Journal of Business Economics and Management ISSN 1611-1699
2006, Vol VII, No 4, 243–249

INNOVATIVE METHODS TO ENHANCE TRANSACTION SECURITY OF BANKING APPLICATIONS

Gregor Költzsch

University of Applied Sciences Stralsund, Zur Schwedenschanze 15, 18435 Stralsund, Germany
E-mail: Gregor.Koeltzsch@gmx.de

Received 20 March 2006; accepted 19 September 2006

Abstract. The increasing number of identity theft incidents such as credit card fraud, card duplication and internet attacks threaten the banking business that is mainly based on customer trust. Information and communication technologies create new business opportunities and innovative applications but do also enable new attack scenarios. Therefore, maintaining security and integrity is essential for the future economic success of banking.

Biometric technologies such as fingerprint and facial recognition provide the means to enhance banking security. They are concerned with the measurement and evaluation of human physiological or behavioral data. Although the security-oriented use of biometric technologies has become the most important field of development, they also enable a variety of convenience-oriented use cases and applications. The article describes the security issues raised by technology-based banking applications and outlines the idea of biometric technologies. Eventually, potential security and convenience-driven use cases for biometrics in banking are illustrated based on examples given by a variety of professional project reports, magazines and other sources.

Keywords: **b**iometrics, biometric technologies, banking, security systems, banking security.

1. New security threats to banking

Trust is the basis of the banking sector's success. Banks have been an attractive target to fraudsters since the beginning of modern financial management in the Renaissance. The success of eCommerce and electronic banking has raised new security issues that were not known in traditional banking business. The virtual nature of transactions and the increasing automation of financial processes have generated virtual crime. The new telecommunication media used for virtual transactions do also imply the potential for fraudulent use, and must be secured against fraud.

For the last years we have seen a growing number of phishing, card fraud and other identity theft incidents.

According to the United States Federal Trade Commission, identity theft and the misuse of the data was the issue of 40 % of all frauds reported in the United States from 2002 to 2004. 46 % of these cases were related to bank accounts, credit cards and other financial transfers [1]. The yearly amount of loss due to credit card fraud reaches USD 4 billion [2]. On the one hand, financial institutions seek after methods and technologies to enhance virtual transaction security. On the other hand, innovative technologies also provide the measures to enhance physical security in the banking sector.

The implementation of biometric technologies in banking processes has been discussed for years but in practice, only few installations have been successfully introduced. In the present article, an introduction to biometric technologies is provided. Potential application fields and selected examples of biometrics in banking security will be described, and the success perspectives will be discussed.

2. Introduction to biometrics

The term biometrics derives from the Greek words "bios" (life) and "metron" (measure). In a broader sense, biometrics can be defined as the measurement of body characteristics or biological statistics [3]. Criminal prosecution, identity management and police records have used biometric data like facial pictures, body height and finger prints for a long time [4]. Research on computer-based, automated recognition

started in the 1960s, and the first commercial use, a fingerprint application at a bank, took place in 1968 [5]. In the present article, the term "biometric technologies" refers to automated methods of recognizing a person based on physiological or behavioral characteristics [6].

Recoll, that traditional authentication methods are based on knowledge, e.g. a PIN or a password, or possession, e.g. a key or a smart card. Any person knowing the secret or possessing the key can use the identity. A system that is based on knowledge or possession is not able to verify if a user is actually the person he/she claims to be.

Therefore, traditional PIN and password solutions are not sufficient for identification purposes [7].

Biometric methods are based on physiological or behavioural characteristics. Since they take advantage of mostly unchangeable characteristics, they are more reliable than traditional methods of authorization. Automated systems based on biometrics to recognize persons enable fast, user-friendly and highly secure identification and verification processes. The most-used biometric data are individual physiological characteristics such as the fingerprint, the facial image and the iris image. In comparison to these physiological characteristics, the signature and the voice do also include behavioral aspects [8].

3. The economic perspective – biometrics in the financial services industry

At least since 11 September 2001, the international community supports the development and implementation of biometric technologies. The market environment is influenced by political actors like the United States of America, the European Union, and Japan. Triggered by security concerns and international terrorism, public interest in these technologies has increased constantly over the last years. The needs to improve border protection, issue more secure identification documents and enhance security at public places have strengthened the development and market penetration of biometric products. Biometric technologies are of particular economic interest because they are widely applicable, connected to political and security-related interests and have a strong interdependency with other security technologies. Forecasting the international and national biometric markets is difficult considering the high diversity of analysis results in international studies but significant market studies forecast world market growth at an annual rate of 30 to 60 % [9]. The commercial relevance of biometrics is particularly high because they are usually part of large systems and combined with other technologies that are necessary to exploit their advantages, e.g. storage and processing mediums such as servers and smart cards, as well as communication technologies such as Radio Frequency Identification (RFID). The pure biometric recognition itself has no immediate value.

The usage of biometric technologies in the financial services industry and, particularly, the banking sector has been discussed for years because the potential application fields seem to be very promising. Since the first installation in 1968, banks have evaluated biometric technologies for their security purposes. According to the International Biometric Group, the revenue generated with biometrics in the financial service industry will reach USD 405.5 million in 2008. A large portion of this revenue will be generated in the banking sector. Growth is primarily supported by the various authentication requirements in existing applications for bank employees and customers [10].

However, until today the implementation of biometric technologies in the banking sector has not been successful on a large scale. Most applications focus on employee authentication, e.g. access control to security areas, vaults, etc. The few existing customer applications focus on access to safe deposit boxes and other stand alone approaches. Only few complex biometric intra-bank biometric identification systems have hardly been installed, and inter-bank systems involving a group of banks are even more difficult to realize than proprietary banking security solutions.

We can identify several reasons for this: First, the banking sector is not very open to new technologies because banks fear to scare conservative customers. Second, banking systems are highly complex and require intense standardization. The more banks are involved and the more customer-centered the desired approach, the higher standardization and integration efforts will be. Consequently, customer-oriented solutions are still in the early stage of development and evaluation [11]. Third, the number of system users in closed, proprietary systems is relatively low, and the users change not very often, which eases system administration and maintenance. Biometric trials in banking security were characterized by [Fig]:

- Focus on access control,
- Focus on employees,
- Proprietary solutions,
- Small and stable user groups,
- High unit costs.

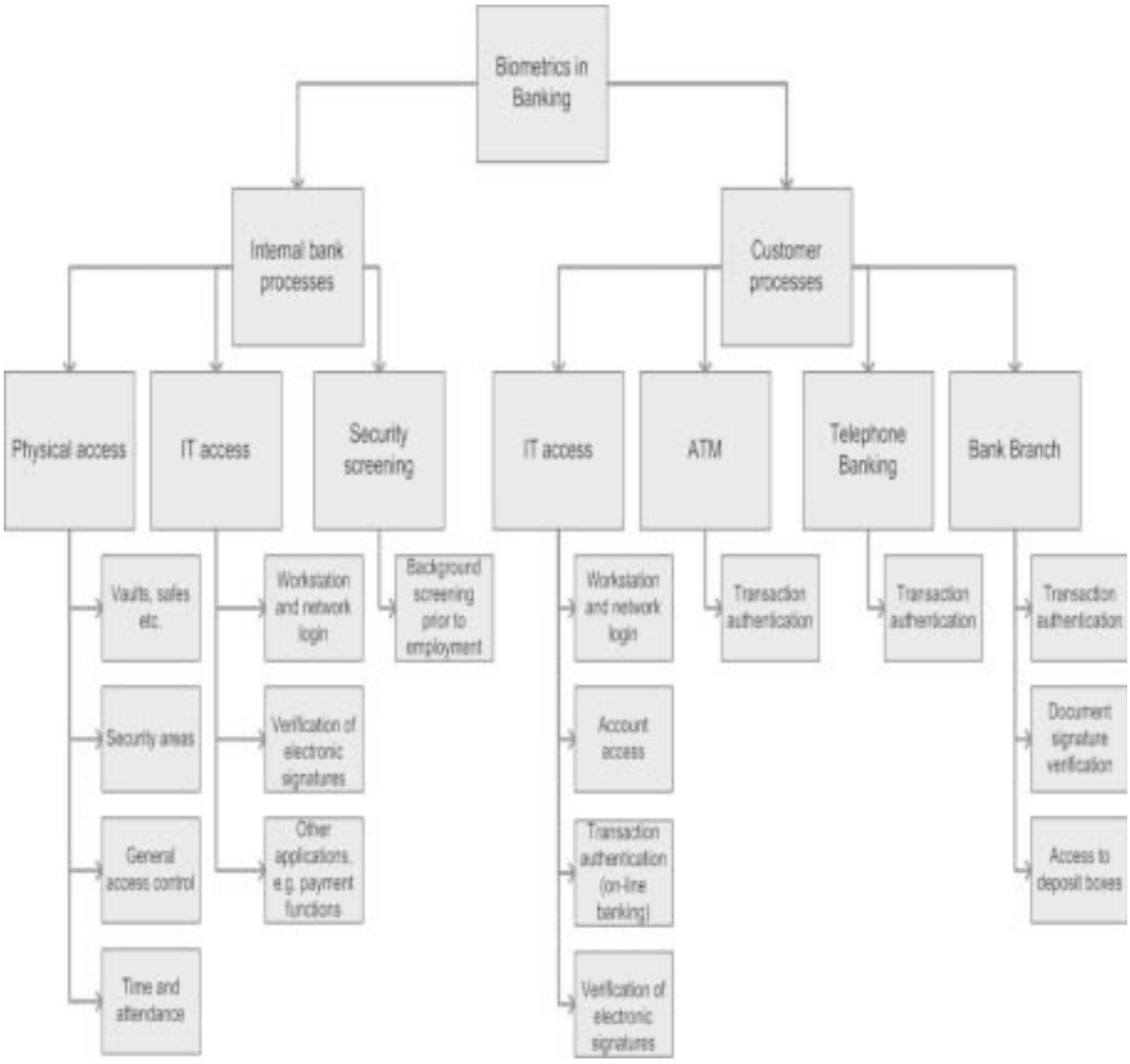
Although standardization issues are under discussion, it turns out to be a difficult task to agree on worldwide technological standards for biometrics in banking. Implementing a biometric solution, banks and security providers still take the risk to invest in a "wrong" technological approach or solution. Nevertheless, international biometric standardization has made progress during the last years. Biometric standardization initiatives have started to create standards to implement biometrics in the financial services industry. The increasing number of phishing and identity frauds puts pressure on banks to implement transaction authorization processes that are more secure than the traditional PIN card methods, and we will see a growing number of trials in the next years. Recent surveys show that customers are willing to use biometrics in banking. According to a survey among UK banking customers, one third of banking customers would use biometrics to improve transaction security [12].

It is suggested to differentiate the application fields of biometrics by internal banking applications and customer-oriented applications.

4. Internal bank processes

Physical access

Considering internal bank processes, **physical access control** for employees used to be the first application field of biometrics, and it is still the most important today. The extent and characteristics of employee access control may vary from access to high securi-



Potential application fields of biometrics in banking

ty areas and vaults to general access control in the branch. **Time and attendance control** may be combined with access control.

There are different possibilities for data storage and processing. If the biometric reference data is stored and processed decentrally in the reading device, the user does not need an additional storage medium. During verification the user gives the biometric feature to the reading device, which matches the captured data with the stored reference data. This solution is the most simple because it does not require high integration effort.

Since reading devices may be stolen and biometric data may be compromised, many approaches focus on data storage at additional security mediums that are under the user's control, e.g. smart cards. The user applies the card to the reading device; the live data is captured and compared to the reference data stored on the card. Thus, the biometric data cannot be stolen from the reading device. The data on the card is secured with cryptrographic methods. Contactless smart cards (RFID) are the most preferred solution for access control today [13]. Another possibility is to store the reference data in a database. Data storage on secure storage mediums should be preferred considering the data protection perspective. Fingerprint, iris recognition and face recognition are likely to be the most used technologies in employee access control.

Today's trials mostly represent proprietary solutions in single bank branches. Large scale access control solutions for banks with numerous subsidiaries and thousands of employees will raise more complex and cost-intensive system development and integration issues. A higher level of interoperability is required because at different locations the system may have to interoperate with different processes, interfaces and routines. It is expected that biometric access control solutions become more attractive to banks if the market prices and unit costs of cards and readers drop further due to economies of scale and learning curve effects.

IT access

The second application field of biometrics in internal bank processes is IT access control. Access to **workstations and networks** such as desktops, notebooks and company networks may be secured with biometric technology. For example, Citibank evaluates fingerprint verification for employee PC log-in [14]. Access control may also be performed on the application level, e.g. if employees work with sensitive data and programs.

Biometric technologies may also be used to **verify electronic signatures**. Today the user of an electronic signature verifies him/herself against a signature card with a PIN. This verification process is based on possession of the card and knowledge of the secret PIN. A biometric verification could close the gap between the holder and the signature card.

Additonal benefits may be provided by interfaces to **other applications** such as payment functions, e.g. at company stores, canteens etc. If employees use their employee ID card for payments, the money value is usually stored on the card and could be secured with biometric methods.

Biometric IT access is still in an early implementation stage at banks. We will see an increasing number of implementations in future with the goal to strengthen the protection of sensitive data. Loss, exchange or theft of passwords will no longer be possible, and the number of support cases will diminish. Administrators can always verify who is logged in the system. However, the costs of biometric data management may be higher than access management based on password and PIN management. Banks should consider whether the additional security is worth extra costs or wait until the market prices fall further.

The most promising technologies for these applications will be fingerprint and signature recognition because the sensors can easily be integrated into the IT equipment and the technologies do work under difficult sourrounding conditions.

Security screening

In the United States most employees in financial services must undergo a background check prior to employment. A fingerprint is taken on ink basis and matched against official AFIS or other databases where ink-based fingerprint pictures of criminals or wanted people are stored [15]. This process can be conducted faster, cleaner, more reliable and more convenient with modern electronic fingerprint recognition technology. The quality of digitally enroled fingerprints is better compared to scans of ink-based fingerprints.

5. Biometrics in customer applications

Use cases involving the customer are more complex and more difficult to realize in comparison with internal bank processes because:

- The user community is not concentrated at a certain location like bank employees.
- Additional hard and software is necessary to perform biometric verification.

- Applications need to comply with various IT infrastructures, customization may be required.
- Users are not willing to spend a significant amount of money for biometric solutions.

Due to these reasons, the use of biometrics by banking customers lags behind biometric solutions in internal bank processes. Nevertheless, some application fields seem to be very promising:

IT access

Workstation and network login applications for customers are only partly comparable to the IT access in banks. The introduction of centralized biometric solutions using data bases and smart cards for login is too complex compared to the benefits. Customer IT access should be reasonable to choose decentralized verification solutions. For example, a computer or laptop may have an integrated fingerprint reader or a comparable external device, e.g. at the USB hub or included in the mouse. Fingerprint and signature recognition are most suited for this approach because the sensors may easily be integrated in the computer or workstation and work under the most conditions.

More effort should be spent for ***Account access and transaction authorization.*** Online banking is among the most important eBusiness applications, and it is the most attractive fraud target. Therefore, online banking should be secured appropriately. Many banking customers have experienced fraud attacks to PIN-TAN online banking, e.g. phishing and other identity theft. To increase the security of online banking, access to accounts and transaction authorization could be bound to biometric verification. An appropriate solution requires a secure storage medium for the reference data, e.g. a smart card, and a device that is able to read and process the data and perform secure communication. The most promising technologies are fingerprint and signature recognition.

Like in internal bank processes, biometrics could also be used for **verification of electronic signatures**.

The integration of biometric IT access control into customer processes is a challenging task for the industry. The diversity of hard and software infrastructures at the customers' side requires solutions that are scalable and adjustable but also highly standardized. A significant barrier is the need for additional hard and software at the customer's workstation, e.g. smart card readers and biometric sensors. It cannot be assumed that customers are willing to take the costs. Banks will also have to invest in a new service and maintenance structure to support the customers new hard and software.

The costs of biometric solutions for homebanking are still too high compared with the actual additional value. This inproportion will change the higher the damage due to fraudulent attacks in the banking business is, and the lower the equipment costs in future will be. It is also likely that future end devices will have integrated sensors and readers.

Another difficult issue is inconvenience. Debit and credit cards are not likely to be used to store the biometric reference data of the banking customer because banks do not wish to enable the user to read banking cards with home devices. Customers will have to use an additional signature card including biometrics, or even two additional cards if the biometric data cannot be stored on the signature card.

As soon as these issues have been solved, biometrics will enable convenient and secure verification solutions for large and widespread user populations. Banks should have high interest in supporting their customers with secure banking solutions to re-establish trust in online transactions.

ATM

Authorization of transactions at **Automated Teller Machines** used to be one of the first application fields of biometrics in banking discussed by a broad professional community. The idea was to store the biometric data on a debit or credit card [16]. Biometrics may also be used to authenticate customers at other self-service stations like kiosks and deposit boxes.

From 1999 to 2002, the TeleTrusT association accomplished the BioTrust project which was concerned with the evaluation of biometric technologies in the banking sector. The results demonstrated that biometric solutions at ATMs are complicated by the high organizational and technical effort to integrate biometrics in the existing ATM infrastructure [17]. The technological possibilities could not meet the expectations, and the costs for a complex biometric ATM transaction solution are still too high to be considered a practicable alternative to traditional PIN solutions.

For customer convenience, banks must agree on standards to guarantee that customers can use one card for verification at ATMS of different banks. The most intensive efforts to standardize and implement biometrics in banking have been made in Japan, and several tests and trials have been conducted by Japanese financial institutions, e.g. the Bank of Kyoto, the Juroku Bank, Japan Post and the Bank of Tokyo-Mitsubishi [18].

The results of the BioTrusT study show that the use of biometrics in ATMs will not be profitable in the mid-

term future. Prior to implementation in the field, more trials have to be conducted [19]. There are several barriers that prevent the use of biometrics for customer self-service banking. ATMs are integrated in bank networks that are highly complex and linked to other banks' networks. Integration to these networks requires high standardization and interoperability, which is typical for a mature technology. Moreover, integration requires investments in hard and software and causes costs for integration, biometric enrolment, user and administrator training, equipment of existing terminals etc. Eventually, costs may be higher than the benefits.

Depending on the damage by fraudulent attacks and the market prices for biometric solutions, the calculation may change in future. The integration of contact chips to debit and credit cards and the EMV standards[1] will further accelerate the use of ID technologies in banking.

Telephone banking

The use of voice recognition technology for automated customer verification in **telephone banking** is supported by the success of the call center business and the need to automatize banking processes to cut costs. In comparison to automated PIN-TAN verification, voice recognition has the potential to make telephone banking more secure. Another advantage is that banks do not have to handle calls from customers that have lost or forgotten their PIN or password anymore.

One barrier to the quick success of biometric telephone banking is system training. Since the system needs to train to the customer's voice, the user has to enrol at the bank to prove his/ her identity. According to the International Biometric Group, voice recognition technologies will be implemented for account access in automated telephone banking or call centers. The decisions of the large credit card institutes will strongly influence the further development of biometrics in the financial sector by setting standards [21]. It is expected that biometric telephone banking has a successful future.

Bank branch

Biometric customer applications in bank branches focus on **transaction authentication.** Transactions in the bank branch can be authorized by the customer with a biometric characteristic [22]. Fingerprint, face and signature recognition seem to be most practical for this application field. Another area of interest is **document signature verification.** A large percentage of identity fraud in banking is caused by falsified signatures on cheques, remittance slips etc. Signature pads can be used to capture and verify the signature directly in the branch. If the document has been signed manually, signature recognition technology may compare the written signature to stored reference data of the holder.

Access to safe deposit boxes and safes is one of the most popular customer-focused applications of biometrics in banking.

Customer-focused biometric applications in bank branches are easier to implement than ATM or homebanking applications because the customers come to the point of installation. This minimizes the necessary investments in hard and software as well as the integration efforts. Access to deposit boxes has been the first biometric application in banking, and it is likely to play an important role in the market in future. Considering signature recognition at teller transaction, there is a large intersection with existing technologies such as signature scanning and verification at checks, which may create cost synergies and also diminish inhibitions by bank responsibles to introduce the new technology.

6. Perspectives of biometrics in banking applications

We have seen that biometric technologies enable secure and convenient identification processes in banking applications and have the potential to increase user trust in virtual transactions. Employee and customer-oriented applications will both play a significant role but due to their complexity, high costs and logistics efforts, customer-focused applications have penetrated the financial service market less than internal bank applications.

In general there has been a clear tendency to more complex and integrated solutions for the last years. Most of the commonly used biometric identifiers are suited for usage in banking. There is no single technology, solution or product that serves all requirements in banking security. The reasonable choice of technologies and solutions depends on the area of use, and on the targets the user pursues.

Although banks are conservative and risk averse in their approach to new technologies, the increasing standardization, growing experiences with biometrics in other application fields like electronic ID documents, and the growing damage caused by ID theft and other

[1] EMV (Europay, MasterCard, Visa) is a standard for chip-based payment with debit and credit cards which was developed to improve security in card payment, compared to the existing magnet stripe standards [20].

fraud will facilitate the widespread use of biometrics in banking. It will be the security industry's task to develop and implement measures to protect eBusiness and maintain the banking customer's trust. Biometric technologies may be enablers to prevent identity fraud in banking in future.

References

1. National and State Trends in Fraud & Identity Theft January–December 2004 Federal Trade Commission, February 1, 2005, p. 70 and 11.
2. Stobbe, A. Biometrie – Wirklichkeit und Übertreibung. In: Deutsche Bank Research (eds) (2002), Economics Nr. 28 vom 22.05.2002, p. 1–12.
3. Nolde, V. Grundlegende Aspekte biometrischer Verfahren. In: Nolde, Veronika/ Leger, Lothar (Eds.) (2002): Biometrische Verfahren, Fachverlag Deutscher Wirtschaftsdienst, Cologne, 2002, p. 20.
4. Albrecht, A.; Probst, T. Bedeutung der politischen und rechtlichen Rahmenbedingungen für biometrische Identifikationssysteme. In: Behrens, Michael/ Roth, Richard (Publ.): Biometrische Identifikation; Grundlagen, Verfahren, Perspektiven, Verlag Vieweg, Braunschweig/ Wiesbaden, 2001, p. 31.
5. Amberg, M. et al. Biometrische Verfahren; Studie zum State of the Art, Friedrich-Alexander-University Erlangen-Nuremberg, Erlangen/ Nuremberg 2003, p. 5.
6. European Biometric Forum. Biometrics Lexicon. http://www.eubiometricforum.com/index.php?option=content&task=view&id=29&Itemid=46. (Download 08/05/2006).
7. Bellens, P. New ways to pay. In: Global Identification, Issue May 2005, p. 16–19.
8. BIOVISION Consortium. Roadmap for Biometrics in Europe to 2010. Roadmap to Successful Deployment from the User and System Integrator Perspective. Ipswich, 2003, p. 19.
9. International Biometric Group. Biometric Market Report 2003–2007, New York, 2003, p. 2.
10. International Biometric Group. Financial success for biometrics? In: Biometrics Technology Today, p. 9–11, Issue April 2005, Oxford 2005, p. 9.
11. Bruce, L. Banks not yet banking on biometrics. http://www.bankrate.com/yho/news/bank/20020723a.asp (Download 16.07.2006)
12. Sturgeon, W. 'We want biometrics' say bank customers. 6 May 2005. http://software.silicon.com/security/0,39024655,39130185,00.htm (Download 10.07.2006).
13. Cummings, N. Access Control Technology. In: Global Identification, Volume May 2005, Milano/ Bruxelles, 2005, p. 44–45.
14. Giesen, L. Biometrics: Ready for Prime Time? *Banking strategies*, Issue May/June 2006, Volume 82, Issue 3. http://www.bai.org/BANKINGSTRATEGIES/2006-MAY-JUNE/Biometrics/index.asp (Download 17.07.2006).
15. International Biometric Group. Financial success for biometrics? In: Biometrics Technology Today, p. 9–11, Issue April 2005, Oxford 2005, p. 10.
16. Karasu, I. Privatkundengeschäft und Banktechnologie: Meilensteine auf dem Weg ins Online-Zeitalter. In: Die Bank – Zeitschrift für Bankpolitik und Praxis, Issue 06/2005. http://www.die-bank.de/index.asp?issue=062005&art=400#biometrie (Download 10.07.2006).
17. BioTrust Summary 1999–2002. http://www.atbc.de/biotrust/ (Download 09.07.2006).
18. Zeidler, L. Wie Biometrie die Bankenwelt erobert. In: Geldinstitute, issue 02/2006, p. 44–49.
19. BioTrust Summary 1999–2002. http://www.atbc.de/biotrust/ (Download 09.07.2006).
20. Anonymous. FAQ – EMV. http://www.kartensicherheit.de/ww/de/pub/glossar_faq/emv.php (Download 17.08.2006).
21. International Biometric Group. Financial success for biometrics? In: Biometrics Technology Today, p. 9–11, Issue April 2005, Oxford 2005, p. 9.
22. Giesen, L. Biometrics: Ready for Prime Time? *Banking strategies*, Issue May/June 2006, Volume 82, Issue 3. http://www.bai.org/BANKINGSTRATEGIES/2006-MAY-JUNE/Biometrics/index.asp (Download 17.07.2006).