Public Perceptions, Preferences and Legal Aspects towards ATMs with Biometric Authentication in Austria

Christoph Hochwarter[1], Dietmar Jahnel[2] and Andreas Uhl[3]

Abstract: This article presents the results of a research project designed to investigate (1) the general attitudes and acceptance of the Austrian public towards biometrics in general, (2) towards ATMs with biometric authentication technology, (3) the kind of biometry they prefer for this kind of application, (4) motivational factors and hindrances concerning a potential roll-out of biometric ATMs in Austria and (5) gives legal background information regarding the employment of biometrics in ATMs and the processing of the biometric data. The data used as a basis was provided by a quantitative online survey (n=706). Results indicate that while a (large) minority is opposed to the concept of ATMs with biometrics (28%), an even larger share was positively inclined towards the concept. However, there was no strong preference for a single biometrical approach towards ATMs in the Austrian populace.

Keywords: Acceptance, Austria, Biometrics, ATM, Attitudes, Socio-technological Aspects, Public Perception, Legal Aspects.

1 Introduction

The prevailing authentication technique when withdrawing cash at ATMs is a one factor technique based on PIN-codes. Disadvantages include low security and low usability as the PIN is often forgotten. Biometric authentication at ATMs is a promising approach exhibiting several advantages. Scientifically, the first aspects considered have been oriented towards improved human-computer interaction and usability [CDJ03, He08]. Biometric ATMs can be operated as one factor authentication system omitting the traditional smartcard (e.g. Bank Islami, Pakistan or MoneyOnMobile, India), as a classical two factor system using smartcard and biometric ATMs, or by replacing the ATM interface with a mobile app, allowing customers to arrange a withdrawal via an NFC-enabled smartphone after biometric authentication using the smartphone's integrated sensor (as developed by Diebold Nixdorf in cooperation with Samsung). Also, biometrics-enabled smartcards with an integrated biometric sensor and NFC might be used at ATMs in the foreseeable future (as developed by MasterCard and Zwipe).

In several countries ATMs allowing authentication via biometric methods are already established. The biometric modality supported however differs among countries

[1] Institute for Empirical Social Studies, Teinfaltstraße 8, 1160 Wien, christoph.hochwarter@ifes.at
[2] Fachbereich Öffentliches Recht, Völker- und Europarecht, Universität Salzburg, Kapitelgasse 5-7, 5020 Salzburg, dietmar.jahnel@sbg.ac.at
[3] Department of Computer Sciences, University of Salzburg, J.-Haringerstr. 2, 5020 Salzburg, uhl@cs.sbg.ac.at

[HM12]. We find ATM installations using iris recognition [CDJ03] in Turkey, Italy, US, Jordan, Egypt, Norway, Yemen, ATMs using face recognition [He08] in Japan, Spain, Taiwan, and ATMs using fingerprint recognition [He05] in India, Nigeria, Mexico, Egypt Malaysia, Cambodia and many more countries. ATMs relying on finger vein recognition are found in China, Japan, Poland, Turkey, and South Korea, while palm vein recognition is used at ATMs in Japan and Turkey. Many European countries, including D-A-CH and France, are rather reluctant with respect to introducing biometric ATMs.[4]

The Austrian banking sector has yet to deploy biometric technology in ATMs. This work gives a descriptive overview of a selection of main results of a survey conducted amongst the Austrian population concerning their general attitude and acceptance towards biometrics in general, regarding the concept of ATMs with biometric authentication, and their preferences, anxieties and hopes concerning this matter. Moreover, it provides information related to the legal background in Austria on the employment of biometrics in ATMS as well as on the processing and storage of the biometric data.

2 Research Methodology

To inquire into the preferences and attitudes concerning ATMs with biometric authentication, a survey among n=706 respondents from the Austrian population was conducted in February and March 2019. Biometrics is still a field new to many respondents (especially in the context of ATMs). As telephone-interviews only permit short verbal descriptions, it was decided to conduct the interviews as Computer-Assisted-Web-Interviews (CAWI), held in German Language, which allow for visual representation of the necessary explanation texts and graphical depictions. The respondents were recruited through an Online Survey Panel using quota design with final weighting to ensure the equivalence of the main sociodemographic characteristics between sample and general Austrian population (sex, age, educational level, as well as a sufficient variation in place of residence in Austria[5]), though this only resulted in small changes (cf. Tab. 1). Only those respondents who declared to "have a debit card and to use it at least occasionally" were included in the survey. Those without a card or who do not use it at all were screened out, in order to ensure validity for those who are the target group of ATMs with biometrics.

[4] Viable online sources for keeping track of new developments regarding ATMs with biometrics include https://findbiometrics.com/topics/atm/ and https://www.biometricupdate.com/?s=atm&submit=Search

[5] The geographical distribution of respondents over the different Austrian federal provinces in the sample follows closely the actual distribution of the populace, with deviations pre- and post-weighting amounting to less than 1% for each federal province.

n=706	pre-weighting	post-weighting
male	49%	50%
female	51%	50%
16-29 years of age	20%	23%
30-44 years of age	25%	25%
45-59 years of age	29%	28%
60-80 years of age	26%	24%
below upper-secondary-education	71%	71%
upper-secondary-education or higher	29%	29%

Tab. 1: Sample demographics

When asked to estimate the frequency of their ATM-usage, 41% of respondents reported to use ATMs at least once a week up to daily; 49% at least once per month; 9% less frequently than once per month; 1% never. This is similar to the results of the "OeNB Monitoring", a representative survey conducted each half year with 1400 respondents financed by the Austrian National Bank concerning the populace's attitudes and behaviour in financial aspects, showing that in 2018 45% of respondents used ATMs at least once per week (up to daily), 48% used them less than once a week but at least once a month, and 7% less than once a month (5% never) [Oe18]. Thus, our sample seems to capture adequately the ATM-usage pattern of the general Austrian population.

3 Results

This section states and discusses the results of the conducted online survey.

3.1 Opinions on ATM-Security

Main arguments in favour of the use of ATMs with biometrics often refer either to gains in security or in usability compared to established authentication methods. In our sample, the majority of respondents (67%; grade 1+2) consider the established authentication method for common ATM cash withdrawal as "secure" (cf. Fig. 1).

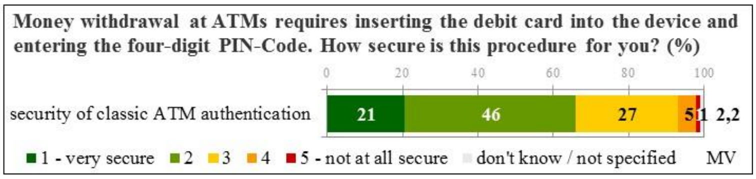

Fig. 1: Estimation of security of classic ATM authentication in Austria

3.2 Attitude and Knowledge towards Biometrics in General

To ensure a common understanding, biometric procedures of authentication were described as “measuring body characteristics of persons to distinctly recognise persons and to allow access to areas and devices”. After this introduction, respondents were asked regarding their attitude concerning biometrics in general (cf. Fig. 2). Depending upon the wording, approximately 11%-13% voiced strong rejection of biometrics (grade 1), with additional 10%-20% having voiced at least some concerns (grade 2).

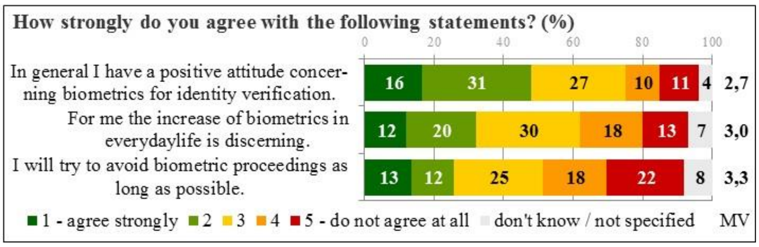

Fig. 2: Attitude towards biometrics

Technical sociology studies pointed out the so-called “digital gap”: participation in technological progress (especially modern information technology) is not distributed equally amongst all members of society, but is often differentiated according to sociodemographic characteristics, especially age and gender [Pe13,Se12]. Our results show a gender effect according to attitude towards biometrics (e.g. 53% of male respondents agreed to having a positive attitude towards biometrics for identity verification, but only 40% of female respondents; with less distinct differences for the other items). Differences according to age were less distinct. It is important to keep in mind that the interviews were conducted as online interviews. Therefore, especially the more elderly respondents are not necessarily representative for the whole of elderly people, because of the thus induced pre-selection of respondents towards higher affinity for modern information- and communication technologies. This affects older age groups more than younger ones, for whom internet-usage is living practice in Austria.

Knowledge about new technology can help raise acceptance, as it tends to meliorate diffuse anxieties [Ra09]. Respondents were asked to rate their knowledge of biometrics on a scale from “1 – extensive knowledge” to “5 – very small knowledge”. While 23% reported to have (some) knowledge about biometrics (grade 1+2), 40% claimed to have only (very) small knowledge of biometrics (grade 4+5). Major parts of the Austrian populace therefore do not consider themselves well informed concerning biometrics. Higher self-rated knowledge (grade 1+2) was associated with male respondents (33% versus 12% of female respondents), with younger age and higher education (below higher-secondary-education: 19%; higher-secondary-education or university: 33%).

In our sample, 80% of respondents claimed to have experiences with at least one kind of biometric procedures (targeting eyes, face, fingerprints, finger- or hand veins), with fingerprint recognition being the modus respondents were most familiar with (experienced by 74% of respondents).[6] Those with experiences with biometrics reported better knowledge of biometrics (with experiences: 27% grade 1+2; no experience: 8% grade 1+2), were less inclined to avoid biometric proceedings as long as possible and were more open towards biometrics for identity verification. However, there were little differences towards finding the increase of biometrics in everyday life discerning.

3.3 General Attitudes and Preferences towards ATMs with Biometrics

After being shown a short, simple introduction text explaining the concept of ATMs with biometrics[7], respondents were asked about their general opinion (cf. Fig. 3).

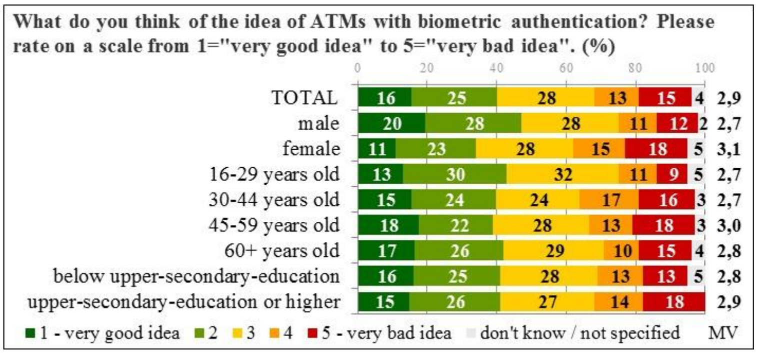

Fig. 3: General attitude towards ATMs with biometrics

16% expressed a strongly favourable attitude (grade 1), further 25% were still somewhat favourable (grade 2). 28% expressed (somewhat) strong reservations (grade 4+5). Male respondents were more favourably inclined than female ones, and there is no clear pattern according to age. This might be due to the survey being conducted via internet, so that especially the elderly participants were above-average innovation- and biometrics-friendly. Those with experiences with biometrics (45% grade 1+2) were also more favourable inclined than those without (27% grade 1+2).

Initially, when asked whether they preferred biometrics technology for ATMs requiring physical touch to the device or operating touchless, 25% preferred touchless, 15% with contact, and 33% would equally agree to both options (with 21% again voicing rejection of ATMs with biometrics and 6% who “didn’t know”). Nonetheless, after being

[6] Since 2009 capturing the fingerprint is mandatory for receiving the EU passport in Austria, which might explain this high percentage.

[7] The description included a short explanation of the enrolment process in a branch bank (identifying oneself in a bank office and being assisted by a clerk in the capturing of the respective biometric trait from which a score will be computed and recorded). In addition, biometric ATM were characterised as again capturing the respective biometric trait and computing the score in a likewise manner and then comparing this score with the one that has been computed during the enrolment process. If the scores match, access is granted.

confronted with exemplary pictures of ATMs with different biometric technologies, at the end of the survey finger-print-based ATMs (described as requiring contact) received the most favourable acclaim (cf. Fig. 4), with touchless vein-based technology a close-second. Especially the ratings for “10 – definitely” should be considered as the measure for real intention to use the technology, with scores between 8-9 showing a generally positive attitude already. The results for the “contact/touchless”-preference taken together with the results concerning preference for distinct biometric technologies for ATMs indicate that there is no strong majoritarian preference for either of those solutions in the Austrian populace.

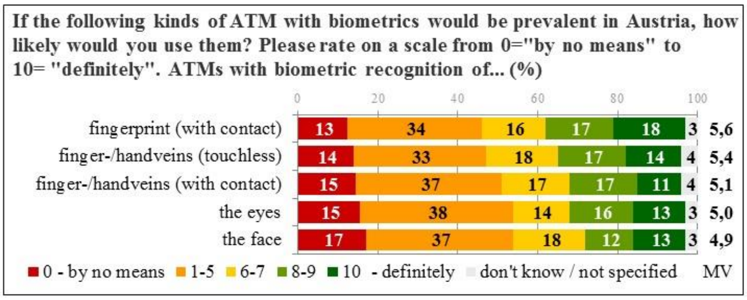

Fig. 4: Self-rated likelihood of using ATMs with biometrics

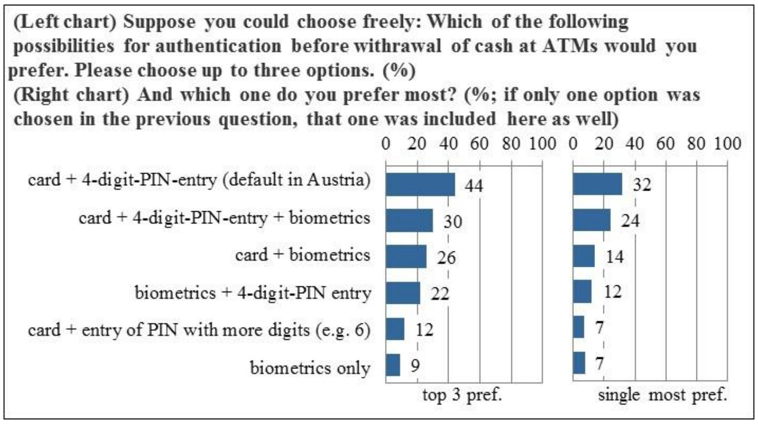

Fig. 5: Overall-authentication preferences

When asked to choose among several options for authentication (for the sake of information and regardless of potential difficulties for factual implementation; cf. Fig. 5), 44% of the respondents selected the default-method in Austria (card+4-digit-PIN-entry) amongst their three most preferred methods, and 32% as their single most preferred one. Interestingly, the probably more convenient solution “card+biometry” only ranked third (chosen by 14% as most-preferred), while the arguably more secure albeit slower method of combining card, PIN-code and biometry was chosen as the second most preferred overall (by 24%). Preference for the implementation of biometrics was higher amongst those with reservations concerning the security of the default-method and among those with reported experiences with biometric procedures.

3.4 Perceived Risks, Motivators and Barriers

Respondents were asked how strongly they agree with a set of statements concerning security and privacy issues connected with the discussed technologies (cf. Fig. 6). From the issues asked, clandestine use of biometrical data by the operating banks was the most prominent one (with 27% of respondents voicing strong and additional 19% somewhat strong concerns). Similarly prevailing were the concerns about data stolen or forged. Less prominent was the danger that biometrical data could be used to make further inferences about the client (strongly acknowledged by 15% of respondents). Those results indicate strong reservations which must be tackled by corresponding information in case of a roll-out of such technology.

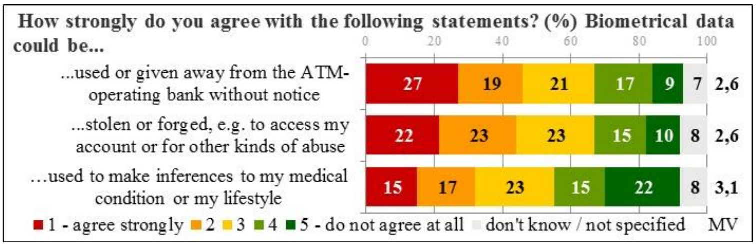

Fig. 6: Security and privacy issues

Respondents were also given (prior to the questions above) the chance to express their thoughts concerning possible advantages or disadvantages of ATMs with biometrics compared to common ATMs by answering semi-open questions ("none" and "don't know / not specified" were offered as options in addition to an otherwise unrestricted input field). Answers have been thematically grouped. 32% of total respondents pointed at possible gains in security. Furthermore, 5% (also) said that it would solve the issue of forgetting the PIN-code, further 4% expressed hopes regarding enhancements of convenience, usability or speed. However, 27% chose the "no advantages"-option and further 34% "didn't know".

The most frequently raised doubts involved concerns about data security or data privacy (9%), as well as lack of faith in the technology (e.g. being prone to malfunction; 9%). 6% had concerns about the general security of the new technology. For 6% it would be disadvantageous that with (only) biometrical authentication they could not pass their card and their PIN-code to other persons who could withdraw money for them (which might apply in cases of elderly or sick people). The possibility that such ATMs could be slower or less hygienic than regular ATMs was only expected by approximately 1% of the respondents. 25% chose the option "no disadvantages", and 45% "didn't know".

3.5 Limitations

With the survey being conducted online, only respondents with internet-access were questioned. While this does not strongly affect lower age groups as internet-usage amongst them is very common, it can be expected that there is still a selection-bias on the inclusion of older respondents, who can therefore be expected to be above-average technically-inclined for their age group. Respondents of higher age are not frequent in online pools. Therefore, the age of the respondents in the given study was capped at 80. Hence, the results are indicative of the populace up to the age of 80. Also, as the survey was conducted in German language, only those with skills in that language could participate. As there are currently no ATMs with biometrics available in Austria, the results of this survey are hypothetical as in all pre-implementary-research, where respondents do not have “first hand experiences” with a technology. Studies have shown the impact of those experiences in shaping intentions for further usage also in the field of biometrics technology [Ba15]. In addition, apart from intention and attitudes, actual usage is also influenced by many other factors, e.g. private and social norms, as well as the concrete technicalities of a device at hand. However, “intention to use” is often used instead of “factual usage” in technology acceptance research, and studies have shown that intention and factual usage have mediocre up to strong correlation with each other [TT95]. Therefore, the answers given in this article are still strongly indicative. Finally, as only respondents owning and at least occasionally using debit cards have been included in the survey, the answers here cannot claim to be representative for the whole Austrian population, but are tailored towards actual debit-card-users.

4 Legal Aspects

This section discusses the legal aspects related to the employment of biometric technology at ATMs and the processing and storage of the biometric data with respect to the current legislation in Austria and the European Union.

4.1 Legal Base for Processing Biometric Data

The legal base for processing biometric date is the same in Austria as in the European Union as the general data protection regulation (GDPR) is directly applicable for data processing in all member states of the European Union.

According to Article 4 (14) GDPR ‘biometric data’ means personal data resulting from specific technical processing relating to the physical, physiological or behavioural characteristics of a natural person, which allow or confirm the unique identification of that natural person, such as facial images or dactyloscopic data.

As regulated in Art. 9 GDPR (‘biometric data for the purpose of uniquely identifying a natural person’) biometric data is to be considered sensitive personal data, respectively special categories of personal data. This article of the GDPR calls for a higher level of protection on those categories of personal data. As such, their processing is prohibited under GDPR, unless one of the exceptions provided in Art. 9 Para. 2 GDPR are applicable. The most important are:

- If consent has been given explicitly
- If biometric information is necessary for carrying out obligations of the controller or the data subject in the field of employment, social security and social protection law
- If it is necessary to protect the vital interests of the individual and he/she is incapable of giving consent
- If it is vital for any legal claims
- If processing is necessary for reasons of substantial public interest, on the basis of Union or Member State law which shall be proportionate to the aim pursued
- If it is necessary for reasons of public interest in the area of public health.

At the present stage there are no specific Union or Austrian laws regulating the processing of biometric data for identification purposes. Therefore the only exception in Art 9 Para 2 which applies to biometric authentication in the context of ATMs is the explicit consent of the data subject.

As of Art 4 (11) ‘consent’ of the data subject means any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her. The term ‘explicit’ refers to the way consent is expressed by the data subject. Explicit consent means that the data subject must give an express statement of consent, for instance in a written statement. It must be taken into account that the legal basis of an explicit consent comes with a range of consequences such as the data subject’s right to withdraw consent but also with the duty of the data controller to be able to demonstrate that the data subject has given consent.

In addition to the explicit consent as the legal basis, data controllers (for the purposes of ATMs: banks and credit institutions) should also assess whether the processing of the personal data in question is necessary for the purpose pursued, which cannot be achieved by any other less intrusive means. The GDPR requires data controllers to limit the amount of personal data they collect and further process to what is relevant, necessary and adequate to accomplish the purposes they pursue. This requirement of data minimisation is especially relevant in the processing of sensitive data, such as biometric data in the given context. Data controllers should always verify whether there are alternative means, which are less intrusive to the data subject, and by which they could achieve their purposes.

In terms of processing, the European Commission (Justice and Consumers) Article 29

Working Party (WP29) has provided relevant guidance on developments of biometric technologies (the Article 29 Working Party is the predecessor of the European Data Protection Board under the GDPR). For example, in terms of biometric data, the WP29 is of the opinion that generally speaking biometric systems related to physical characteristics which do not leave traces (e.g. vein pattern recognition) or do not rely on the memorisation of the data, create less risks for the data subjects and, thus, are more likely to pass the proportionality test [WP193].

4.2 Other Measures to be taken by the Data Controller

Data controllers are obliged by the GDPR to take several measures especially when special categories of personal data are concerned which is the case in the given context.

Transparency and Information of the Data Subject

According to the principle of fair processing, data subjects must be aware of the collection and/or use of their biometric data (Art. GDPR). Any system that collects such data without the data subjects' knowledge must be avoided. The data controller must make sure that data subjects are adequately informed about the key elements of the processing in conformity with Art. 13 GDPR, which includes: their identity as controller, the purposes of the processing, the type of data, the duration of the processing, the rights of data subjects to access, rectify or cancel their data and the right to withdraw consent and information about the recipients or categories of recipients to whom the data are disclosed. As the controller of a biometrics system is obliged to inform the data subject, biometrics must not be taken from the data subject without his/her knowledge.

Technical Measures

Pursuant to the GDPR, data controllers should take relevant technical and organisational measures even by default and by design. This obligation is especially relevant in cases of processing of biometric data, which include the use of new technologies. More specifically, biometric data may be used by means of new technology, as a way of authentication of the identity of individuals. As technology evolves, it becomes more apparent that special measures should be enforced in order to protect individuals from malicious theft of their biometric data. Moreover, the collection and further processing of these types of personal data adds extra security obligations on organisations that use the data, especially they need to provide enough evidence of their need. Examples of technical measures are: biometric data should be stored as biometric templates whenever that is possible. Whenever it is permitted to process biometric data, it is preferred to avoid the centralised storage of the personal biometric information [WP193, p. 31].

Data Privacy Impact Assessment

As processing of biometric data will, in most cases, involve the use of new technologies and be conducted on a large-scale basis, its performance will usually need a Data

Privacy Impact Assessment (Art. 35 GDPR) to be conducted. In such cases, data controllers should be in the position to identify the risks of processing and set in place adequate measures to mitigate them.

Data Protection Officer

Pursuant to the Art. 37 GDPR the controller and the processor have to designate a data protection officer when processing biometric data on a large scale.

4.3 Specific Biometric Systems and Technologies

The Opinion 3/2012 on developments in biometric technologies of the Article 29 Working Party [WP193] contains comprehensive references to the following specific biometric systems and technologies:

- Vein pattern & combined uses
- Fingerprints & combined uses
- Facial recognition & combined uses
- Voice recognition & combined uses
- DNA and
- Signature biometrics.

5 Conclusion

This article showed that there are only weak security concerns towards the common authentication method at ATMs in Austria. Furthermore, 12% of the respondents voiced strong concerns towards biometrics in general (with depending on the question additional 10-20% being somewhat concerned). However, three quarters of respondents do not consider themselves well informed about biometrics. Towards ATMs with biometrics, 28% have reservations, 41% are positively inclined (rest undecided or between). There is no strong preference for certain biometrical approaches. (Data) security and privacy concerns are amongst the most common perceived risks. Gains in usability or in speed of ATM-usage was less strongly perceived as an advantage than gains in security, though as the established system is perceived as quite secure that lever of adoption can be assumed to not play a critical role in a hypothetical rollout of ATMs with biometrics.

Although the survey was conducted in Austria, it can be assumed that many results can also be transferred to the German population due to the cultural similarities and similarities in the sector of financial services. The legal framework and regulations as discussed in the paper are the same throughout the European Union.

Acknowledgements

This project was funded by the FFG KIRAS project AUTFingerATM under grant No. 864785.

References

[Ba15] Blanco-Gonzalo, R.; Sanchez-Reillo, R.; Ros-Gomez, R.; Fernandez-Saavedra, B.: User Acceptance of Planar Semiconductor Fingerprint Sensors. 2015 International Carnahan Conference on Security Technology, pp.31-36, 2015.

[CDJ03] Coventry, L.; De Angeli, A.; Johnson, G.: Usability and biometric verification at the ATM interface. Proceedings of the SIGCHI conference on Human factors in computing systems, pp. 153-160, 2003.

[He05] Han, F.; Hu, J.; Yu, X.; Feng, Y.; Zhou, J.: A Novel Hybrid Crypto-Biometric Authentication Scheme for ATM Based Banking Applications. Springer Lecture Notes in Computer Science 3832, Advances in Biometrics, pp. 675-681, 2005.

[He08] Hemery, B.; Mahier, J.; Pasquet, M.; Rosenberger, C.: Face Authentication for Banking. First International Conference on Advances in Computer-Human Interaction (ACHI 2008), pp. 137-142, 2008.

[HM12] Hosseini, S. S.; Mohammadi S.: Review Banking on Biometric in the World’s Banks and Introducing a Biometric Model for Iran’s Banking System. J. Basic. Appl. Sci. Res., Volume 2, Issue 9, pp. 9152-9160, 2012.

[Pe13] Pelizäus-Hoffmeister, H.: Zur Bedeutung von Technik im Alltag Älterer. Theorie und Empirie aus soziologischer Perspektive. Springer Verlag, Wiesbaden, 2013.

[Se12] Segert, A.: Informationspraktiken Technikaffinität und Alltagsmobilität. Institut für Höhere Studien, Wien, 2012.

[Oe18] OeNB-Barometer 2018. Zahlungsverhalten und neue Zahlungstechnologien. Tabellenband: 2. Halbjahr 2018. Institut für empirische Sozialforschung, Wien, 2018.

[Ra09] Riley, C.; Buckner, K.; Johnson, G.; Benyon, D.: Culture & biometrics. Regional differences in the perception of biometric authentication technologies. AI&Society, Volume 24, Issue 3, pp. 295-306, 2009.

[TT95] Taylor, S.; Todd, P.A.; Understanding Information Technology Usage: A Test of Competing Models. Information Systems Research, Volume 6, Issue 2, pp. 144-176, 2001.

[WP193] European Commission (Justice and Consumers) Article 29 Working Party (WP29). Opinion 3/2012 on developments in biometric technologies, 00720/12/EN, WP 193, adopted on 27th April 2012.