FINGERPRINTS

ACCESS YOUR SMART HOME

ACCESS THE RIGHT AREAS

SMART HOMES

Connectivity and the Internet of Things (IoT) is making our homes smarter, bringing with it new levels of convenience and smart living. Connectivity, however, brings new ways of thinking about security and access control.

The balance of convenience and security offered by biometrics is well placed to help make a smart home smarter.

SECTION 01

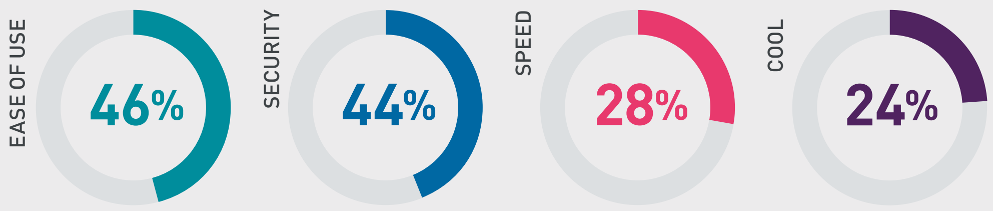
WHY BIOMETRICS?

01

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

In today's connected world we are required to prove who we are many times each day, which can be a burden. Smart homes bring an opportunity to do better.

With so many activities needing fast, reliable and convenient authentication, it is no surprise that consumers increasingly demand seamless and secure interactions.



Top consumer drivers for biometrics

Today there is a broad variety of biometric technologies available to address this need, with fingerprint recognition being the most widely used.

SOURCES: Fingerprints in collaboration with Kantar, 4,000 online consumers in UK, USA, India, China

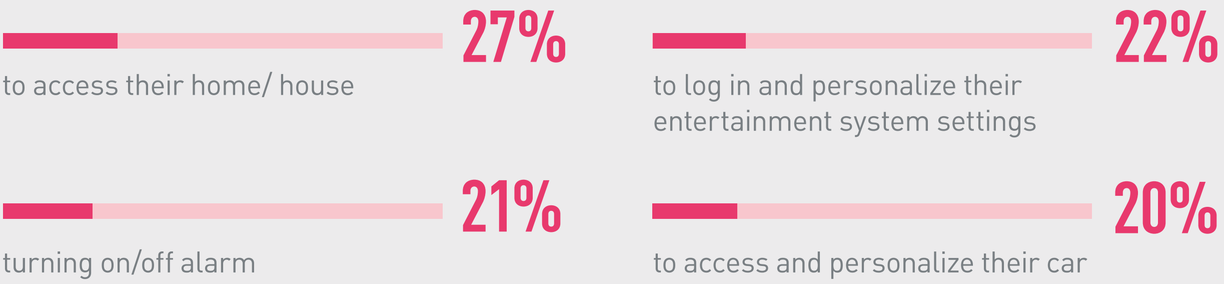
THE PROBLEM WITH PASSWORDS

Although PINs and password are easy to implement, they can be hacked through data breaches, spyware, algorithms or even social engineering techniques like shoulder surfing.

As the number of connected systems in our homes grows, consumers cannot be expected to create, remember and manage a growing list of passwords and PINs.

- *60% of consumers feel* they have too many to remember[1]
- Often, consumers have as many as *85 passwords and PINs* to manage across all their personal and professional lives[2]
- *41% of consumers* admit to reusing the same password or injecting minor variations, risking scalable attacks by hackers if just one password is compromised[3]
- *60% of hacks and data* breaches are a result of stolen credentials such as PINs and passwords[4]

CONSUMERS *WANT BIOMETRICS* TO ACCESS THEIR THINGS



SECTION 02

THE SECURITY AND CONVENIENCE BALANCING ACT

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

Balancing a system's security must take into account how well the biometric identifier can be read and matched with how secure the solution is and how well it prevents unwanted access, hacks and spoofs.

SOURCES: Fingerprints in collaboration with Kantar, 4,000 online consumers in UK, USA, India, China
1. www.fingerprints.com (click to see full link) 2. https://financesonline.com (click to see full link) 3. www.fingerprints.com (click to see full link) 4. www.idagent.com (click to see full link)

ANTI-HACKING MEASURES:

- A mathematical representation of the fingerprint is stored as a template, instead of the image itself.
- Removes the incentive for hacking as it cannot be used to re-create the original fingerprint image.
- The template is stored, and the algorithms involved in the authentication process run in a Trusted Execution Environment (TEE) or Secure Element (SE), keeping data away from threats.

ANTI-SPOOFING MEASURES:

- Increasing the image quality and by using sophisticated matching algorithms.
- Using more than one biometric identifier
- Increasingly sensitive sensors.

No system can be made totally secure – with unlimited time (and money) it is possible to hack and spoof biometric systems. Advanced biometric techniques however make such malicious attacks extremely expensive and time consuming.

MEASURING CONVENIENCE AND SECURITY

FALSE REJECTION RATE (FRR)

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 (FAR)

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 balance between security and convenience. The ideal biometric solution has minimal FAR as well as FRR.

SECTION 03

FINGERPRINT SENSORS: THE STANDARD BEARER FOR BIOMETRICS

03

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.

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

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

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 andand 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.

Fingerprint has risen to the top because it is increasingly familiar amongst consumers and provides an optimum balance between security and convenience, making it ideal for robust and frictionless authentication.

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.

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

SECTION 04

MAKING A SMART HOME GENIUS WITH BIOMETRICS

Smarter access at home whether it is a single house or a residential building. Energy meters, multimedia, lighting and security systems... connected devices are transforming our domestic lives. Biometrics can bring new levels of protection and convenience, unlocking the next generation of smart home.

GROWTH OF SMART HOME SECTOR

	2021	2025
Household adoption of smart home systems[1]	12,3%	21,4%
Value of smart home sector[2]	$78,3bn	$135bn

SOURCES: 1. Statista 2. Research and Markets Smart Home Market Global Forecast to 2025

MANAGING YOUR HOME SYSTEMS

Home alarms and electronics such as remote controls and multimedia systems – all controlled and personalized with a single touch.

CAR ACCESS AND SETTINGS

Unlock your car and it automatically adjusts to your personalized settings.

PROTECTING VALUABLES

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

KEEPING PCs PERSONAL

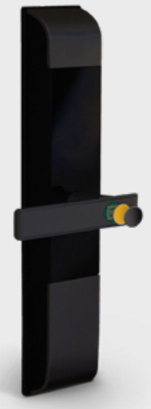
Biometrics in PCs and peripherals – users can unlock computers, login to their profiles and access data, apps and services.

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. Whether it is for doors, garage doors or wardrobes.

LET´S FOCUS ON BIOMETRIC DOOR LOCKS

With biometric door locks, you become the key. PINs and passwords can be hacked, locks can be picked, keys and fobs can be lost or stolen. Fingerprint sensors on locks adds a trusted layer of security without compromising convenience.



BIOMETRICS... IN A DOOR LOCK?

1. Privacy - Fingerprint data is stored securely in, and never leaves, the door lock. Users have total control of their data privacy.

2. Power - Ultra-low power consumption, even when active.

3. Flexible - Manage different access rights and choose from a range of design options to blend seamlessly into the door lock.

4. Discreet - Discreet, super-slim and robust sensor. Authenticate from any angle in less than half a second. Supports up to 10M touches.

Biometrics - providing a worryless, convenient and secure home environment

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

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

Outstanding performance

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

FINGERPRINTS