Deutsche Bank
DB Research

Current Issues

Digital economy and structural change

Homo biometricus

Biometric recognition systems and mobile internet services

June 28, 2012

Author
Thomas F. Dapp
+49 69 910-31752
thomas-frank.dapp@db.com

Editor
Antje Stobbe

Deutsche Bank AG
DB Research
Frankfurt am Main
Germany
E-mail: marketing.dbr@db.com
Fax: +49 69 910-31877

www.dbresearch.com

DB Research Management
Ralf Hoffmann | Bernhard Speyer

Traditional identification procedures based on knowledge and possession show vulnerabilities that are being highlighted precisely by digitally driven structural change and the growing use of internet technologies and mobile devices.

In an era when a variety of sectors are being suffused by digital processes biometric recognition technologies offer a broad range of potential applications. The fast-growing mobile internet services segment represents a particularly lucrative potential market.

Many experts remain sceptical about the deployment of biometric recognition systems in mass markets. Nevertheless, biometric procedures are already accepted by millions of people every day on a variety of (social) internet platforms.

Whether as a complementary technology or even as a replacement technology, biometrics deliver greater reliability and increased ease of use for verifying identity claims – first and foremost in mobile mass markets.

Wherever minor system errors are easier to excuse, this is where biometric recognition procedures will (initially) spread. Banks tend not to be among the "early adopters" because the acceptance risk is (still) too high and/or the robustness required of biometric systems is not (yet) sufficiently guaranteed.

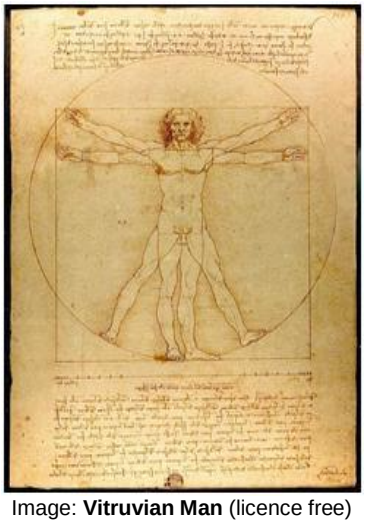


Image: **Vitruvian Man** (licence free)

Man is not only the measure of all things according to Renaissance thought, man is also the model for the cosmos. [Leonardo da Vinci *1452; † 1519]
(own translation)

1. Biometrics – an alternative security technology

Methods of identification[1] are used wherever people are unknown and they have to identify themselves or gain access to a system. At many locations people have to undergo individual authentication, whether they are at the airport, crossing a national border, picking up a parcel or executing an online credit transfer. A variety of methods can be used to carry out this task: for example, trusting in the reliability of a third party, an identification document (e.g. ID card) or a previously agreed password. The cited identification methods are based on either possession or knowledge or a combination of both. Cash machines, for example, only dispense cash if the possession of a bank card corresponds with the knowledge of the PIN code or password and grant access to the system.

Traditional identification methods have vulnerabilities

Traditional identification procedures that are based on knowledge and possession show vulnerabilities that are increasingly being highlighted precisely by digitally driven structural change and the growing use of internet technologies – especially via mobile devices. Possession and knowledge are personal and can easily be passed on to third parties. This means there is no guarantee that the current bearer of the credentials (possession or knowledge) is actually the authorised person. For example, bank cards, keys or tokens are lost, passwords and PINs are forgotten or stolen or are increasingly being hacked online using sophisticated spyware and malware. Germany's Federal Criminal Police Office (BKA) confirmed that the number of cybercrime offences rose in 2010, with the actual total undoubtedly far higher than the number recorded in the official statistics.[2] The economic losses caused by the offences in 2010 were estimated at EUR 61.5 m – and the figure is rising (+66.7% vs. 2009).

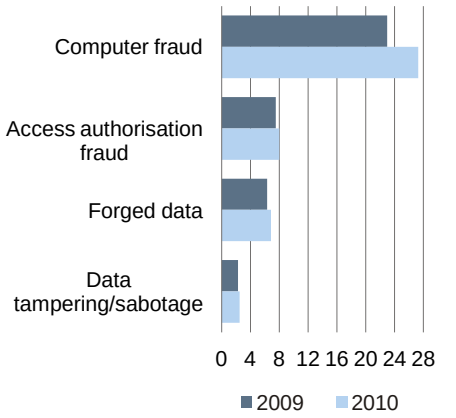
Users often fail to exercise due care when choosing passwords or the numbers to make up a PIN. Given the increasing number of logical and physical access controls people attempt to preclude losing their passwords or keys by storing them in what are often unsuitable locations or by even using identical online passwords for several services. Passwords that are used for online banking, for various IT systems or for other internet services are often too short or lack complexity and can for example be "cracked" relatively easily using the brute force method.[3] Moreover, many owners of mobile devices (smartphones, tablet PCs) are not as diligent in using antivirus software and/or firewalls as they are with desktop PCs, which makes surfing the internet a generally unsafe activity.

Given the well-known vulnerabilities, undoubtedly also in the wake of the 9/11 attacks the debate about alternative, secure authentication procedures is gaining in intensity. Biometrics thus has a pivotal role in security technologies of the future, and certainly offers lucrative market potential.

This report focuses on biometric identification procedures and their potential applications in everyday life. Chapter 2 deals with the principles of biometrics , describing the system-related terminology as well as the most common procedures. In addition, explanations are given of factors such as the performance capability of biometric procedures and the legal framework (data protection). Chapter 3 focuses squarely on the use of biometric recognition procedures in the fast-growing mobile internet services segment – especially in the bank-related services segment. This is followed in chapter 4 by comments from experts from the worlds of science and business who discuss the use of biometrics in the banking segment. The report concludes with examples of

Cybercrime 1

Cases by offers ('000)



Source: Federal Criminal Police Office (BKA)

Brute force method 2

In the IT segment the "brute force method" signifies the most simple of all algorithmic solutions. The brute force method is frequently used to "crack" passwords. It systematically and completely automatically tests every potential sequence of characters or whole dictionaries. Since lots of people use the same passwords and PIN codes for various IT services or purposes the criminal whose "cracking" efforts are successful immediately gains access to several computer programmes or internet services.

According to the Federal Office for Information Technology Security (BSI), PIN codes are sometimes written on EC cards or easy-to-crack passwords such as the number "1234" are used. One frightening statistic is that the password "1234" is one of the ten most popular passwords in the English-speaking world.

Sources: Perfect Passwords, Mark Burnett

[1] Identification means establishing the identity of an individual from within a given group of people.
[2] Federal Criminal Police Office - BKA (2010). Cybercrime. Bundeslagebericht 2010. Wiesbaden.
[3] Federal Office for Information Security (BSI). Lagebericht, Q1 2011.

Ambivalent (German) debate about biometrics 3

The (predominantly German) debate as to whether the technology for biometric recognition processes (also for data protection reasons) is already suitable for mass markets is irritating, because the digital online ecosystems have successfully used image and voice recognition processes for years already. Biometrics has already reached mass markets online (in Germany, too) via millions of users of social platforms. On the internet, users accept interaction with biometric recognition procedures every day – and the numbers are rising. Pictures of individuals are marked, linked, distributed virally and commented upon. Furthermore, voice apps are offered on mobile devices that can serve as a kind of a personal assistant for routine tasks. They can be used to execute voice commands or answer simple questions. The marking of images on social platforms and the compiling of voice profiles by the providers are contentious with regard to data protection regulations, but are nevertheless largely accepted unchallenged by users.

current biometrics research as well as a brief outlook concerning biometric recognition procedures in the coming years.

2. Biometrics – principles

The term "biometrics" is derived from the ancient Greek words "bios" (life) and "metron" (measure). Biometrics is thus the science of bodily measurement of living beings and the measurement and evaluation procedures required to do this.[4] Biometrics is a field that has interested mankind for centuries already. Leonardo Da Vinci[5] already described and measured parts of the human body, and in the early 16th century Albrecht Dürer also attempted to make detailed measurements of the human hand in order to identify common features and patterns. Today, forensics is probably the best-known application of biometric measurement procedures. Criminal investigation authorities try to catch criminals or identify victims using biometric technologies.

In an information technology age with digital processes becoming integral elements of numerous sectors biometric recognition technologies offer a broad range of potential applications, especially in the fast-growing mobile internet services segment. To date, biometrics have mainly been used for physical access control (e.g. to high-security areas in power stations or to secure military installations). In these cases people are usually identified on the basis of their anatomical and physiological characteristics. Anatomical characteristics[6] are shaped by *bodily structures* (face, finger) and the physiological characteristics[7] by *bodily functions* (voice, facial expression, way of walking, keystroke).

In order that biometric recognition procedures can deliver greater benefits than traditional methods the physiological (passive) and behavioural (active) characteristics must possess specific features: the characteristics must be

— *universal* (present in every human being),

— *unique* (different in every human being),

— *constant* (do not change over time) and

— *quantitatively detectable and/or measurable* using technologies.

Live check reduces uncertainty

The detectability of characteristics is important because they are processed electronically. The integrity of the characteristics is guaranteed via a "live check", i.e. sensors must be able to identify specific criteria such as body temperature or blood circulation.[8] Characteristics can thus not simply be copied and then replaced with a fake, "inanimate" copy (e.g. artificial finger). Every biometric identification is based on a comparison between one or more characteristics of the individual and the previously captured biometric reference template. When a person's biometric characteristics are captured for the first time they must be entered into a system, i.e the person makes him/herself known to the system. This results in the logging of a reference template of the measured person that is linked to the person's identity. The template is then stored in a memory device (database or smartcard). This procedure is called *enrolment*.

How enrolment works

[4] The International Organization for Standardization defines biometrics as follows: "automated recognition of individuals based on their behavioural and biological characteristics" [ISO/IEC FDIS 2382-37, 2012].

[5] 1492 saw the creation of the Vitruvian study of bodily proportions (cover page photo), as well as studies of the proportions of human bodies and faces as well as anatomical analyses.

[6] Other biological characteristics are retina, hand geometry, iris or vein pattern.

[7] Other behavioural characteristics are, for example, signature, keystroke or gestures/facial expression when speaking.

[8] TeleTrusT (2006). Bewertungskriterien zur Vergleichbarkeit biometrischer Verfahren. Kriterienkatalog. TeleTrusT Deutschland e.V. Erfurt.

Template is filed away in the storage medium

Several measurements are usually made during enrolment. Either an average is derived from the repeated enrolments or the differing measurements are filed away directly in the storage medium as the database for subsequent matching. This end-product of this procedure is called a template. Storing a template takes up only a few bytes of memory, because it contains only a few specific attributes that are extracted from the measured data and used for the matching procedure. This means that the tiniest smartcards are ideal for storing templates. Depending on the procedure the number of extracted individual features varies and thus also the size of the template. The time required for enrolment depends on the procedure and can range from a few seconds to several minutes.[9]

Variety of biometric recognition processes

Biometric systems and technologies can utilise numerous biometric recognition processes. Several of these processes are already in everyday use, whereas others are still at the research and development stage. With some people the characteristics cannot be measured with sufficient precision because they lack definition or due to the individual inadequacy of a characteristic. Such a case can occur, for example, if a person's specific fingerprint characteristics cannot be measured properly. The provider of biometric recognition procedures must then offer alternative, additional procedures in order that these persons are not ruled out *per se*.

In the following we list the most common biometric processes, divided into behavioural and physiological attributes, as well as the characteristics on which they are based:

Basis: Physiological characteristics

Synopsis of biometric recognition procedures 4

Biometric recognition procedure	Attribute	Representation of the biometric attribute
Fingerprint	Skin pattern of the fingerprint	Image of the ridges on the finger, classification, characteristic features (minutiae)
Hand	Measurements and shape of fingers and palms	Length of the fingers, hand geometry
Face	Facial image and geometric attributes	Transformation approach: Covariance analysis of facial images; attribute approach: attributes such as nose; eyes, etc. and their specified geometric sizes and structures
Iris	Tissue pattern surrounding the pupil	Texture analysis
Retina	Pattern of the blood vessels at the rear of the eye	Texture analysis of the circular scan of the retina/the blood vessels behind the retina

Sources: Behrens, M. und Roth, R. (2001). Biometrische Identifikation. Grundlagen, Verfahren, Perspektiven. Vieweg Verlag.

[9] Amberg, M. et al. 2003. Biometrische Verfahren. Studie zum State Of The Art. Friedrich-Alexander-Universität Erlangen-Nürnberg. Nuremberg.

Basis: Behavioural characteristics

Synopsis of biometric recognition procedures 5

Biometric recognition procedure	Characteristic	Representation of the biometric attribute
Voice	Voice	Set texts or independent solutions
Signature/writing	Writing behaviour	Speed, pressure, acceleration of the writing action
Keystroke	Keystroke rhythm/speed	Measurements of pressure duration and intervals between keystrokers
Visual speaker	Facial expression	Analysis of sequences of movement while reciting agreed texts

Sources: Behrens, M. und Roth, R. (2001). Biometrische Identifikation. Grundlagen, Verfahren, Perspektiven. Vieweg Verlag.

Performance capability of a biometric system

The success and failure of biometric recognition processes are determined via probabilities. Each biometric process has an inevitable residual error rate. It is, however, difficult to establish this objectively, as it depends on the subjects (e.g. people with less pronounced features) and the respective test conditions (e.g. background noise when voice recognition is being used). In practice it is not uncommon for the error rates to deviate from the figures quoted by the manufacturer of the identification process. In order to assess the manufacturers' error rates concrete data must be provided concerning the test procedure and the test conditions. Only the individual adjustment of the process to the requirements of the individual operator allows statements to be made about the actual usability of the process. This means that not every biometric recognition process is equally suitable for all applications. The important thing is that the use of a specific biometric characteristic matches its capabilities. Since in practice the conditions are never the same when biometric data is measured on separate occasions and the objects being measured (fingers, veins, face etc.) are subject to natural fluctuations there will never be a complete match between the freshly captured measurement data and the previously stored reference data, but there will only be a certain similarity. When assessing the performance capability it is therefore tested whether the measured data falls within a "tolerance range" that has to be specified in advance and attains the predefined level of matching.[10]

1:1 match vs. 1:n match

The most important biometric recognition tasks are *verification* and *identification*. With verification, the person to be verified has to supply the system with a name or login details, for example. Afterwards the biometric system decides whether the person matches the template data set (1:1 match). With identification, the person to be identified supplies only their biometric characteristics. The system uses the individual characteristic to determine the associated name or login details (1:n match) by comparing with the template data sets of all persons. The reliability of identification and verification is mainly judged according to two criteria: the False Acceptance Rate (FAR), which measures the allowable rate of unauthorised acceptances, and the False Rejection Rate (FRR), which measures the rejection rate of all authorised persons.

[10] TeleTrusT (2006). Bewertungskriterien zur Vergleichbarkeit biometrischer Verfahren. Kriterienkatalog. TeleTrusT Deutschland e.V. Erfurt.

Data-protection-relevant application areas for biometrics 6

Biometrics for employees

Companies use numerous biometric authentication systems for access to rooms, computers, networks and services. This enables cost-saving rights management. Use by the employee may be obligatory, alternative solutions are, however, possible and necessary.

Biometrics for customers

Companies are increasingly offering their customers services that are based on biometric authentication. Examples are non-transferable season tickets or subscriptions for concerts, fitness studios, solariums, zoos, swimming pools, video rental outlets, payment systems etc.

Biometrics for personal applications

These include applications that are totally under the control of the person concerned. Examples are domestic PC access, entry to the home or use in one's own car.

Source: TeleTrusT Deutschland e.V.

Data protection

Since biometric processes measure specific physical human characteristics, person-based data storage is required. In Germany, this data is subject to the protection of the individual's right to decide how their personal data is used and is anchored in the data protection laws of the federation and the *Länder*. The most important legal principles on which data protection law is based can be found in the European Data Protection Directive, the German Data Protection Act (BDSG) and the *Länder* data protection laws.[11] According to Section 3(7) 7 of the BDGS "[...] each person or institution that collects, processes or utilises that personal data for itself or mandates a third party to do this on its behalf" is responsible for complying with data protection regulations. Responsibility for monitoring compliance lies with the respective supervisory authority, i.e. the federal and *Länder* governments.

With regard to data protection the reference library is particularly important as this is the long-term storage location for personal user data until they are potentially deleted. As a consequence of all the ease-of-use benefits of biometric methods it must be checked whether these methods can also be a source of danger for the persons using them. From a data protection point of view the differentiation between verification (1:1) and identification (1:n) is thus important, as databases containing biometric characteristics are basic prerequisites for identification. Data in a centrally stored database is outside the control of the person concerned and is at risk of being misused with the information being utilised for additional purposes that do not conform with data protection regulations.

When personal, physiological or behavioural characteristics are captured electronically so-called excess data/information is also recorded.[12] When the vein pattern of a person's hand is scanned other medical information can also be filtered out (secretly) which could then technically be misused with the aid of the appropriate algorithms. Supplementary information can relate to the personality, the health or ethnic origin of the individual. This information can fall into the hands of third parties. An operator of biometric recognition processes thus bears great responsibility not to pass on biometric data to third parties under any circumstances. In addition, such operators should delete all sensitive data if it is no longer required for its originally agreed purpose.

The debate continues about the extent to which biometric data may be used for surveillance purposes[13] and not solely for the predefined identification task. So there is a risk that biometric data which is stored centrally in a database may be misused and (secretly) utilised for purposes for which no consent has been obtained from the person concerned. It is therefore of particular interest to the person concerned how well his or her personal data is protected against unauthorised access.

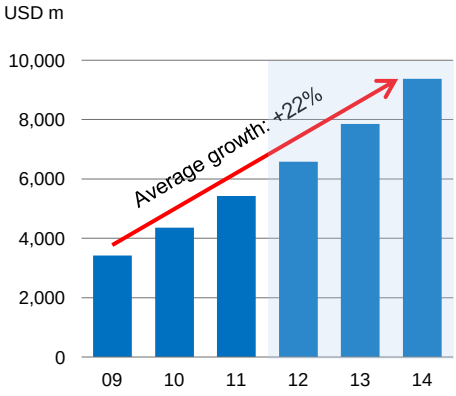
The currently debated obstacles and problems arising from biometric recognition processes are thus less technical in nature, but instead focus on where the attributes of *homo biometricus* are ultimately physically stored. The decisive factor for the use of biometric recognition processes is thus always the overall structure of the process and not the individual technology.

[11] TeleTrusT (2008). White Paper zum Datenschutz in der Biometrie. TeleTrusT Deutschland e.V. Arbeitsgruppe Biometrie. Berlin. www.teletrust.de.

[12] Schaar, Peter (ed.) 2006. Biometrie und Datenschutz – Der vermessene Mensch. Tagungsband zum Symposium des Bundesbeauftragten für den Datenschutz und Informationsfreiheit. Berlin.

[13] Cory Doctorow (an American science-fiction writer) paints the picture in his book *Little Brothers* (2008) of a police state with the ability to carry out identification using RFID and biometrics.

Biometrics sector: Annual sales 7



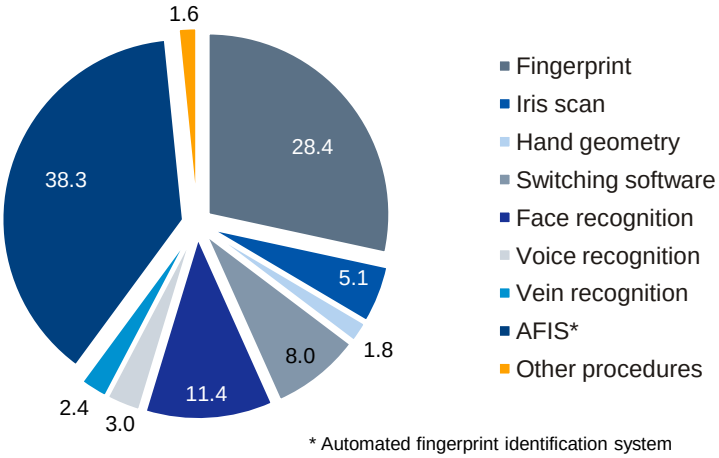
Sources: International Biometric Group, DB Research

Biometrics is a growth area

Biometric recognition processes are said to promise major growth potential going forward. For instance, experts forecast that sales of biometric solutions will grow at an annualised average nominal rate of more than 22%. Total revenues are projected to amount to USD 9 bn in 2014. Looking at the individual biometric processes reveals that the majority of revenues are currently generated in the fingerprint segment, followed by face recognition and the IT infrastructure associated with biometric recognition processes (software, hardware etc.).

Biometrics sector: Sales breakdown 8

%, by technology, 2009



* Automated fingerprint identification system

Source: International Biometric Group

Biometrics in the banking segment is still in its infancy 9

The use of biometric processes not only at cash machines and in online banking, but also in modern payment systems is still in its infancy – at least outside Japan and Brazil. At the end of 2011 there were 40,000 cash machines in Japan equipped with finger vein biometrics. In Brazil, too, there were already 21,000 cash machines converted to palm vein biometrics, and the conversion of online banking for business clients to palm vein recognition is underway (Turkey: 3,000 cash machines with palm vein recognition).[14] Despite the acceptance of biometric processes at cash machines of foreign banks it will still take a few more years before bank customers in Germany can withdraw money from cash machines using their palm veins or fingerprints. This still requires improvements in technology with regard to robustness as well as public acceptance. The sooner the benefits of biometrics become more apparent, and the more negative experiences and economic losses are caused by spyware and malware in online banking, the more likely biometric processes are to become established.

The reason for the currently high share of fingerprint recognition business is that it can be implemented relatively inexpensively and is easy to use. Especially in highly populated countries fingerprint processes are being used more widely for security and cost reasons (e.g. for identity documents [e-passports]). Experts predict that over the long term there is strong growth potential for voice recognition because digitally driven structural change means that sales of mobile devices are growing constantly and people want to be able to access their data and accounts wherever they are and whatever the time of day. Moreover, the costs of implementing voice recognition on mobile devices are lower than for palm vein or iris recognition. Iris recognition is likely to play a minor role due to the lack of customer acceptance of this technology, since at least subjectively it intrudes deeply into a sensitive personal area (the human eye). Consent is in any case an important prerequisite for the use of biometric processes and is thus dependent on the cooperation of the person concerned.

3. Biometrics and mobile internet services

Not so very long ago mobile phones were only used for making calls and texting. Now, the latest smartphones are gradually supplanting conventional mobiles and offering users numerous embedded sensors[15] together with the corresponding additional functions. Technological advances have come so far in

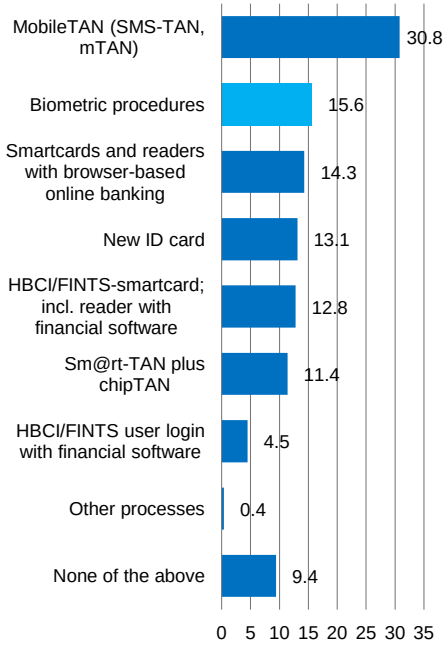
[14] Information supplied in an interview with Dr. W. Grudzien, The Association of German Banks, in March 2012.

[15] Sensors capture parameters such as distances, movement, electromagnetic fields, pressure, speed, humidity, position or temperature and usually convert them into electrical signals.

Homo biometricus

Acceptance of biometric identification processes in online banking 10

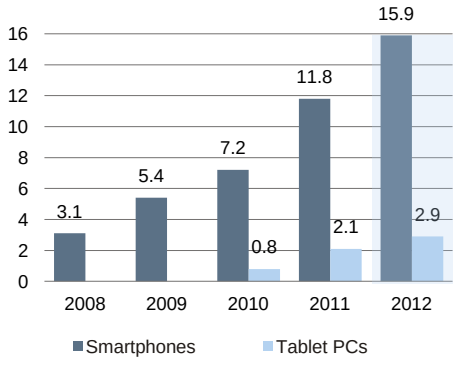
% of population over 14, n=1,006



Source: (N)Onliner Atlas 2011

Mobile devices taking over the mass market 11

Unit sales (million), DE



Sources: EITO, IDATE, Bitkom

the meantime that sensitive sensors can be mass produced cheaply and in miniaturised form, which will make the growth market in the mobile device segment highly dynamic and give it added momentum.

Modern devices contain motion sensors, photoelectric sensors, altitude meters, digital compasses, proximity sensors etc. The latter ensure for example that a device's touchscreen is automatically deactivated when it is held to the user's ear. A motion sensor or a microphone enables a person's walking, running, talking or driving to be measured, for example. Specific algorithms then enable human walking, speaking or driving profiles to be drawn up and stored in smartphones, i.e. smartphones recognise their owners from the way they walk, run, talk or drive. This means that owners of smartphones can also relatively easily authenticate themselves for a variety of transactions or activities online without entering passwords or codes because their individual motion characteristics are unique.

All the additional functions offer the customer a new range of potential applications, causing major disruptions to many (analogue) business models in an extremely wide variety of sectors. An IEEE[16] report contains the following statement: "We believe that sensor-equipped mobile phones will revolutionize many sectors of our economy, including business, healthcare, social networks, environmental monitoring, and transportation."[17] Mobile technologies thus also give rise to new research areas that examine the cross-sectoral use of mobile sensors – the mobile device is just one of many potential applications (clothing, glasses, household appliances etc.) for sensor technology. Growth is driven by, among other things, the desire of many people to be constantly mobile and online. The simultaneously growing human demand for online security will in the coming years presumably be the growth driver for the IT security sector and biometrics. In a survey of the German population over the age of 14 more than 15% of respondents stated that they could conceive of biometric recognition processes being used in online banking in future. This surprisingly large percentage is presumably also due to the growing level of cybercrime.[18]

Not without my smartphone

In Germany some 16 million people have a smartphone and another three million people have a tablet PC – and the numbers are rising. It is second nature for people to carry their smartphones along with their keys and wallets wherever they go, though the latter could become superfluous in future should biometric technologies and mobile digital payment systems become established. Growing unit sales and the increasing functionality of mobile devices are posing major challenges for the financial services sector, too. Banks would be well advised to (further) expand their mobile services activities – while at the same time guaranteeing the necessary security of virtual banking transactions.

The following examples in the mobile internet services segment show how banks will open up more communication and service channels in order to interact with their customers. The transformation of traditional online banking services into the mobile (touchscreen-activated) internet world will mean the banks incur short-term costs, but in the medium to long term mobile banking services can make a significant contribution to reducing costs thanks to their lower operating costs. Biometric recognition procedures are likely to deliver twofold benefits in the future: on the one hand, they will make the client login procedure more user friendly, and on the other, they will guarantee increased transaction security.

[16] The "Institute of Electrical and Electronics Engineers" is a global association of professional electrical and IT engineers based in New York.
[17] Lane N. et al.(2010). A Survey of Mobile Phone Sensing. IEEE Communications Magazine.
[18] Dapp, T. (2012). Growing need for security in online banking. Biometrics enjoy remarkable degree of acceptance. Banking and Technology Snapshot. Deutsche Bank Research, Frankfurt am Main.

Mobile banking

Mobile financial services are more extensive than traditional online banking. Mobile financial services are centred on mobile applications (apps) that can be used via smartphones and/or tablet PCs. For many customers the routine use of internet-enabled devices significantly boosts their quality of life ("OnLife"[19]). Financial service providers' dormant business potential can therefore be leveraged with bank-specific applications (apps) that customers use frequently and can be helpful in everyday situations. Future mobile banking services will provide the customer with service and information along the value creation network of a bank.

Mobile services will range from simple payment transfers and consumer credit right through to securities trading. Some customers might also find it appealing to participate in interactive exchanges with bank employees, traders, analysts or other customers on the bank's own social platforms or fora – all via mobile device channels.

Many banks are still at the very beginning of this journey. However, it is probably only a matter of time before the digital sales and service channels are opened further and customers can access their banks' services anytime and anywhere. There are already banks using apps to offer their clients up to EUR 1,000 of consumer credit. The smartphone is the medium used to guide customers through a standardised creditworthiness assessment programme. If the loan is granted, the client is provided with the amount requested just a few moments later and has immediate access to the money.

Mobile trading

Smart trading, for example, offers clients more than the hitherto available services of buying and selling securities and the ability to check their portfolio online. Banks could conceivably offer their own social platforms on which customers could converse with one another about certain investment strategies, or other financial products. Client fora, live chats or blogs on specific topics with analysts provide the community with relevant information or details of developments in securities. Participants exchange information in real time. Contests to come up with good ideas or a game-playing approach (gamification) to the banking business can reach additional (internet-savvy) target groups and create additional incentives for users to remain on social platforms and/or in the financial community.

(Growth) potential for biometric recognition processes

Biometric recognition processes can optimise the security of transactions conducted using the above-mentioned new mobile (banking) service facilities. Instead of using the standard TAN method of identification the customer could in future execute the transaction using voice activation for example. The concept of *mobile banking* with voice biometrics is based on the 2-channel technique, which is specified by the banking industry: a transaction is sent to both the online banking server and the security server, which checks the sender against the stored voice pattern and notifies the online computer of the result. A future credit transfer could take the following shape: using the mobile phone's camera the bank customer could digitise the standard pre-printed credit transfer slips (QR[20]scanners are also ideal for this). The digital credit transfer slip is read using text recognition software and automatically transferred to the bank server,

[19] Expanding digitisation is also increasing the demand across all sectors for universal and seamless connectivity at no extra cost/effort.

[20] The QR (Quick Response) code consists of a square matrix of black and white dots that can give a binary representation of coded data.

where the transaction is booked. Instead of entering an (i)TAN[21] the customer will in future be called by a speaking computer and be asked to repeat a random sentence or random sequence of numbers. This is how the customer authenticates themself and confirms their credit transfer request. Some speech biometric systems are already certified, function without the customer requiring additional equipment and thus entail comparatively low investment costs for customers and banks.

Another possibility is fingerprint recognition of the bank customer. NFC (Near Field Communication)-enabled[22] devices can verify a person's identity via a smartcard.[23] The face, the iris and the palm vein are under discussion as alternative characteristics to be used for the recognition process. The costs of these processes are higher, though. Although voice recognition is the simplest for everyday applications, the future probably belongs to hybrid solutions that offer several security processes or can link up with each other. The customer can then choose between either finger *or* voice recognition or else opt for both characteristics, that is the voice *and* the finger of the customer are measured. The latter would provide the customer with greater security than isolated processes, which will be a not insignificant factor in Germany with regard to customer acceptance.

Data protection taking voice recognition as an example

Using voice (but also finger and walking style) for the biometric recognition process does not exacerbate an already existing data protection problem. The stored data sets of the enrolled persons (in this case the voice of the customer) can be secured via appropriate functions. It suffices to store the enrolled data set on the user's smartcard (in this case the customer's smartphone). A central database is therefore not necessary. Verification – the 1:1 matching – of the biometric characteristic would then only occur in the customer's smartphone smartcard.[24]

Success of mobile internet services

The success of new mobile (banking) services definitely depends on the benefit to the customer and customer acceptance. In the rapidly developing app market, flexibility is a fundamental feature of the mobile strategy. That is why factors such as the design (of the app), the integration of the data provided with the internal IT infrastructure, the convenience and of course the security precautions that the bank must guarantee for its clients are so important and must be constantly modified. The content supplied by the providers must promise real benefits in the customer's everyday life so that people use the app regularly. Particularly in the mobile services segment biometric identification procedures will offer greater benefits than traditional identification processes, because the use of biometric characteristics is personalised, i.e. the security gap between the identification medium and authorised person (PIN and TAN) is plugged by biometric recognition processes. As customer verification, that is the 1:1 match, is only performed on the customer's mobile device, the data protection issue does not arise.

[21] The indexed TAN (iTAN) is a refined version of the traditional TAN in which the TANs on the list are numbered in sequence or indexed. The iTAN is specified by the bank.
[22] Near Field Communication is an international standard for the contactless transfer of data over short distances of up to 4 cm. To date, this technology has mainly being used for cashless payments (micropayments).
[23] The German banking industry is introducing the new function of contactless payment in a pilot project with 1.3 million customers. Press release, January 11, 2012, Frankfurt am Main.
[24] Information supplied in an interview with Dr. W. Grudzien, The Association of German Banks, in March 2012.

Banks must not miss the boat

Cut-throat competition or cooperation?

If financial service providers delay taking an active interest in mobile business developments (for too long), other competitors could rapidly set the tone in the *mobile business*. Digital ecosystems such as Google, Apple or Facebook are already successfully (and acceptedly) employing biometric voice and image recognition processes; other providers are proving their expertise with digital payment systems. If the internet giants dock onto the appropriate interfaces of their counterparts with their respective strategies, a large provider of mobile payment systems could relatively quickly become a major market player in biometric security technologies. The banking licences required for such activity have already been secured in some cases. This will result in cut-throat competition between banks, but it will also open up new opportunities for alliances with the already established providers. The big internet platforms are focusing their efforts on the mobile market and successfully tapping into the preference of the internet-savvy generations to implement business models.

4. Comments from the worlds of science and business

Supplementing the DB Research view of biometrics, we shall also present expert opinions from those in the research and business segments. Our primary focus is on the potential applications for biometric technologies in the financial services sector. The topics addressed include the current situation, acceptance, legal, technical and financial aspects as well as regulation. We were delighted that the following experts took the time to be interviewed: Professor Dr.-Ing. Christoph Busch[25] of the Fraunhofer Institute for Computer Graphics (IGD) in Darmstadt and professor at Hochschule Darmstadt University of Applied Sciences as well as Bernd-Josef Kohl[26] from IT services provider GFT in Eschborn. What both experts have in common is many years of experience with biometric recognition technologies, the opportunities and risks as well as the potential applications not only in niche markets, but also in mass markets.

DB Research: Professor Busch, Mr Kohl, what is biometrics currently capable of and which processes will become established?

Prof. Busch: the recognition performance of biometric systems has improved vastly over the last decade. Facial recognition processes have been regularly tested by the US National Institute of Standards and Technology (NIST) since 1993. The first test result of a constant False Match Rate (FMR) of 0.001 was combined with an unacceptably high False Non-Match Rate (FNMR) of 0.79. This error rate was reduced from an FNMR=0.54 in 1997 to an FNMR of 0.2 in 2002. The test in 2006 yielded an FNMR of 0.026. The latest test in 2010 achieved an impressive increase in performance to an FNMR of 0.003.[27] Furthermore, India's UIDAI[28] system, even with the enrolment of nearly 100 million individuals showed that biometric recognition is also possible in identification mode. It uses a multimodal system (a combination of finger, face and iris scans).

Kohl: Biometrics is already being used widely, but not yet in mass markets. In Germany, biometric processes can be found in selected areas such as controlling access to company premises and at nearly all airports. In other countries (e.g. India, Japan, Brunei and Brazil) the use of biometric technology is already a mass market.

FMR vs. FNMR 12

The False Match Rate (FMR) states the probability that the newly captured data of an unauthorised user is erroneously identified as being a correct match with the reference template of an unauthorised user.

The False Non-Match Rate (FNMR) states the probability that the newly captured data of an authorised user is erroneously identified as not being a correct match with the reference template.

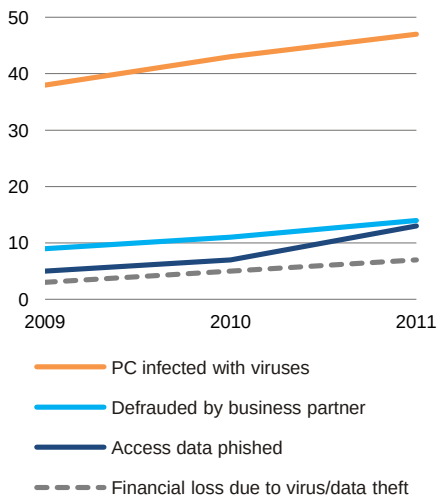
Source: TeleTrusT: Bewertungskriterien zur Vergleichbarkeit biometrischer Verfahren. Kriterienkatalog 2006.

[25] http://www.igd.fraunhofer.de/Institut/Abteilungen/Identifikation-und-Biometrie/Mitarbeiter/Prof-Dr-Ing-Christoph-Busch.
[26] http://www.gft.com/de/de/index.html
[27] For further information see: http://www.nist.gov/itl/iad/ig/mbe.cfm
[28] Unique Identification Authority of India. Planning Commission, Government of India.: http://uidai.gov.in/

Homo biometricus

Experience of cybercrime 13

% of German population over 14



Sources: BITKOM, Forsa

DB Research: Will biometrics be a supplementary or replacement technology?

Prof. Busch: I am convinced that biometrics will replace traditional identification methods, simply because the authentication factors possession and knowledge are not scalable. In the technology-suffused home and work environments each individual has a constantly growing number of keys, smartcards and corresponding PINs to manage. In the long term the individual will no longer be able to handle this. The only alternative is biometrics.

Kohl: In my opinion biometrics will in the medium to long term replace PINs and TANs as well as magnetic stripes on cards. I expect there to be two dominant processes: firstly, voice-based biometrics for numerous applications in the mobile device segment, and secondly, finger and vein scans on bank cards, that could then also be used for non-banking applications such as collecting parcels from “Paketstationen” (automated mail and parcel depots in Germany).

DB Research: Which biometric methods could play a bigger role in the banking world in future?

Prof. Busch: In the concrete case of biometric online banking tamper-proof biometric sensors are essential, as interaction and biometric recognition are conducted at the sensors without a surveillance check being made by the system provider (the bank). The operator must be certain that the sensor has not been tricked by a fake biometric. Good recognition performance, which guarantees user satisfaction, is also necessary. In future we can expect a “biometric secoder” to be used that authenticates transactions by combining fingerprint recognition with finger vein recognition.

Kohl: While voice biometrics can be used on mobile devices for many user groups (also banks or internet portals), the use of fingers/vein patterns is being heavily promoted by the banking sector.

DB Research: Which (technical, legal, financial) obstacles need to be surmounted and how much of a role does data protection play?

Prof. Busch: The technical obstacles are minor. The sensors currently in use can be miniaturised further. Since the imaging of the vein recognition by LEDs[29] and CCDs[30] can be achieved in the near-infrared area of the spectrum, it is merely an engineering task in my opinion. There are no legal obstacles as no biometric data whatsoever is stored on the bank’s server. The financial obstacles are low. I estimate that the extra costs will be a few euros more than for the tokens currently in use. A data-protection-friendly technical structure is an important factor especially with biometric systems. Data protection friendliness is fully assured with the proposed biometric online banking system as the protocol is based on ISO/IEC 24745[31] and no biometric reference data are stored on a server.

Kohl: Very high priority is given to data protection and consumer protection in the EU and perhaps even higher priority in Germany. Each bank will approach the use of biometric technologies very cautiously in order not to get any bad press, which in my opinion is a bigger burden than data protection itself. Depending on the biometric process the requirements concerning security, ease of use and costs are met to differing degrees. Not every process is suitable for universal use in a customer environment. A balance has to be struck between the conflicting factors of ease of use, the attainable level of security and the associated costs. Robust solutions based on biometric technologies have to be

[29] Light Emitting Diode.
[30] CCD sensors are light-sensitive electronic components based on the internal photoelectric effect. CCD = charge-coupled device, which is also used in a CCD sensor.
[31] The international standard ISO/IEC 24745 defines the specifications and a general model for biometric template protection processes. Biometric Template Protection refers to a class of processes for protecting the characteristics data for biometric recognition of humans.

Prof. Dr. Christoph Busch 14

Prof. Christoph Busch has been responsible for System Development in the Media Faculty of the Technical University of Darmstadt since the summer semester 2005. In autumn 2007 he was also appointed as a professor at Gjøvik University College in Norway.

He was assigned by the Federal Office for Information Technology Security (BSI) as project coordinator for the BioIS, BioFace, BioFinger and BioKeyS Pilot-DB projects. Within the EU's Sixth Framework Programme for research he was the initiator of the integrated project 3D-Face. Within the EU's Seventh Framework Programme for research he is the partner for the TURBINE, BEST Network and FIDELITY projects.

He is head of the TeleTrusT Biometrics Working Group and also chairs the BIOSIG Special Interest Group on Biometrics within the Gesellschaft für Informatik. In this function he takes charge of the annual BIOSIG conference.

Christoph Busch chairs the German standardisation body on Biometrics (DIN-NIA37) on behalf of the Fraunhofer Institute for Computer Graphics (IGD) and is an active member of the CEN Focus Group on Biometrics. He is head of the German Delegation in the plenary of the ISO/IEC JTC1 SC37 (Biometrics) and is the convenor of Working Group 3 (Biometric Data Interchange Formats).

More info: http://www.christoph-busch.de

Bernd Josef Kohl 15

Mr. Kohl is Head of International Business Consulting at GFT Technologies AG in Eschborn. He is responsible for Retail Banking, Business Development as well as Current Account Payment Transactions. Mr. Kohl has been active in the field of biometrics for some time and can look back on 5 years of international project experience.

For more information (in German):
http://www.gft.com/de/de/index.html

Multidisciplinarity in biometrics 16

Numerous scientists from the most varied disciplines are conducting research into new applications for biometric recognition processes. The field of biometrics generally requires the cooperation between many branches of science. Besides formulating (technical) security solutions, law, arts and social sciences are often involved in order to comply with data protection and societal requirements. Research focuses on the practical, everyday application of biometrics in order to enhance the quality of human life.

balanced in three dimensions and must deliver benefits in all three dimensions. Combining ease of use with high security will be instrumental in determining acceptance in a mass market. A biometric characteristic is convenient because I can make use of it for as many application areas as possible anytime anywhere. From a legal point of view I do not see any need for action.

DB Research: In your opinion how strong is popular acceptance of these technologies at present and how can it be boosted?

Prof. Busch: The general use of biometric processes will become a routine activity with the introduction and use of biometric passports. The acceptance of the use of biometrics as an additional authentication factor in non-sovereign applications will in my opinion grow by the amount by which the actual losses increase in traditional online banking, for example.

Kohl: Acceptance appears to be high in the niche segments where biometrics are used, whereas for the mass market this is difficult to gauge. A key prerequisite for public acceptance is in any case the separation of everyday use from sovereign applications. Acceptance will be heavily dependent on the launch strategy. The launch of the new electronic identity card in Germany was a perfect example of how not to do it. Greater security is taken for granted by the general public, while acceptance depends on the ease of use. That is why the starting point has to be simple applications. The higher costs of security in online and mobile banking can be passed on via integration into flat fees, for example, for a customer's current account. This would also meet with customer acceptance.

DB Research: How can politicians pave the way for more widespread use of biometrics?

Prof. Busch: The growing threat to the public from the misuse of identity characteristics ("identity theft") will force politicians to take action. It is conceivable that for certain transaction volumes another (biometric) factor will be obligatory.

Kohl: Regulation is sufficient in my opinion. One thing that remains important is clear communication, that a distinction must be made between sovereign applications on the one hand and everyday uses on the other, i.e. that the government will not use existing private and commercial information for its own purposes. Further support could be provided by the government certifying the security of biometric processes.

DB Research: Where do you see potential for mass applications in the near future?

Prof. Busch: In online banking and at POS[32] terminals.

Kohl: Tests are already being carried out with biometric cash machines and with bank cards in which a biometric characteristic is embedded. I see further mass-market potential for example in access control and attendance checks for buildings and premises, for general identity checks, at POS terminals, in mobile and stationary payment transactions or with credit cards and debit cards.

5. Biometrics 2030

Biometrics will in future be used as a security and recognition technology across a variety of sectors due also to the fast pace of technological advance. The areas outlined below represent only a small fraction of the future potential applications. Some of this may (still) sound like science fiction, but several

[32] Point of sale.

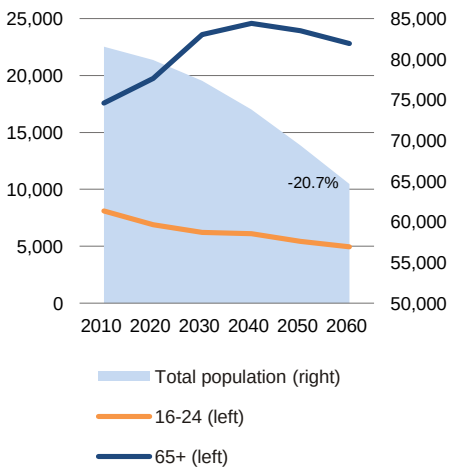
Smart Home 17

The smart home is a privately used dwelling (e.g. owner-occupied house, rented property), in which the numerous automated domestic systems (such as heating, lighting and ventilation), household appliances (such as refrigerator, washing machine), consumer electronics and communications equipment become smart objects that are geared towards the requirements of the occupants. By linking these objects with one another new assistance functions and services can be provided for the resident's benefit and deliver added value that exceeds the separate benefits supplied by the applications present in the home.

Source (in German):
http://www.iit-berlin.de/veroeffentlichungen/iit-studie-smart-home

Demographic development 18

By age cohort ('000), DE



Sources: Federal Statistical Office, DB Research

Technical standards 19

One major obstacle for the internet of things is the incompatibility of conventional (heterogeneous) standards. There is a lack of cross-sectoral system standards that enable appliances from different manufacturers to work together. Neither protocols nor data transfer formats can be linked with one another, which can cause considerable additional costs in the innovation process and prevent the introduction of systems/technologies. The creation of complex, dynamic systems and/or the convergence of technologies will only be made possible in the long term by the diffusion of common standards.

processes are already proving to be successes in the market or are in their pilot phases.

Convergence of technologies

The relatively straightforward diffusion of technology via mobile devices enables many people to benefit from the latest technologies relatively promptly and inexpensively. Potential application areas are not only IT and security, but also healthcare and the auto industry. Wherever ICT is the key technology used and people want to authenticate themselves or operate particular systems or equipment, there are interfaces and opportunities for biometric recognition processes. In future, a sharper focus will be trained on the linking of everyday objects that communicate with one another and make people's routines more amenable. The respective technologies will be integrated as flexibly as possible into the environment and people's everyday routines (internet of things) and as modern interfaces between man and machine will thereby create new (digital) business models. One fundamental prerequisite is the internet and the accessible and wireless linking of everyday objects.

For example, in the "smarter living" segment many everyday objects can be conveniently and efficiently integrated into man's daily environment. Internet-enabled devices and systems as well as services based on them are increasingly finding their way into apartments and houses and into people's everyday lives. This creates home networks which – thanks to the convergence of network technologies and everyday technical equipment – can provide occupants with increased benefits and make their routine activities easier. Convenience and the personal desire to maintain an independent lifestyle (disabilities or old-age-related physical impairments) are the focus. Demographic shifts mean that in future especially the area of maintaining personal independence will see lucrative growth markets open up in the over-65 age cohort in Germany.

On the technical side there is currently still a clear demarcation between consumer electronics, household equipment and home automation.[33] The convergence of these segments will, however, be accompanied by rapid growth and shorter innovation cycles. The internet serves as a basic technology. Many ambient ICT systems[34], especially the radio and infrared-based technologies, offer personalised applications that necessitate user authentication. The convenience of biometrics in this respect makes it an attractive security technology. Everyday objects are fitted with the tiniest, virtually invisible processors and sensors that communicate with one another. The interface between man and machine is controlled via individual human (biometric) characteristics such as voice, gestures or fingerprints. The technology is centrally operated via touchscreen-enabled devices (such as smartphones), for example in the areas of access and locking systems, surveillance or emergency functions. Alarm systems will thus in future be biometrically controllable, i.e. front doors or garage doors will be opened via finger or vein scans, and refrigerators, window blinds or entertainment equipment will be centrally controlled via voice recognition.

In the automotive sector, too, biometric processes will relatively swiftly make major inroads into markets: vehicles will be able to automatically identify who is sitting behind the steering wheel. Regardless of whether individual seating preferences, preferred interior or wing mirror settings, whether favourite radio stations or personal GPS destination settings in the onboard computer: all the usual and individual requirements of the driver will be adjusted automatically as

[33] Strese, H. et al. (2010). Smart Home in Deutschland. Institut für Innovation und Technik. Berlin.
[34] Ambient technologies are defined via an interaction with the spatial environment. This often requires the geographical location of the user or the devices. That is why smartphones with a navigation system are particularly suitable for using these technologies.

soon as the biometric recognition process has identified and authorised the driver. This can be conducted via face scan, voice recognition or fingerprint or else combined with several identification processes.[35] Since mobile devices have become a permanent fixture in people's lives, they can play a bigger role in health-related tasks in everyday life. Certain sensors can constantly capture and monitor behaviour patterns, such as an individual's pulse or perspiration, so that for example, an early and accident-averting intervention can be made when there is a change in the driving characteristics of the person behind the wheel of the vehicle. For example, the vehicle could be prevented from being started if the sensors detect untypical behaviour when the driver climbs into the vehicle or a talking computer could prompt the driver to take a break during the journey, if the system registers signs of tiredness.

Federal Ministry of Education and Research (BMBF): MARS (**M**obile **A**uthentication via **R**etina **S**canning) research project 20

One current research programme commissioned by the BMBF focuses on the use of biometric recognition processes on mobile devices. The research project initiated by the BMBF to this end is called "MARS" (Mobile Authentication via Retina Scanning). MARS commenced in January 2012 and has EUR 3.58 m of funding as part of the "Research for civil security" programme until the end of 2014.

One of the five challenges that the German government identified in its High-tech Strategy 2020[36] is the issue of security. Security research is designed, among other things, to help protect information and communication networks against spyware and malware. Efficient organisational structures and technical instruments for prevention as well as defence against and management of impediments or downtimes are also meant to be developed. The focus of MARS research is based on biometric technologies. The objectives are, on the one hand, improving security via biometric recognition processes and on the other enhancing the security of biometric processes themselves. Modern optical technologies and improved digital image processing allow innovative biometric processes to be developed and/or existing recognition technologies to be improved by combining different biometric processes.

Particularly in the area of mobile (internet-enabled) devices there are growing numbers of unauthorised logins to user accounts and of unauthorised access to sensitive infrastructures by phishing passwords or identity theft. MARS seeks to investigate the interface between user and mobile device in order to be able to guarantee increased security for services on the internet. The research objective will be a new mobile user authentication process. The aim is to make everyday online services easier to use with biometric verification of the user via a retina scan carried out using the mobile device. The applications are diverse: they range from mobile banking and electronic mail right through to access to private property or access control for sensitive areas in sectors where security is a high priority.

6. Conclusion

Biometrics has already arrived in mass markets

Biometric technologies will become established across numerous sectors in the medium to long term. Although many experts continue to have reservations about the use of biometric recognition processes in mass markets, a number of processes are readily used by millions of people each day. For instance, various internet firms successfully offer their clients voice and image recognition processes on a variety of social platforms.

Banks in Germany still hesitant

What will generally apply is that wherever minor system errors are easier to excuse, these are the areas where biometric recognition procedures will (initially) spread. Banks tend not to be among the "early adopters" because the acceptance risk is (still) too high and the robustness required of biometric systems has not (yet) been reliably attained. This means that for the time being there will still be insufficient customer acceptance in this sensitive area.

All the same, biometric technologies will become established (also in the banking segment and in digital payment systems) and complement existing identification methods based solely on knowledge and possession – and might also replace them. Not all biometric processes are equally suitable for everyday applications. Voice recognition will become established for many mobile internet services and in the medium term also in (mobile) online banking, while finger, vein and iris scans will become the appropriate technologies for use at airports

[35] Recorded personal driving styles could also be transmitted straight to the car insurance company, and depending on the individual's driving style they would be put in the corresponding risk category. Whether the customer will, however, consent to this incursion into their personal space remains to be seen.

[36] Ideas: Innovation. Prosperity. High-Tech Strategy 2020 for Germany. Federal Ministry of Education and Research. Berlin 2010.

or border/access controls. Hybrid biometric processes will undoubtedly also be deployed so that no-one will be discriminated against by individual processes on account of a weak or changing characteristic (e.g. ageing for facial recognition). There will, however, always be people who take a more sceptical view of biometric technologies. They will continue to execute their online transactions using PINs and TANs until the new technology has replaced the old one.

Data protection is a particularly contentious issue in Germany

With regard to data protection and in keeping with idea of individuals deciding how their personal data is used, there are two conditions that have to be satisfied for biometric recognition processes to be implemented successfully in the mass market: for the customer it must be transparent when, where and by whom personal data is collected, processed, stored and used. Moreover, customers must have the opportunity to decide about the disclosure and use of their personal data.

Biometrics offers more benefits than knowledge and possession-based processes

100% security is an illusion and will remain so, because there will always be criminal activity and a certain residual amount of risk. Despite this residual risk, biometrics – serving as a supplementary or also as a replacement technology – delivers more reliable results than processes based on knowledge and possession and offers people greater convenience when verifying identity assertions – also and primarily in mobile mass markets. People can be expected to become increasingly aware of the benefits of biometric processes over the coming years and to accept and use the technology as a routine instrument. This will not, however, happen overnight. After all, just ten years ago no-one would have thought that we would be able to access the World Wide Web using pocket-sized devices from wherever we like.

Thomas F. Dapp (+49 69 910-31752, thomas-frank.dapp@db.com)

Printed by: HST Offsetdruck Schadt & Tetzlaff GbR, Dieburg

Print: ISSN 1612-314X / Internet/E-mail: ISSN 1612-3158