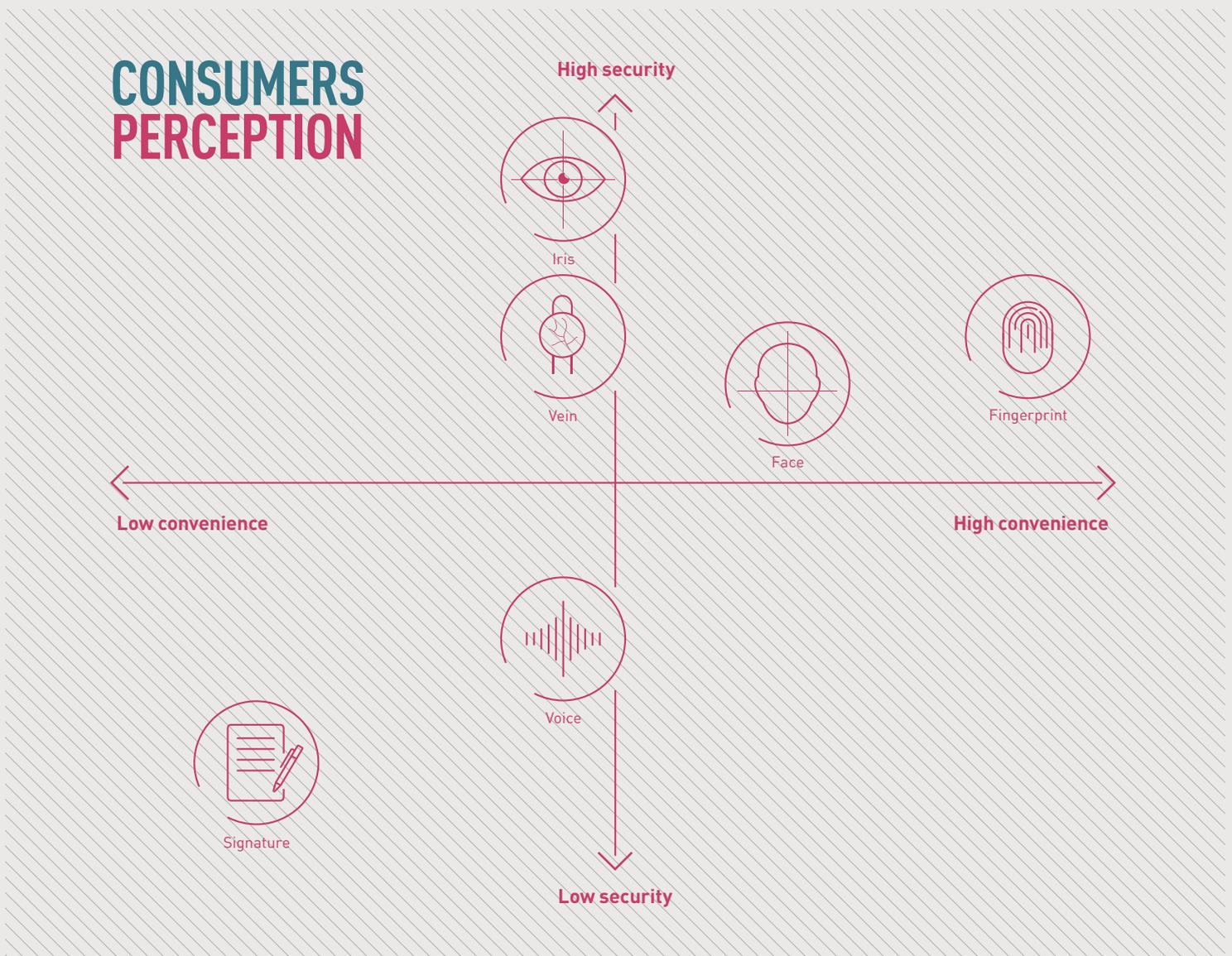
As an example of an anti-hacking measure used in today's modern consumer devices, a mathematical representation of the fingerprint is stored as a template, instead of the image itself. Storing the representation reduces hacking risks, since it cannot be used to re-create the original fingerprint image.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

Similarly, payment cards are equipped with a Secure Element, i.e. a chip that offers a dynamic environment to store, process and communicate biometric information securely. If you try to tamper with the chip in any way, it may self-destruct, but will not allow you to gain unauthorized access.

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.



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

No system can be made absolutely secure – with unlimited time (and money) you can hack and spoof anything. Advanced biometric techniques however makes 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.

FAR

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.

VS

FRR

False Rejection Rate

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

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 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

Highly unique, easily collectable, very 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

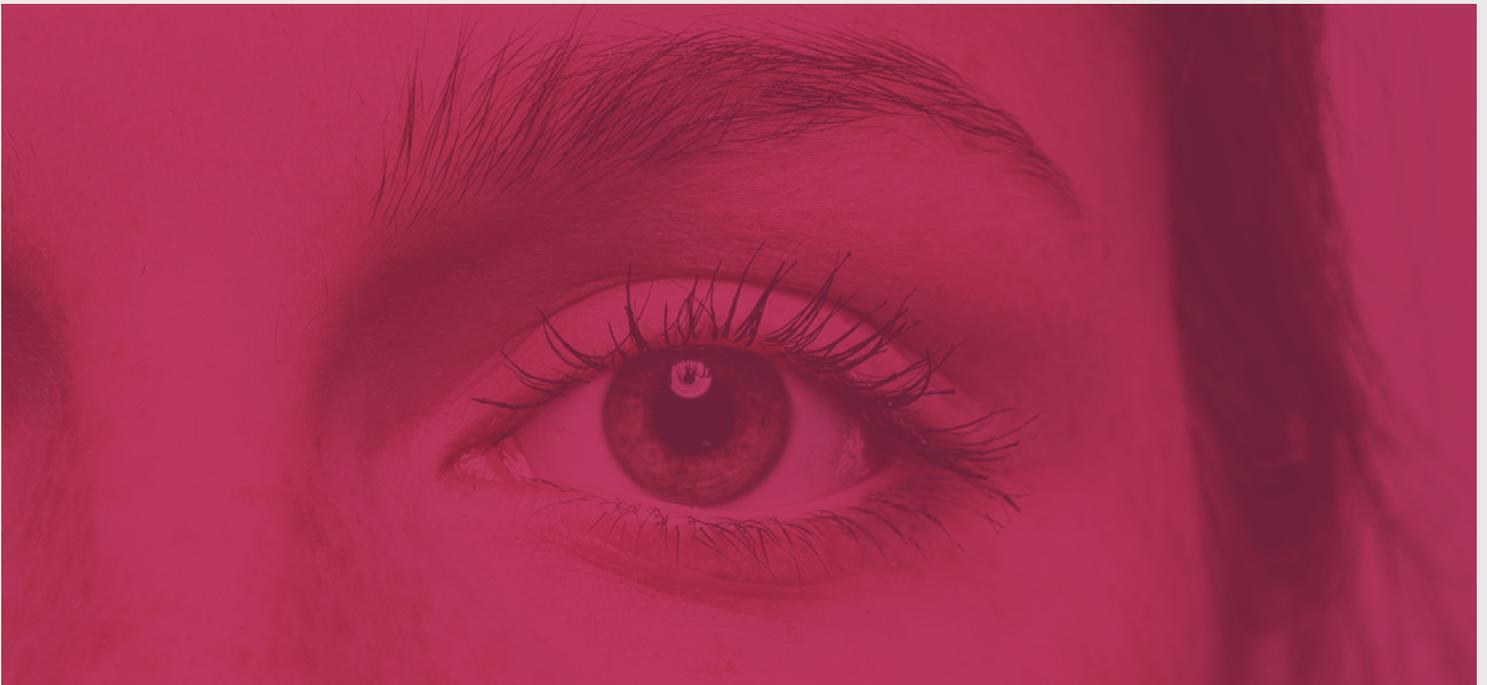
Similar to fingerprint, the characteristics of eyes are unique and permanent. In the past it has often been used in government use cases like border control, but with new advancements and simpler enrolment processes it is now being used in consumer devices like smartphones. It now also works in darker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

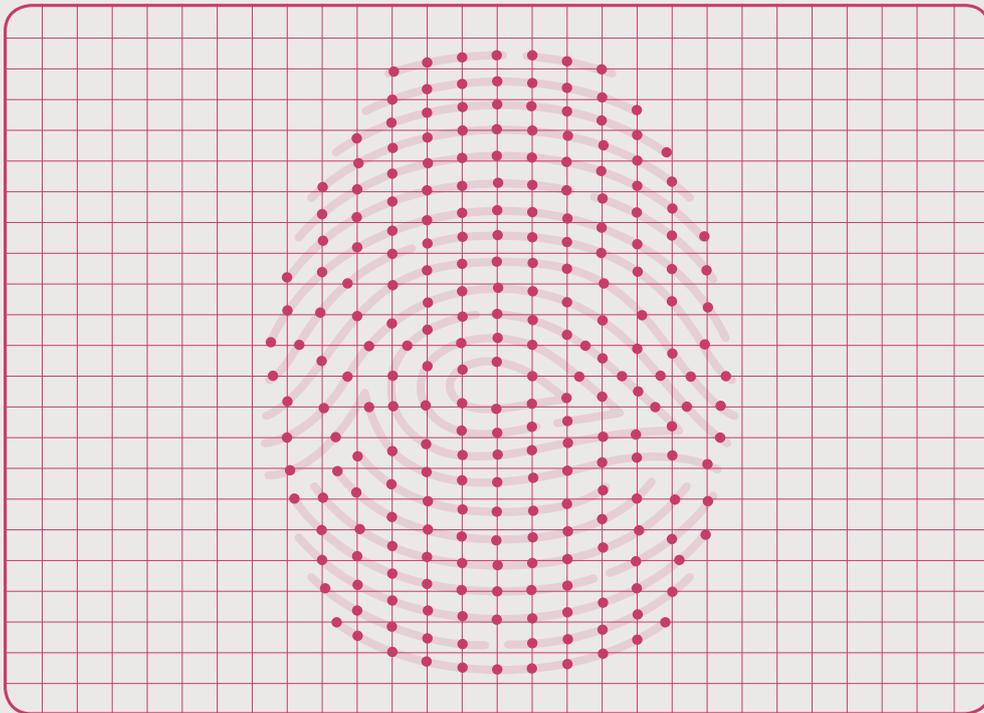
Fingerprint has risen to the top of the pile because of its position in the nexus between security and convenience. It is now a very stable technology that consumers are familiar with which makes it the ideal candidate to unify authentication across multiple device form factors.

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 fingerprint sensor to be 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.

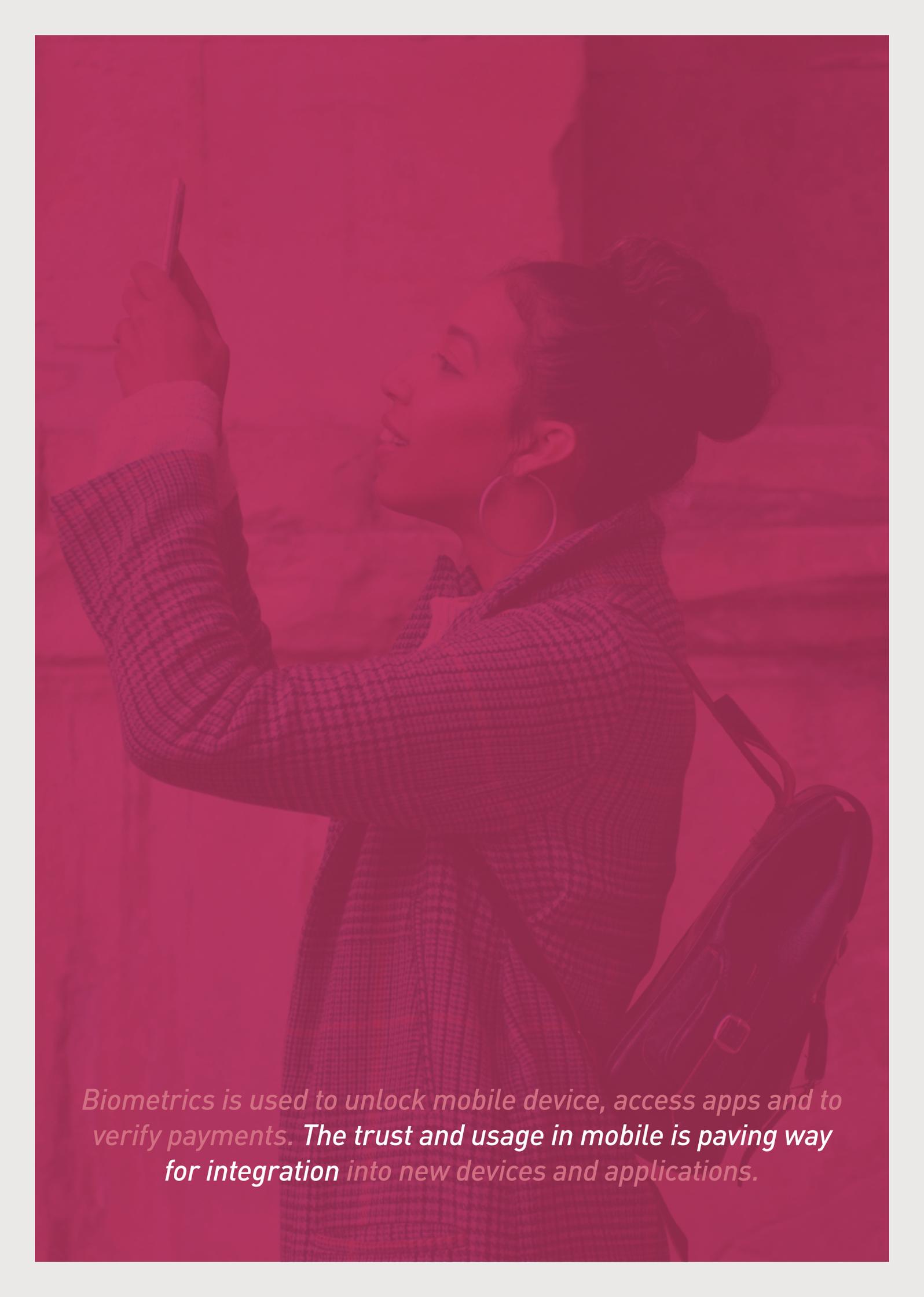
Limited adoption as they often have high power requirements, are not able to capture fine details, can be quite large, can't create 3D images and are sensitive to "wear and tear".

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.

A woman with her hair in a bun, wearing a plaid coat and large hoop earrings, is shown in profile holding a smartphone. She has a black backpack on her back. The entire image is overlaid with a semi-transparent red filter. At the bottom, there is a white text block.

Biometrics is used to unlock mobile device, access apps and to verify payments. The trust and usage in mobile is paving way for integration into new devices and applications.

TO ACHIEVE MASS MARKET ADOPTION, THE FOLLOWING CHARACTERISTICS ARE ESSENTIAL:



IMAGE QUALITY AND RESOLUTION

High quality images allow smaller sensors to be produced. Largely, this is possible with ultrasonic and active capacitive sensors.



SPEED

Operational speed has a direct correlation to convenience and user experience. Capacitive, thermal and pressure-based sensors can all be made to operate extremely quickly.



POWER CONSUMPTION

Low power requirements are fundamental for portable devices like smartphones and smartcards. Capacitive sensors currently have the lowest power consumption.



SIZE

Small sensors are more easily integrated into devices, and cost less. Active capacitive sensors allow the best compromise between size and image quality.



COST

Key factor in driving widespread adoption in cheaper phones, smartcards and other large volume devices.



PACKAGING AND DESIGN OPTIONS

Sensors must be able to complement the design of the device and active capacitive sensors offer the most flexibility. As they have smaller footprint they leave more room for the design ID and can be integrated into very small devices like a card or wearable.



SECURITY AND CONVENIENCE

Finding the right balance is key to ensuring strong authentication is usable. Active capacitive sensors can deliver low false rejection and approval rates.

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				
Design flexibility				
Technology maturity				
Security				
Convenience				
Power efficiency				
Mobile device adoption				

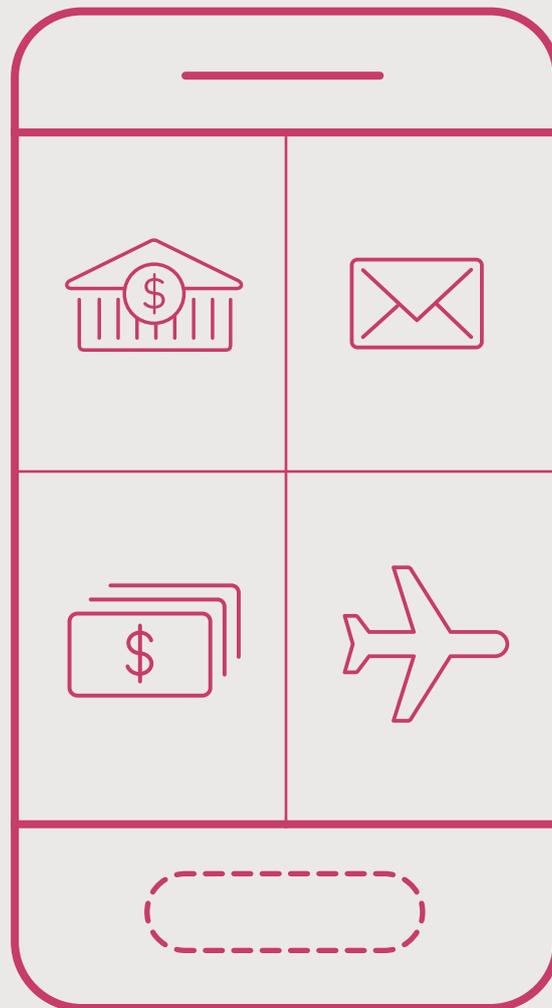
High Medium Low

03



THE SUCCESS OF FINGERPRINT IN MOBILE

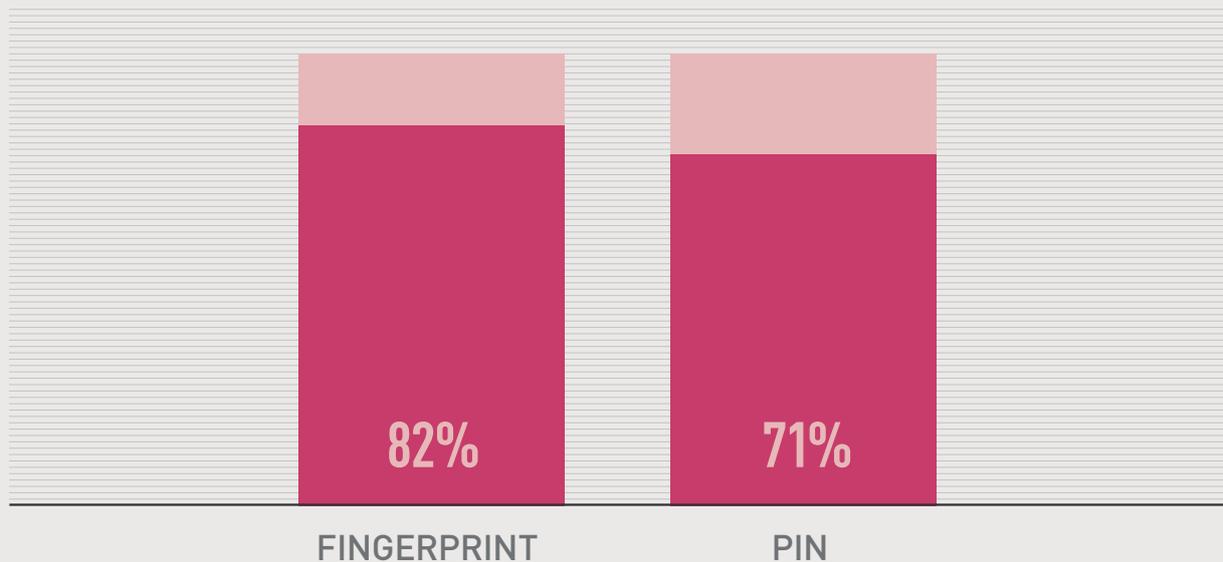
Mobile devices are central to our daily lives, but they are no longer just for calling and SMS. We now use them for travel, payments, emails and banking, and with each new use case comes even more sensitive information.



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. Indeed, research suggests that more than 70% of all smartphones shipped in 2019 will feature a fingerprint sensor, which could total in excess of 1 billion.

FINGERPRINT IS NOW MORE USED THAN PIN WHEN AVAILABLE ON THE SMARTPHONE



76%
of smartphone owners use the fingerprint sensor on their mobile

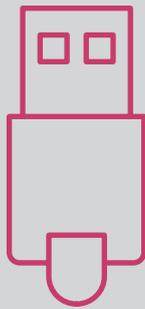
23%
Use biometrics for mobile payments

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.

NEW PAYMENT USE CASES

We have established that fingerprint recognition is the predominant modality – and that capacitive sensors offer the most flexibility in terms of size, security, convenience, power consumption and cost – it is therefore unsurprising that new devices are integrating capacitive sensors.

As strong authentication becomes ever more important on-device, in-store and online more devices can benefit from supporting a biometric sensor.



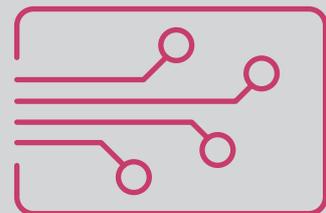
USB DONGLES

Bring strong physical authentication to online purchases and services



WEARABLES

Protect device unlock and wearable payments with a touch



SMARTCARDS

Bring trust to contactless payment cards and scrap the payment cap

These use cases and more are **already integrating fingerprint sensors**. Biometric payment cards can bring huge benefits to consumers, banks and retailers alike.

04



SCALING DOWN – ADAPTING MOBILE TECH FOR PAYMENT CARDS

Fingerprint is, of course, the only viable biometric authentication medium that is workable for plastic payment cards because of size, power and other limitations. But it has been a long road to get here. Mobile biometric systems were too big, thick and power hungry to be integrated into smart cards and a huge amount of R&D has gone into scaling the hardware and software down.

Because of the unique requirements of smartcards, the following needed to be considered and addressed:

01. MANUFACTURING PROCESS

To ease adoption, it was key that the integration of a fingerprint sensor did not significantly impact standard card manufacturing processes. We therefore designed a sensor module that can be easily supported by current machinery.

02. SYSTEM-ON-CARD

For maximum security and privacy, it was important that all template storage, processing and matching took place on the card itself, an approach that is already widely accepted in the ID world.

03. SENSOR SIZE

It took a lot of work to get a sensor thin and small enough to work perfectly in a plastic card. But we have also pushed hard to enhance the quality of the sensor itself so that we can reduce the footprint on the face of the card, maximizing room for branding and design.

04. HARDWARE FLEXIBILITY

Smartphones don't bend (yet!), but cards do. In fact, they must pass vigorous quality and flexibility testing. This is where our revolutionary T-Shape™ design comes in.

05. IMAGE QUALITY

To get the best possible image, hardware and software must work in perfect harmony. Getting this right finds the sweet-spot by getting the best image possible with the smallest sensor in the fastest time using the lowest power. It's all about the best UX with the lowest false rejections possible.

06. LOW POWER CONSUMPTION

Everything has to work as precisely and quickly as possible using only power borrowed from the payment terminal so there's no need for battery in the cards. We have therefore optimized everything to work with the lowest power output available from some terminals. If there's more power available, our algorithms run even faster!

07. SOFTWARE QUALITY

People often focus in on the hardware, but the software is where the real magic happens. Fraud prevention, image enhancement, intelligent updates of the templates – the quality of the software is the difference between tap&go and tap&slow.



08. LOW LATENCY

Shoppers don't have time so having a processor that needs to boot was not an option we were willing to consider. Our sensor is always in standby and ready to go.

09. SECURE CONNECTIVITY

The secure element and fingerprint sensor are distinct units but security is fundamental so we have worked hard with our partners to ensure the secure connectivity meets the same levels as in the smartphone world.

10. ENROLMENT

There can be no one way to enroll, banks have different preferences and so do consumers. It was therefore essential that a number of enrolment options have been considered to bring flexibility, and the process has been carefully considered to make it as easy as possible for cardholders.

Our vast experience in the mobile space has enabled us to look at every aspect of the biometric system and optimize it for use on payment cards. In fact, some aspects of the hardware and software are now so advanced that we are not yet using them to their full potential. This will be valuable in the future.

05



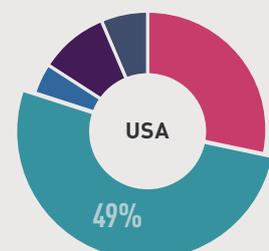
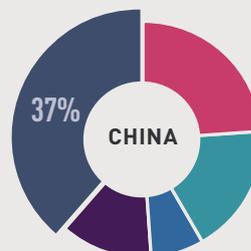
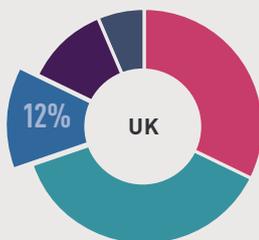
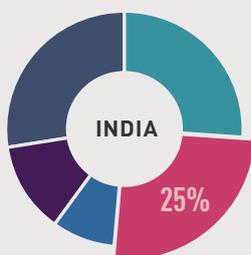
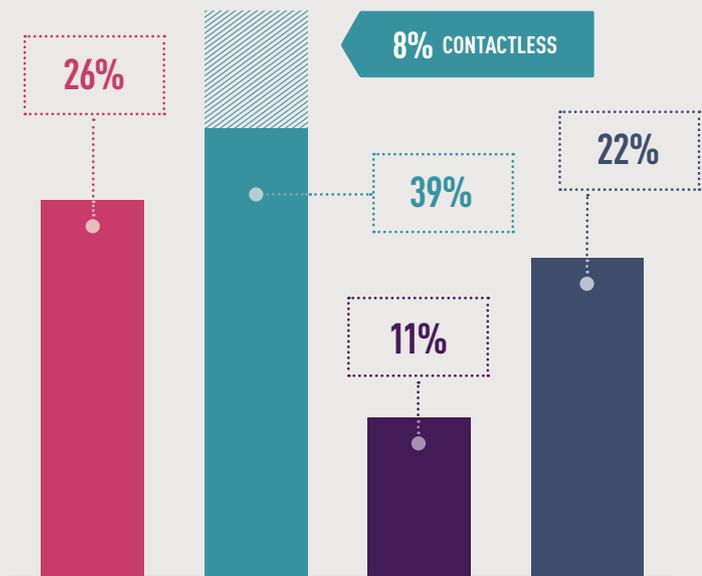
PAYMENT CARDS – THE NEXT USE CASE

Cards remain the most popular way to pay across the world, and their use is growing year on year – despite the option to now pay via smart-phones. 80% of consumers have debit and/or credit cards and nearly 3.5 billion payment cards are sold annually, half of which are contactless. However contactless has a low share of weekly purchases given current caps and limited infrastructure. Visa and Mastercard mandates all merchants to accept tap & pay in most regions as of 2019 which likely will see the share increase.

WEEKLY PURCHASES

Split between methods

- Cash
- Contactless & debit/credit card
- Online payment
- Mobile payment



Source: FingerprintsTM in collaboration with Kantar TNS. Base: 4,000 online consumers in China, India, UK, USA

But contactless adoption still faces challenges, with 38% saying that contactless does not feel secure and 51% very concerned about fraud.

Happily, the technology is now available to bring biometrics to payment cards. This gives consumers all the speed and convenience of contactless payments, with the added confidence and security of biometric authentication.

But what are the benefits?

SCRAP THE PAYMENT CAP

The £30 (UK), €25 (France) and \$100 (Canada, Australia) payment limit on standard contactless cards can be another barrier to sales. The higher level of security on biometric payment cards means this cap could be lifted.

Consumers will welcome the increased convenience of contactless for every purchase, combined with the reassurance of biometric authentication. Which is likely to increase both spend and throughput for merchants and other businesses such as restaurants. Consumers spending more on debit/credit cards is also good news for banks' revenues.



COOL NEW CARDS, SAME TERMINALS

In regions where the latest technology is prized as a status symbol, biometric payment cards have a natural appeal.

In other regions, the advanced technology will enable banks to increase their status and consumer trust by showing they're at the cutting edge with a cool new technology. A more positive financial experience will benefit the consumer, while also helping banks to attract new customers and retain existing ones.

Importantly, this technological advancement doesn't come at a cost for retailers, as there's no need to upgrade their existing contactless-enabled POS terminals.

GREATER FINANCIAL INCLUSION

Chip and PIN cards, or those needing a signature, can also present a problem for a variety of people, including those who:

- ➔ Are illiterate
- ➔ Use a different set of numerals
- ➔ Struggle to remember PIN codes

Biometric payment cards overcome this because the cardholder only needs their fingerprint to prove their identity.

There's the opportunity for banks to increase financial inclusion by providing these cards to people who can't use other kinds of authentication. Financial services can be accessed by a new consumer base for the very first time, meaning small businesses and retailers in previously low-access areas will see on-card spending increase at an unprecedented rate.



SECURE SELF-CONTAINED DATA

Stored in the card's secure element are:

- ➔ Template of the cardholder's fingerprint
- ➔ Personal and account details
- ➔ Matching engines that check the fingerprint presented at payment is authentic.

Consumers keep hold of their biometric data rather than a third party storing it. And if they lose the card, their data remains safely encrypted in the secure element where no one can use it.

NO BATTERIES OR TERMINAL UPGRADES

Energy from the payment terminal powers the card's biometric sensor. The card doesn't need batteries or recharging and can be used with existing terminals designed for contactless or chip-based payments.



CAN BE USED GLOBALLY

Payment schemes ensure the card works securely and meets today's EMV and ISO standards. So a biometric payment card issued by a bank in one country can be used to make payments safely in another country.

EASY AUTHENTICATION AND PRODUCTION

Embedded in the card is an ultra-thin, low-power fingerprint sensor. You can touch this from any angle, so authentication is fast and simple. Manufacturing biometric cards is straightforward too as the sensors are integrated using existing manufacturing processes.

06

What's next? Questions to ask your card partner



QUESTIONS TO ASK YOUR CARD PARTNER

With so many options, banks need a way to qualify the best technology for their needs. Here is a list of questions for banks and financial institutions ask their card manufacturer to ensure they get the best tech for their risk profile and customers.

GENERAL

- Can I see a live demo of the product in action?
- What trials and pilots have been conducted globally and can you share feedback?

HARDWARE

- Do you offer a silicon based sensor? (These offer better quality and 3D images – aim for 500+ dots per inch)
- Is your sensor active capacitive? (The best compromise of cost, power efficiency, size, convenience and more)
- Do you offer a system-on-card solution?
- How small is the sensor? (Smaller sensors leave more room for your brand)
- Does the processor need to boot up or is it always ready? (This limits latency, increasing speed and convenience)



SOFTWARE

- How quick is the verification process? Should be under one second
- What is the FRR of the product? Aim for under 3%
- What security measures does the product offer?
- What are the enrolment options for in-bank or at home?
- How many touches does enrolment need? (this makes getting up and running easier for the user)
- Does the algorithm learn each touch or is enrolment static? (This can limit false rejections)
- Does the software support 360° fingerprint recognition? (The right fingerprint should be recognized, no matter the angle)

WHHA

T'S

NE

X T ?

WHAT'S NEXT?

It has taken time and incredible expertise to bring fingerprint sensors to smartcards for uses like payments. Everything is now in place. 2019 and beyond will see biometric cards rolled out by banks and financial institutions around the world, benefiting their business, merchants and consumers.

Regardless of the use case, issuers need to be able to evaluate the different technologies available to them so that they can make informed decisions that will bring maximum benefits to them and their customers. What kind of sensor is best for our requirements? How effective is the fraud prevention software? What are the enrolment options? What additional functions is available that maximize the everyday usability? All of this impacts the quality of the product and the user experience and, if these do not meet consumer requirements, adoption will be slow and money wasted. Biometrics can unify secure customer authentication across all forms of payment, it is simply a matter of choosing the right method.

ABOUT US & OUR PARTNERS



FROM SMARTPHONE TO PAYMENT CARD

Over 30 leading brands have integrated our sensors in more than 330 smartphone models. Beyond this our solution is also integrated in various innovative IoT devices used for secure authentication and payments. We've adapted this hugely successful technology with our unique T-shape sensor module, tailor made for payment cards. Thin and small, it offers high image quality with optimized and proven biometric performance for smaller surface areas such as a payment card. And with best-in-class low power consumption it enables contactless authentication without a battery. Our sensors can be made cost-effectively and at high volumes with standard card production processes. They can also be laminated, so there's no compromise to a card's design.

HOW WE'RE MAKING BIOMETRIC PAYMENT CARDS A REALITY

The potential of on-card biometrics is huge, but we can't make it happen alone. We're collaborating with a wide range of representatives from the payment ecosystem (illustrated below), which each have a vital part to play.



BIOMETRICS LEADERS

Like Fingerprints are leading the way. Using our expertise with high-volume smartphone sensors, we're driving forward innovations to take biometric payment cards to the mass market.



SOLUTION PROVIDERS

Like NXP, Zwiipe, Linxens, CardLab are adapting and developing components including secure elements, prelams and inlays to fit the new requirements.



CARD MANUFACTURERS

Like IDEMIA, Gemalto and Kona-I are developing and manufacturing biometric payment cards and other smart cards, and are working with card issuers.



PAYMENT SCHEMES

Like Visa and Mastercard and bodies like EMVco and Eurosmart are working to ensure technologies are interoperable, secure and stable for a standardized, sustainable industry.



ISSUING BANKS & LARGE RETAILERS

Are sharing their requirements to ensure they have the right product for their customers.



CONSUMERS

Are using biometrics increasingly more in daily life* and are looking for the same level of authentication for payment cards, without compromising on speed or convenience.

* An average smartphone user unlocks the phone about 100 times per day, for many biometrics has replaced the PIN already

