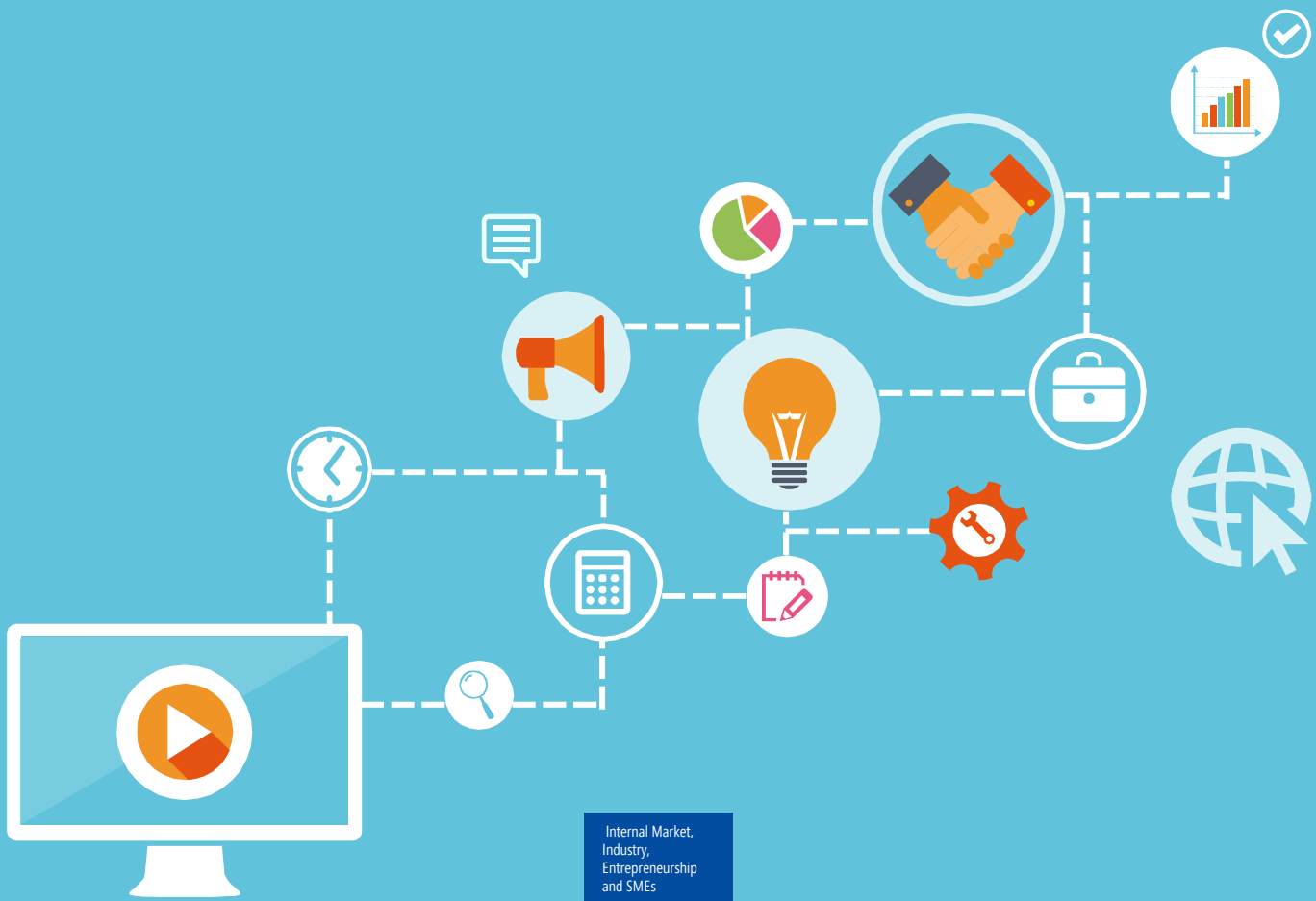
European Commission

Digital Transformation Monitor

Biometrics technologies: a key enabler for future digital services

January 2018



Internal Market, Industry, Entrepreneurship and SMEs

© www. Gemalto. com

Biometric technologies: a key enabler for future digital services

Biometric technologies refer to all processes used to recognize, authenticate and identify persons based on physical and/or behavioral characteristics. The global biometrics market is growing at a fast pace, initially due to the need to combat the rising security challenges. Today, with fingerprint and facial recognition applications dripping down to consumer market through smartphones, broader applications of biometrics will be highly expected for the future digital world.

1

Biometrics penetrating in different markets

The rising usage of biometrics

Overview of biometric technologies

Biometrics are initially known for the application in authentication. Authentication is the process by which the identity of a user is verified. Various factors can be used for authentication.

Traditional methods include "Something you have" such as physical token or smartcard, and "Something you know" like user login and password. Biometrics otherwise act as " Something You Are ", using unique biological traits of the user to identify them.

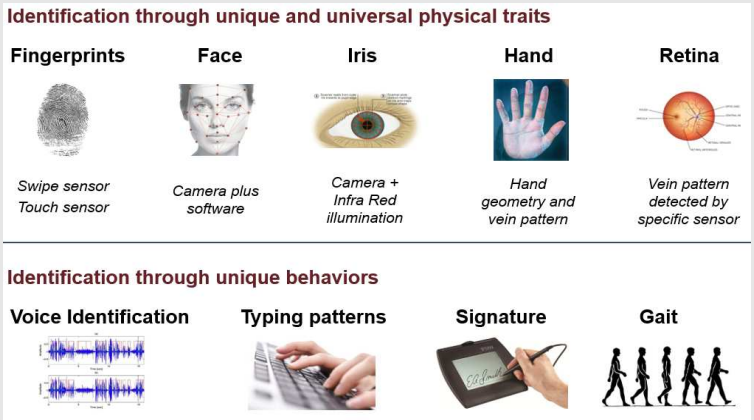
Various traits can be measured and recognised uniquely, which can be in general devided into two categories:

- **Unique and universal physical traits:** fingerprint, iris, face, hand and retina.
- **Additional alternatives based on unique behaviour of the end user:** voice recognition, typing patterns or signature recognition.

Those different factors are often merged in 'MultiFactor Authentication' (MFA), a technique to heighten the security of the user identification process, compounding two or more independent credentials mentionned above.

No matter what biometric data is used, thoses solutions rely both on hardware (the sensor) and software to improve the security of user authentication. Specific software is applied, though differing in each case, for analysing and matching the authentication factors, and allowing applications on a device to use the sensor through an API.

Figure 1: Different biometric factors being used for authentication



Source: IDATE DigiWorld, December 2017

Main applications of biometrics

An increasing number of implementation of biometrics is taking place, and the usage is multiple.

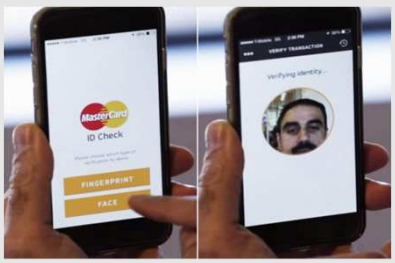
Biometrics have long been used for **customer identification,** where fingerprint firstly opened the market for smarphone unlock. Beyond that, different biometrics are applied to various use cases, for instance, voice verification for call centre identificiation, facial recognition or typing patterns for online identification.

Biometrics for **secure access control** also becomes prevelent.

Unique biometrics like fingerprint are capable of restricting unauthorized persons from reaching pre-defined areas.

More particularly, in highly security-sensitive cases such as military or nuclear applications, retina or iris recognition is more often used. The blood vessel (retina) and iris pattern are considered to be very stable over time and false match rates are the lowest of all biometric identification methods. However, the costs of such identification systems are much higher than others.

Figure 2: Facial recognition-based 'Pay by selfie' by MasterCard



Source: : MasterCard

Biometrics technologies also extend to **online banking and payment sector**. Apart from fingerprint authentication, MasterCard also launched a payment authentication solution using face recognition and a custom mobile app: 'pay-by-selfie'. Apple has launched a similar payment service in 2017 as well.

Public sector is another focused market for biometrics applications. It ranges from paperless process for digital identity, visa application, to border control, to public security monitoring. Fingerprint remains the most often used biometric element, whereas facial recognition plays a key role in identifying criminals in public places.

Other emerging use cases, albeit non-exhaustively, include social networks tag using facial recognition, or fraud detection and forensic evidence using voice identification.

Current market development

Market dominated by fingerprint technology

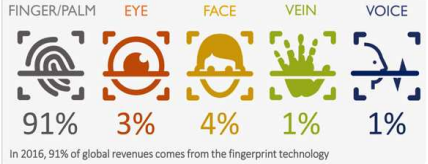
The biometrics market is growing rapidly – the cumulative worldwide revenue[1] is forecast to reach nearly 70 billion USD during the period 2016 – 2025, at a CAGR of 22.9%.

Fingerprint sensing, as having been embedded in smartphone identification system for years, is becoming the mainstream deployment. Another study[2] estimated that 91% of global revenue came from fingerprint technology in 2016.

Facial and voice recognition is catching up due to increased daily use cases. The latest launched iPhone 8 and iPhone X are expected to make the facial recognition climb up the growth curve.

Voice recognition development will be linked to growing adoption of virtual assistants, coming with the popularity of Amazon Alexa and Google Assistant. The two services, though voiced interactive, have not integrated voice recognition yet to distinguish the person who gives orders.

Figure 3: Share of main biometric technologies in global revenues



Source: Yole Developpment, 2016

Different deployment approaches between consumer and business markets

The main target of the biometic solutions is the B2B market is enabling companies to better manage the identity and authentication of their work force, or helping governments improve public security and management. Strong multi-factor authentication systems are thus adopted, combing biometrics to other authentication methodes such as password, PIN and physical identity card.

Since multi-factor authentication is more costly and generally has negative impacts on ease-of-use, they seem to be targeting the consumer market only at the situations where «security» is very critical, such as for mobile payment. Otherwise, end users tend to accept biometrics authentication more often for its convenience than security concern.

2

Key stakes for biometrics adoption

A developing regulatory landscape

There are actually, to date, no particular legal provisions in the world specific to biometric data protection. The collection and use of biometric data is generally regulated within the framework of personal data protection and privacy laws in a broad sense.

For instance, in Europe, the biometric data is subject to some fundamental rules of GDPR (General Data Protection Regulation), including users' consent and "the right to be forgotten".

In the US, though no single federal law exists to govern the use of biometric data, a handful of states have enacted specific biometrics-related regulations. Illinois, Texas and Washington, for example, have passed biometric privacy laws subsequently since 2008.

To a broader sense, general guidelines have also been put forward by some biometric consortium, aiming to remove barriers for biometric data use. IBIA (International Biometrics and Identity Association), among others, provides key principles for commercial biometric use, such as disclose the reason for fingerprints collection, and to destroy biometric data at agreed conditions.

National ID programs favoring biometrics adoption

Public sector in both developped and emerging eonomies is increasingly adopting biometric technologies, with purpose generally centred around security concerns and border control.

The UK Home Office planned to invest **£96 million** in biometric technologies.

Under the immigration trend and challenges from terrorism, the UK Home Office planned to invest £96 million in fingerprint, facial recognition and DNA verification for law enforcement, visa application and counter-terrorism since mid-2017. The US has similar plans to install biometric-based systems in all major airports within four years.

In African nations, though at different development stages, new efforts have been announced to improve biometric registration. Zimbabwe is on track for 80% biometric electoral registration; Ethiopia is also carrying out a large-scale biometric enrollment project for refugees protection and assistance.

Growing user acceptance

Unlike traditional authentication methods such as Facebook login and password, biometrics-baseed solutions are much less trapped by trustness and privacy issues from the user side.

It is noted that unless some serious security or privacy scandal dents customer trust, users will continue using biometrics such as fingerprints to facilitate the authentication, although fingerprint is not significantly stronger than certain conventional authentication methods.

In the consumer market, biometric identification on mobile becomes more and more standard. Most high-end mobile phones were already shipped with a fingerprint sensor in 2015 and many mid-range mobile phone have one today. In late 2017, the release of iPhone 8 and iPhone X also makes facial recognition known to public.

Users are increasingly acknowledged of biometric technologies and using them, primarily owing to the convenience and rapidity in authentication process. Biometrics reduce the need of formal authentication of many other methodes, such as no tokens and no cards. This trend is likely to continue for the coming years.

Lack of direct revenue for business adopter

Despite improved experience and security for the end-user, biometrics solution remain a cost for business adopters, such as retailers and automakers who integrate biometrics in their products and services. On this basis, the price sensitivity of end-user makes it difficult to launch biometric solutions as direct paid service.

Since monetization of biometric technologies is, for the time being, not straightforward, biometrics-based offerings typically go to market by bundling to premium products and services, for example, luxury car brands.

3 Potential impact on automotive industry

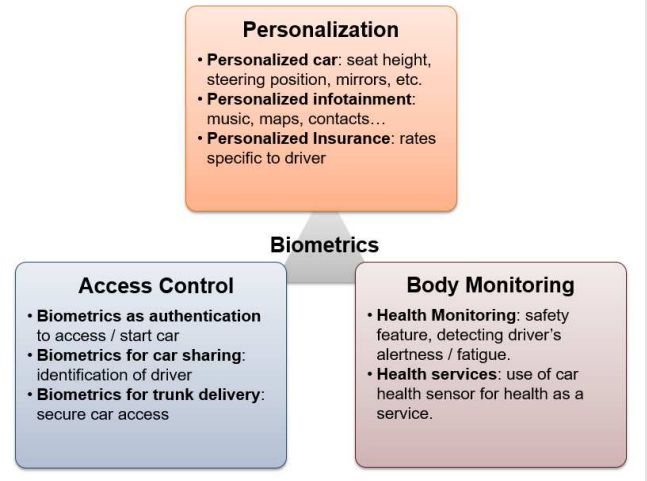
Biometrics in cars

The automotive industry shows great interests in biometrics technologies, primarily aiming to increase security through driver identification and authentication, as well as provide a more convenient experience.

Technological options specific to a wide range of in-car use cases

Among others, the biometric technologies that are favored by auto makers include fingerprint, facial recognition, iris recognition, voice identification and gait tracking.

Figure 4: Main use cases of biometric technologies for vehicles



Source: IDATE DigiWorld, December 2017

Each technology has specific in-vehicle scenarios to fit in. Fingerprint-based authentication are typically used to substitute car key or certain buttons.

By contrast, touchless authentication leveraging facial, or iris or voice recognition technologies provides more convenience to drivers and passengers

Apart from driver identification, many other services using biometrics are being developed. This is particularly the case for premium car models. For instance, face and iris recognitions are integrated to vehicle camera system, allowing alertness monitoring when drivers demonstrate any fatigue or drowsiness.

On top of that, biometric sensors embedded in car seat can enable a personalised comfort, as car seat can adapt itself to the drivers' physical features such as height and preferred steering position. In addition, personalized services become available, for instance, voice-controlled infotainment services.

Existing initiatives in automotive industry

Several initiatives have been announced by car manufacturers and equipment suppliers starting from 2015. Those initiatives are mostly at the concept stage for now. The trend is, as showed in the Table 1, the majority of experiments using biometrics are taking place in the access control and personalisation area.

Social impact

Reduction of accidents risks

Indeed, crashes are currently overwhelmingly attributed to driver related-causes, typically speeding, alcohol, distraction and fatigue. According to the NHSTA (National Highway Traffic Safety Administration)[3], 94% of all crashes are caused by human errors and inattention, and only 2% of accidents can be attributed to the vehicle itself.

94% of all crashes [3]

are caused by human errors and inattention.

Biometrics-enabled driver monitoring system will recognize and evaluate the level of awareness of the driver, through detection of drowsiness and other distractions. With alerting integrated, driver monitoring system will help reduce accidents resulting from fatigue and inadvertent mistakes.

It is widely agreed within auto industry that the autonomous driving are still years away to meet the safety standards. During this transition period from human driving to self-driving, it is thus of great value to bring in biometrics technologies to assure road safety.

Table 1: Existing initiatives using biometric technologies in vehicles

Company	Biometrics use case	Biometrics Technology	Year
Continental	- Access Control: biometrics authentication as a second factor of authentication (key + biometrics)	- Fingerprint sensor	2017
Continental	- Personalised cars settings (seat & mirror position)	- Face recognition	2017
Delta ID	- Access control and personalisation	- Iris recognition	2017
Chrysler	- Car personalization (seat & mirror) - Infotainment personalisation	- Face recognition	2017
Jaguar Land Rover	- Door access system	- Face recognition - Gesture recognition	2016
GM	- Driver Alertness Monitoring, sleep detection	- Facial recognition	2016
Samsung (Harman International Industries)	- Driver Alertness Monitoring, sleep detection	- Pupil monitoring	2016
Gestigon	- Health issue monitoring	- Gesture detection	2016
Optalert	- Smart glasses to detect drowsiness	- Eye monitoring	2016
Empatica	- Wristworn device to detect seizure	- Wearable sensors	2016
Sober Steering	- Detect alcool usage	- sensor embedded in steering wheel	2016
Vigo	- Detect driver distraction and drowsiness	- headset with sensors	2016
Mitsubishi Electric (EMIRAI concept car)	- Access control - Personalised car	- Facial recognition - Temperature sensor - Heart rate sensor	2011
Valeo (partnered with Morph)	- Driver Monitoring of drowsiness and distractions	- Facial recognition	2015

Source: IDATE DigiWorld, December 2017

Indirect social costs reduction

According to the association for safe international road travel[4], nearly 1.3 million people die in road crash each year. Accidents represent a cost of more than 500 billion USD per year, costing an average of 1-2% of the annual GDP of each country.

With regard to societal effects, biometrics-based driving monitoring and alerting tends to lead to the dropping down of the public costs, along with reduced car accidents risk.

Economic impact

Reduction of car security related loss

Vehicle theft is on the rise, particularly for the premium models. The number[5] of cars being stolen has increased by 30% during 2013 to 2016. Compared to physical key loss or duplication, cyber vulnerability causes more car theft - 74.5% of stolen cars[6] are those equipped with keyless entry or remote start.

Unlike traditional locks, biometric fingerprint or iris lock is not susceptible to being copied or picked. This system is thus capable of failing unattended car access. In addition, to start the vehicle, facial or fingerprint authentication of a drive adds duplicated security even if telematics system is hacked remotely,

Taking account of the loss that can be potentially saved by biometric access, 35% of UK drivers would prefer biometrics system, as being requested in a survey[7].

Added value gained from personalised in-car experience

Personalised experience can lead to higher customer satisfaction and potentially result in more consumption of in-car services.

Apart from increasing demand on enhanced security, consumers also expect more personalized in-car experience. About third drivers (35% in UK, 30% in Germany)[7] want their cars to remember their individual preferences on the road.

The body monitoring of drivers' physical characteristics such as height and gait will allow more individual adaptation, such as automatic seat back tilting.

Beyond that, biometrics for multi-platform authentication could build seamless experience for consumers, for instance, to synchronize music play in car like at home. This personalized multimedia service will be of greater value particularly at self-driving era, when drives are hands-free.

A third of drivers[7] (35% in UK, 30% in Germany) want their cars to remember their individual preferences on the road.

Facilitating mobility services

The utilisation rate of car-sharing will boost from 5% in 2017 to over 50% by 2030, according to a research[8] of Fujitsu America. The prevailing of «mobility-as-a-service (MaaS)» impose challenges to efficent vehicle access management.

Biometrics for access control will overcome many inefficiency of car transfering among different drivers (users). Meanwhile, new services such as car-based payment can ride on MaaS as well, when secure authentication is assured via biometrics.

New auto insurance model

The new auto insurance model is expected to build on different driving habits. As a complementary to in-car sensors such as camera system, biometrics allow to monitor drivers' behavior, which will eventually impact on the premium fees and claim rates.

To begin with, flexible premium fees will be available to drivers, with rates adjusted to their driving behaviour. In addition, in case of any car accident, the biometrics-based driver monitoring can provide evidence during the arbitration procedures. Meanwhile, insurers may bind value-added services such as fatigue alerting as an option to existing auto insurance.

References

[1] Yole Developpement, 2016, Biometrics market analysis, Available at: http://marketbusinessnews.com/fingerprint-recognition-dominates-biometrics-market-now/150339

[2] Tractica, 2016, Biometrics Market Forecasts, Available at: https://www.tractica.com/research/biometrics-market-forecasts/

[3] NHSTA (National Highway Traffic Safety Administration), 2015, Critical Reasons for Crashes Investigated in the National Motor Vehicle Crash Causation Survey, Available at: https://crashstats.nhtsa.dot.gov/Api/Public/ViewPublication/812115

[4] The association for safe international road travel, 2017, Annual Global Road Crash Statistics, Available at: http://asirt.org/initiatives/informing-road-users/road-safety-facts/road-crash-statistics

[5] RAC Insurance, 2017, Police data reveals 30% increase in stolen vehicles in three years, Available at: https://www.rac.co.uk/press-centre#/pressreleases/police-data-reveals-30-percent-increase-in-stolen-vehicles-in-three-years-2173913

[6] Strategy Analytics, 2017, Infotainment & Telematics Connected Car Security, Available at: https://www.itu.int/en/ITU-T/extcoop/cits/Documents/Workshop-201707-Singapore/008%20-%20Roger-Lanctot-Infotainment%20and%20Telematics-Connected%20Car%20Security.pdf

[7] Nuance Communications and YouGov, 2016, The future of driving will be personalized, Available at: https://www.theengineer.co.uk/the-future-of-driving-will-be-personalised/

[8] Findbiometrics, 2017, Biometric Access Control To Become Standard in Car Sharing: Fujitsu, Available at: https://findbiometrics.com/biometric-access-control-car-sharing-report-411166/

About the Digital Transformation Monitor

The Digital Transformation Monitor aims to foster the knowledge base on the state of play and evolution of digital transformation in Europe. The site provides a monitoring mechanism to examine key trends in digital transformation. It offers a unique insight into statistics and initiatives to support digital transformation, as well as reports on key industrial and technological opportunities, challenges and policy initiatives related to digital transformation.

Web page: https://ec.europa.eu/growth/tools-databases/dem/

This report was prepared for the European Commission, Directorate-General Internal Market, Industry, Entrepreneurship and SMEs; Directorate F: Innovation and Advanced Manufacturing; Unit F/3 KETs, Digital Manufacturing and Interoperability by the consortium composed of PwC, CARSA, IDATE and ESN, under the contract Digital Entrepreneurship Monitor (EASME/COSME/2014/004)

Authors: Vincent Bonneau, IDATE and Laurent Probst, Virginie Lefebvre, PwC

DISCLAIMER – The information and views set out in this publication are those of the author(s) and should not be considered as the official opinions or statements of the European Commission. The Commission does not guarantee the accuracy of the data included in this publication. Neither the Commission nor any person acting on the Commission's behalf may be held responsible for the use which might be made of the information contained in this publication. © 2017 – European Union. All rights reserved.