Journal of Computer Science 3 (5): 361-367, 2007
ISSN 1549-3636

Digital Identities and the Promise of the Technology Trio: PKI, Smart Cards, and Biometrics

A.M. Al-Khouri and J. Bal
Warwick University, United Kingdom

Abstract: This article looks at one of the evolving crimes of the digital age; identity theft. It argues and explains that if three key technologies were implemented together namely biometrics, smart cards, and PKI, then they can deliver a robust and trusted identification and authentication infrastructure. The article concludes that such infrastructure may provide the foundation for e-government and e-commerce initiatives as it addresses the need for strong user authentication of virtual identities.

Key words: identity theft, e-government, G2C, online authentication, biometrics, smart cards, public key infrastructure

INTRODUCTION

Identity theft has become the fastest growing crime in the world [1][2]. Undoubtedly, the expansion and increasing sophistication of identity theft threatens the adoption of many strategic information technology (IT) initiatives such as e-government and e-business [3][4][5]. Identity theft is an activity that takes place when an individual's personal details are taken over or stolen by someone else in attempt to impersonate him/her and have access to particular information or service, perform financial transactions, or even commit crimes. Identity theft has many and increasing links to organised crime.

As recently as 10 years ago, people would research to find someone who had died before they ever had a job. They would then apply for a copy of birth certificates in the names of those dead people, and use it to obtain other ID documents. However, with the advances in the field of information technology, identity theft has become much easier. For instance, more than 30 internet websites offer fake ID's for sales from as little as $40 for a social security card, $79 for a birth certificate and $90 for a driving license from any US state. Websites such as www.fake-id.org and www.phonyid.com offer driving licenses with similar security features issued by the US government from all the 50 US states for $100 each, as well as Canadian ID's. Several hundred dollars buys one a complete ID set, including a military ID and a college diploma.

Use of false identification is considered to be a significant threat to homeland security as well as personal and financial security of citizens. It is not easy to gauge the amount of identity fraud at this moment of time, however, the minimum cost to the economy in some countries is in excess of $40bn per annum according to some official studies carried out (see for example: Federal Trade Commission report released in 2004; UK Cabinet Office report released in 2002).

According to Gartner's recent study, about 15 million Americans were victims of fraud that stemmed from identity theft in the period from mid-2005 and mid-2006[6]. This represented an increase of more than 50 percent from the reported 9.9 million in 2003 by the Federal Trade Commission. Current research and studies refer to the advances and spread of computer technology as the main factor behind this dramatic increase in identity theft [7].

The literature shows that identity theft and fraud levels are increasing throughout the world (e.g., Canada, Australia, Britain, and Japan) with gigantic costs to victims and business[8]. Some countries have introduced identity theft legislation that recognises such crimes and puts penalties and additional imprisonment sentences[8]. However, countries around the world are realising that the legislation in itself cannot prevent or combat identity theft unless they adopt more effective and advanced solutions. One of the approaches pursued by many organisations both in government and private sectors is the employment of advanced technologies such as smart cards biometrics, and PKI. It is widely argued that if properly implemented, such technologies can provide secure and accurate identity verification, enhance the security of the system and protect the integrity and confidentiality of information. The next few sections will look at these three technologies and explore them in further detail.

Biometrics: Biometrics is defined as the science of using individual's unique physical, behavioural and biological qualities for identification purposes e.g., fingerprint, hand print, facial recognition, iris, voice pattern, etc. The first modern biometric device was introduced commercially over 20 years ago. Apart

Corresponding Author: A.M. Al-Khouri, Warwick University, UK.

from being non-transferable among individuals, biometrics do not provide data about the person; but rather, information of the person.

The biometric industry found a global market through smart card technology. Biometric identity cards are being adopted in many countries around the world. Analysts predict biometrics to boom in the next few years, referring to the recently released report from the International Biometric Group (IBG), which indicated that the global market sales of biometric technologies will grow from less than $1bn in 2003 to more than $4.6bn in 2008, with fingerprint scanning becoming the most dominant technology, as illustrated in Fig. 1 below. Governments and businesses are increasingly adopting biometric technologies in the belief that they will make identity theft and multiple identities impossible.

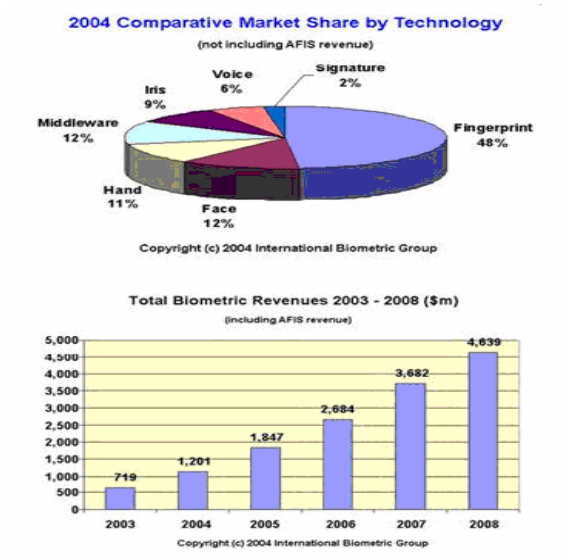

Fig. 1: Biometrics growth [9]

The National Physical Laboratory conducted a performance evaluation test of several biometric technologies for a scenario of positive identification involving the following biometrics: face, fingerprint, hand geometry, iris, vein and voice recognition. Iris recognition had the best accuracy, with 1.8 percent false rejections and no false matches in over two million comparisons as illustrated in Fig. 2 [10]. Of the other systems, fingerprint performed best for low false acceptance rates (FAR), while hand geometry achieved low (below 1 percent) false rejection rates (FRR). The study demonstrated that there is no one universal 'best' biometric system yet for both identification or authentication, rather a combination of two or more biometrics may enhance the FAR and FRR factors [11].

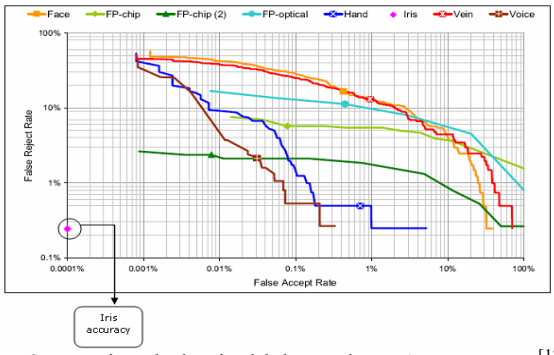

Fig. 2: National physical lab results: FAR vs. FRR [12]

In another evaluation, the UK National Physical Laboratory prepared a comprehensive feasibility study into using biometrics as a means of establishing unique identity, to support the proposed entitlement scheme under development by the UK Passport Service and Driver and Vehicle Licensing Agency [12]. The purpose of the study was to assess the feasibility of three main biometrics namely fingerprint, iris, and face recognition technologies as a medium of identification in a national identity scheme and assessing the associated risks, and forwarding recommendations. The feasibility study concluded once again that biometric methods do not offer 100% certainty of authentication of individuals and that the success of any deployed system using biometric methods depends on many factors such as the degree of the 'uniqueness' of biometric measure, technical and social factors, user interface, etc. However, and in principle, fingerprint and iris recognition were found to provide the identification performance required for unique identification over the entire UK adult population. In the case of fingerprint recognition, the system required the enrolment of at least four fingers, whereas for iris recognition both iris were required to be registered. However, the practicalities of deploying either iris or fingerprint recognition in such a scheme were found to be far from straightforward in terms of the complexity of implementation, user training, etc.

Other studies show that it is the device and the algorithm used that actually determine the effectiveness of the biometric in use. A recent study by the National Institute of Standards and Technology (NIST) revealed that fingerprint identification systems have approached 99 percent accuracy with some enhanced devices and, perhaps more importantly, a slim 0.01 false positive rate i.e., only about one in 10,000 scans resulting in a misidentification [13]. The study tested 34 fingerprint ID systems from 18 companies with about 50,000 sets of fingerprints from 25,000 people. The best systems reached 98.6 percent accuracy for a single-print match, whereas two-finger matches were accurate 99.6 percent of the time.

SMART CARDS: The 'smart card' is a plastic card with an IC (integrated circuit) chip capable of storing

and processing data that may come with optional magnetic strips, bar codes, optical strips, holograms, etc, on a variety of card bodies.

Developed in 1973 by the Frenchman Roland Marino, the smart card was not introduced commercially until 1981, when the French state telephone system adopted it as an integral part of its phone card network. This led to widespread use in France and then Germany, where patients have had health records stored on the cards. Table 1 provides a highlight on the developments of the smart card from the 1970s to-date.

Due to their capabilities, they are increasingly popular in many industries around the world most particularly in telecommunications, but also banking, transportation (e.g., vehicle registration and driving licences) healthcare, insurance, and e- governance. With the increasing need for security, smart cards are being viewed as the ideal medium for implementing a secure identification and authentication infrastructure [14][15].

Table 1: Smart card developments

1970s	Smart Card Technology invented by one of the Schlumberger companies (i.e., Axalto) to curb fraud
1980s	First commercial applications as a pre-paid memory card in the public telephony sector, followed by the banking industry which incorporated microprocessor capabilities
1990s	telecommunication industry adopted smart cards as SIM cards
Mid 1990s	advent of Open Platform cards e.g., Java cards (invented in 1996) which boosted multi-application cards, Usage of complex cryptography and become a medium to store, carry and transact with digital signatures. Introduction of contact-less technology and the invention of combi cards (contact + contactless) in 1996-97
Late 1990s	Applications based on contact-less technology and the invention of combi cards (contact + contactless) in 1996-97
2002	Invention of .NET technology in 2002 which led to the increase of smart card memory capacity to 512 K byte

Smart Card chips normally look like in the diagram below (Fig. 3), with an integrated circuit built into it. This integrated circuit may consist only of EEPROM in the case of a memory card, but may also contain ROM, RAM and a CPU.

As memory capacity, computing power, and data encryption capabilities of the microprocessor increase, many research studies indicate that smart cards are envisioned as replacing commonplace items such as cash, airline and theatre tickets, credit and debit cards, toll tokens, medical records, and keys. Fig. 4 provides further information about the emerging card technologies and their uses.

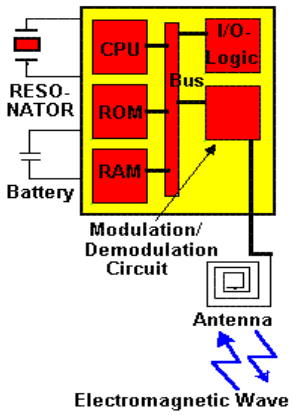

Fig.3: Types of Smart Card

Contact Cards	The most widely used one. They have to be moved past a reader i.e., require insertion into a smart card reader with a direct connection to a conductive micro-module on the surface of the card
Contactless Cards	Require only close proximity (a few inches) of a reader.
Combi Cards	Could be used in both situations. Their main attraction is that one card could fill many purposes, such as credit card, bank card, membership card, ID-card, etc, all in the same card

Smart cards are widely being adopted in many e-government and e-business initiatives as a vital element of a secure identification infrastructure and as a platform to hold both biometrics and PKI [16]. The next section will explain the PKI and its role in providing a higher trusted standard of authentication.

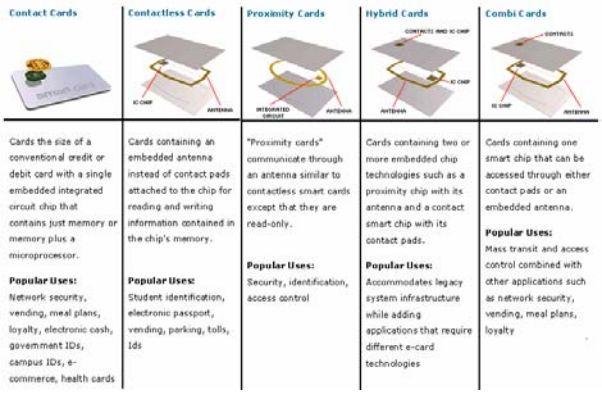

Fig.4: Emerging Card Technologies

Public Key Infrastructure (PKI): is a framework for creating a secure method for exchanging information based on public key cryptography. It is widely considered to be one of the prime components along with smart card and biometric technologies to enhance the overall security of systems. PKI is known to provide two main features: (a) security, and (b) encryption, to fulfil four vital requirements and establish what is called a trust environment (see also fig. 5):

1. authentication
2. confidentiality
3. integrity, and
4. non-repudiation

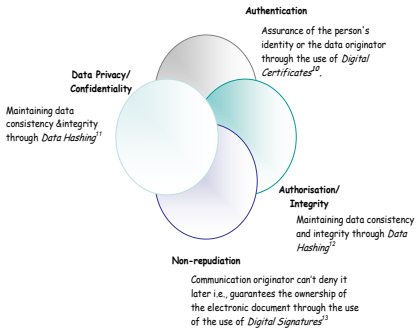

Fig. 5: PKI Trust framework

n a PKI environment, a pair of two different cryptographic keys is used for encryption and decryption purposes, referred to as public and private keys. The private key is kept secret by the user or in the system, and the public key is made public. The keys are mathematically related and could not be deducted from one another. Data encrypted with one key can be decrypted only wit the other complementary key and vice versa (see also Fig. 6).

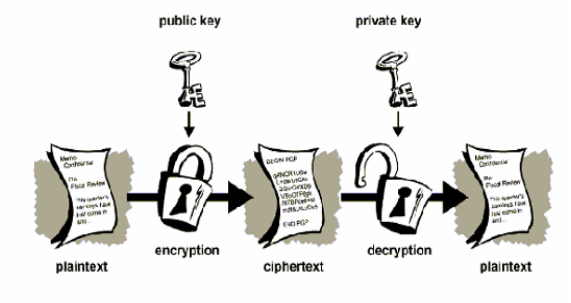

Fig. 6: PKI Trust framework

PKI encompasses a set of complex technologies as illustrated in Table 2 which shows the main PKI components. In a PKI environment, one would require a digital certificate, which usually contains the individual's public key, information about the certificate authority, and additional information about the certificate holder. The certificate is created and signed (digital signature) by a trusted third party; certificate authority (CA). The individual's identity is bound to the public key, where the CA takes liability for the authenticity of that public key, to allow a secure communication environment.

Table 2: PKI Architecture

Security Policy	• Defines requirements and standards for issuance and management of keys and certificates and the obligations of all PKI entities, and used to determine level of trust the certificate affords
Certification Authority (CA)	• Authenticate subscribers, issue & manage certificates, schedules expiry date for certificates and revokes them when the validity period expires.
Registration Authority - (RA)	• provides the interface between the user and CA. It verifies the identity of the user and passes the valid requests to the CA.
Certificate Distribution System	• is usually through a directory service. A directory server may already exist within an organisation or may be supplied as part of the PKI solution.
PKI Enabled applications	• is a cryptographic toolkit employed to PKI-enable applications e.g., communications between web servers and browsers, email, electronic data interchange (EDI), virtual private networks (VPNs), etc.

Source: Certicom - www.certicom.com

The registration authority (RA) is where the individual or the organization requesting the certificate is checked to ensure that they are who they claim they are. Another fundamental component of PKI is the certificate distribution system which publishes the certificates in the form of an electronic directory, database, or through an email to allow users find them. PKI enabled applications usually refer to applications that have had particular CA software supplier's toolkit added to them so that they are able to use the supplier's CA and certificates to implement PKI functions such as in emails and networks for encrypting messages. The certificate policy, also referred to as certificate management system, is where the certificate procedures are defined including the legal liabilities and responsibilities of the involved parties.

Digital Signature: Based on a range of encryption techniques, digital signature; one of the essential services of PKI allow people and organizations to

electronically certify such features as their identity, their ability to pay, or the authenticity of an electronic document. The digital signature also referred to as encrypted hashed text is a digital fingerprint; a value which is calculated from the information in a message through the use of a cryptographic hash function. Any change to the message, even of a single bit typically results in a dramatically different message digest. Figure 8 shows an example of a system generating a hash value from the message and encrypting it with the originator's private key. The message which could also be encrypted is sent along with the digital signature to the recipient who will then decrypt the digital signature with the sender's public key to change it back into a message digest. If the decryption was successful then it proves that the sender has signed the message, because only him/her has the private key. The recipient then calculates the hash value out of the received message, and compares it with the message digest. If the message digest is the same as the message digest created when the signature was decrypted, then the receiver can be assured that the signed message/data has not been changed or tampered with.

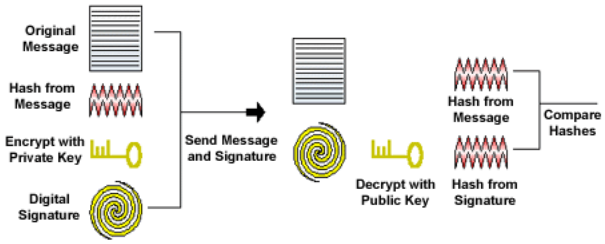

Fig. 7: PKI Trust framework

In their study to understand the PKI infrastructure and how it may support electronic authentication and e-governments, [17] adopted an organisational framework

to facilitate the understanding and classification of electronic services according to their security requirements (e.g. issuing birth certificates, submitting tax forms, conducting electronic payments, etc.). The findings of the study demonstrated that the security services offered by the public key infrastructure can be employed for fulfilling most of the identified security requirements for an integrated e-authentication platform and a one-stop e-government portal as illustrated in Table 3. However, other requirements like availability, performance, un-coercibiliy, un-traceability, and anonymity could not be fulfilled, and additional security measures were found necessary.

In addition, several studies have proved that PKI is the state-of-art technology in the field of digital authentication and overall security infrastructure [17][18][19]. Nonetheless, studies also show that PKI on its own will not provide maximum security for authentication unless it is incorporated with other security technologies such as smart cards, biometrics, virtual private networks, etc. [20][21][22]

The Application of the Technology Trio: As explained earlier, statistical data in the literature provides horrifying data about identity theft and how much it is costing both public and private organizations. In order to combat identity theft, organizations need the means by which they can accurately recognize peoples' identities in two main forms as illustrated in Fig. 8:

(a) identification (1:N) and
(b) verification - also referred to as authentication - (1:1).

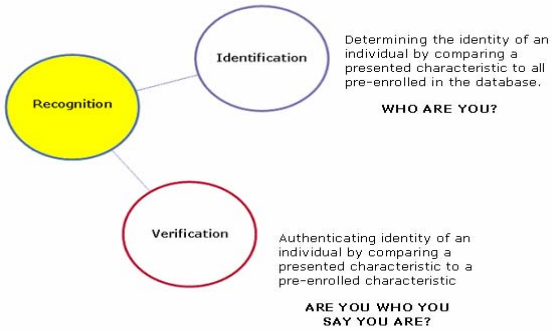

Fig. 8: Accurate identification/verification requirements

The technology trio of PKI, smart cards and biometrics is being widely considered to address the need for precise identification and authentication of individuals. They offer a solid business model that not only addresses high-level security requirements and strong authentication but also protects individual privacy and preserves resources. The adoption of these three technologies will create the two fundamental elements:

1. a trustful mechanism to identify and authenticate individuals, and
2. a secure communication and transactional environment.

Smart cards, for instance, can serve as the issuer's agent of trust and deliver unique capabilities to securely and accurately verify the identity of the cardholder, authenticate the ID credential, and serve the credential to the ID system [23]. PKI, on the other hand, has emerged as the most reliable framework for ensuring security and trust [24][25]. Apart from the main benefit of

PKI in enabling secure electronic transactions, PKI can also be used to encrypt the data stored in the chip (e.g., personal information, digital photo, biometrics, etc.), in addition to the data stored in the database, to limit access to only authorised persons and entities.

Biometrics allows the padlocking of the person to the card. In doing so, the card cannot easily be transferred to another individual. In particular, given the current focus on the use of biometrics in ID card systems, its sets out architecture for strongly-authenticated identity cards that deliver (perhaps counter-intuitively) both enhanced security and enhanced privacy.

Through the incorporation of these three technologies in an identity management system, individuals are not locked into one form of authentication, but rather three different forms of authentication (see also Fig. 9):

1. *knowledge factor:* a password to ascertain what one knows
2. *possession factor:* a token (smartcard) to ascertain what one has, and
3. *biometric factor:* biometric recognition (for example fingerprint or thumbprint) to ascertain who one biologically is.

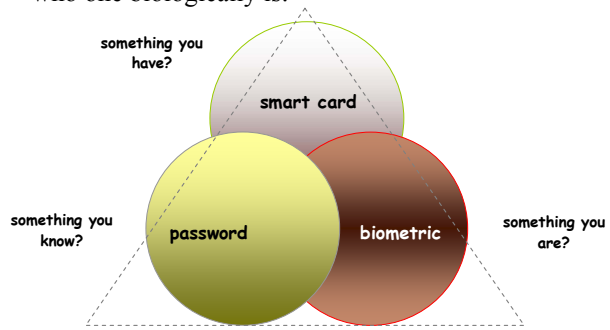

Fig. 9: Three factor authentication

As such, if one factor has been compromised, fraudsters need to pass through another two levels of authentication. By requiring three forms of identification to access credentials, organisations will be able to bind card holders' (digital) identities on the card to their physical identities.

From an e-government perspective, the key to G2C e-government is authentication i.e., the ability to positively identifying and proving the authenticity of those with whom the government conduct business with. Without authentication, other security measures put in place for many G2C transactions can be ineffective. The argument here is that for G2C e-government to progress, governments' need a strong online trusted authentication infrastructure, without which, their efforts is likely to standstill. In other words, governments need varying levels of authentication strength based on the value or sensitivity of their online information or services, balanced against other considerations like usability, deployment, and budget.

It is important to heed that the essence of G2C e-government is that transactions occur between people that are represented by machines. The anonymity of these transactions makes it more difficult to identify the parties involved and to ensure a trusted business relationship. Since all successful business relationships are based on trust, establishing online trust should be one of the primary goals of any e-government initiative[23]. The focus must be building a trust environment that provides a high level of data privacy, data integrity, and user authorisation. Nonetheless, and as mentioned earlier that the real cornerstone of G2C e-business trust is authentication: that is, knowing with whom the government is doing business with. PKI, smart cards, and biometrics are the technologies that are believed to be the key components of the trust model to address both electronic transactions security and online identity authentication. Using the power of the presented technologies in this article, government organisations and businesses alike can use varying levels of authentication depending on the level of security required for a particular transaction as depicted in Fig. 10.

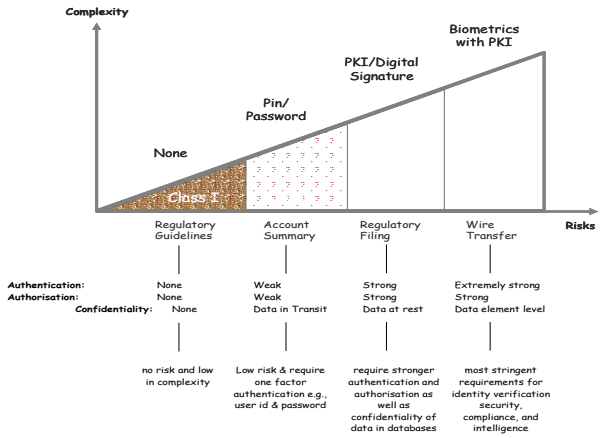

Fig. 10: An example of types of authentication for G2C e-gov services

CONCLUSION

Organisations will be better able to protect their systems and assets with the application of biometrics, smart cards, and PKI, that provides them with a better

verification of both physical and virtual identities. On the plus side, the principal advantage to be gained is more reliable authentication of identities. Without a doubt, strong user authentication must be viewed as the foundation for any e-government and e-commerce initiatives [17]. In fact, apart from improving traditional approaches to identification and authentication, these technologies are seen as the key to e-government, and a secure digital infrastructure. This utilisation of the three named technologies in this paper should have a profound positive impact not only in terms of the reduction of identity theft and fraud activities, but having such an infrastructure should enable the improvement of current government services and paving the way for more investment in electronic services. In short, the promise of the technology trio is colossal. Hopefully, future applications and developments, implemented in well managed products will prove this right.

REFERENCES

1. Briefel, A., 2006. The Deceivers: Art Forgery and Identity in the Nineteenth Century. Cornell University Press.
2. Shute, J., 2006. User I.D.: A Novel of Identity Theft. Mariner Books.
3. Adams, J., 2003. E-Fraud Fight Prompts Credit Agencies' Cooperation', Bank Technology News, vol. 16. no. 6., p. 14.
4. Marcus, R. Hastings, G., 2006. Identity Theft, Inc. Disinformation Company.
5. Middlemiss, J., 2004. Gone Phishing, Wall Street & Technology, August, pp. 38-39.
6. McCarthy, C., 2007. Study: Identity theft keeps climbing, CNET News.com. http://news.com.com/21001029_36164765.html
7. Zalud, B., 2003. Real or fake?, Security, vol. 40, no. 3, pp. 12-18.
8. Anonymous, 2003. ID theft tops fraud list again, ABA Bank Compliance, vol. 2, p. 5-6.
9. International Biometric Group, www.biometricgroup.com
10. Mansfield, T., Kelly, G., Chandler, D. and Kane, J., 2001. Biometric Product Testing – Final Report, National Physical Laboratory, UK, http://www.cesg.gov.uk/site/ast/biometrics/media/BiometricTestReportpt1.pdf
11. Mansfield, T., 2001. Biometric Authentication in the real world, National Physical Laboratory, UK, http://www.npl.co.uk/scientific_software/publications/biometrics/psrevho.pdf
12. Mansfield, T. & Rejman-Greene, M., 2003. Feasibility Study on the Use of Biometrics in an Entitlement Scheme for UKPS, DVLA and the Home Office, National Physical Laboratory, UK: http://uk.sitestat.com/homeoffice/homeoffice/s?docs2.feasibility_study031111_v2&ns_type=pdf
13. McCeary, L., 2004. The Fact of Fingerprints, The Resource for Security Executives, http://www.keep-media.com/pubs/CSO
14. George, T.C., 2003. The inside of a smart story: smart cards are increasingly becoming relevant in our everyday life, Businessline, Chenai, October 22, p. 1.
15. MacGowan, J., 2003. Smart Cards: Enabling e-Government, Bloor Research, http://www.itanalysis.com/article.php?articleid=11151
16. Gardner, S., 2004. Europe Get Smart, euro-correspondent.com, www.eurocorrespondent.com/ed-60_110704.htm
17. Lambrinoudakis, C., Gritzalis, S., Dridi, F., & Pernul, G., 2003. Security requirements for e-government services: a methodological approach for developing a common PKI-based security policy, Computer Communications, vol. 26, pp.1873-1883.
18. Conry-Murray, A., 2002. PKI: Coming to an enterprise near you?, Network Magazine, vol. 17, no. 8, pp. 34-37.
19. Critchlow, D. & Zhang, N., 2004. Security enhanced accountable anonymous PKI certificates for mobile e-commerce, Computer Networks, vol. 45, no. 4.
20. Ellison, C. & Schneier, B., 2000. Ten Risks of PKI: What You're not Being Told about Public Key Infrastructure, Computer Security Journal, vol. xvi, no. 1, pp.1-8.
21. Doan, 2003. Biometrics and PKI based Digital Signatures, White Paper, Daon , www.daon.com.
22. Kolodzinski, O., 2002. PKI: Commentary and observations, The CPA Journal, vol. 72, no. 11, p. 10
23. SCA, 2004. Secure Identification Systems: Building a Chain of Trust, Smart Card Alliance, www.smartcardalliance.org.
24. Hutchison, R., 2000. E-Government: Walk before you run, Canadian Business, Toronto, vol. 73, no. 16, p. 36
25. Russell, S., Dawson, Ed., Okamoto, E., & Lopez, J., 2003. Virtual certificates and synthetic certificates: new paradigms for improving public key validation, Computer Communications, vol. 26, pp. 1826-1838.
26. http://www.idedge.com
27. Al-Khouri, A.M. & Bal. J., 2007. Electronic Government in the GCC countries, International Journal Of Social Sciences, vol. 1, no. 2, pp.83-98.