A MORE SECURE E-COMMERCE ENVIRONMENT BASED ON A SELF-CONTAINED BIOMETRIC USB MEMORY STICK

Dariusz Janiszyn[1], Prof. S.H. von Solms[2]

Standard Bank Academy for IT, University of Johannesburg

[1] P.O. Box 2548, Cresta Center, 2118, South Africa

Tel: +27 11 791 0903, Mobile: +27 82 505 7638, Email: darek@xdesigns.co.za

[2] P.O. Box 524, Auckland Park, 2006, South Africa

Fax:+27 11 489 2138, Mobile: +27 82 553 2436, Email: basie@rau.ac.za

ABSTRACT

It is a known fact that any system is only as good as the weakest link. In an e-commerce environment, using the public key infrastructure, this weakest link is the end user. The average computer users are aware of security threats like viruses, trojans and spyware, but their limited computer knowledge doesn't allow them to identify or respond to these threats, often resulting in an insecure environment. This insecure environment can lead to the disclosure of sensitive personal data that is being stored/processed on computer like documents, passwords, banking details symmetric and asymmetric keys.

Advancements in the biometric fingerprint technologies allow the combination of a fingerprint reader and a USB memory stick to act as a secure mobile data storage device. The USB device has the ability to store data, generate fingerprint templates, do a comparison match on fingerprint templates and perform encryption of data on its own. With the biometric USB stick able to perform biometric identification on its own, we eliminate the need to transfer any authentication data to the host computer whereby we never release any fingerprint templates making it prone to digital spoofing. We now have a mobile and flexible means of protecting confidential information.

In the PKI a lot of emphasis is placed on the security of the private key. If we were able to securely store the private key on a biometric USB stick and perform all public key encryption on the memory stick the private key would never leave its secure and trusted processing environment.

This paper will discuss a research project which integrates the above described USB memory stick and the PKI environment to create a more secure e-commerce environment.

KEY WORDS

biometric, fingerprint, USB stick, encryption, secure storage, e-commerce, PKI

A MORE SECURE E-COMMERCE ENVIRONMENT BASED ON A SELF-CONTAINED BIOMETRIC USB MEMORY STICK

1 INTRODUCTION

What is E-Commerce? E-Commerce is any business that is conducted by two parties by means of an application through the use of the Internet. This business could be you checking the location of a FedEx parcel, doing electronic banking or purchasing products from a store that is on another continent.

Electronic commerce over the Internet is being talked about everywhere. It is already changing the way we do business and increasingly more people are trying to build a web presence in order to get a cut from the $5 trillion global e-commerce expenditure predicted for 2005 [10XM].

Most of these e-commerce services require you to eventually identify and authenticate yourself over the Internet to complete a transaction. With the Internet being an uncontrollable environment made up of millions of anonymous users, it is difficult to trust just anybody that has a website or sends you an email. There is however an infrastructure that can identify and authenticate Internet users, this solution comes in the form of the PKI. The public-key infrastructure (PKI) is the combination of software, encryption technologies and services that can provide necessary security in order for business transactions to take place over the Internet.

1.1 So what is the PKI? (Public-key Infrastructure)

The PKI integrates public-key cryptography, digital certificates and certificate authorities to offer wide network security. One of the crucial components of the PKI is the Public-key cryptography. Public-key cryptography consists of two mathematically linked asymmetric keys known as the private/public key pair and an asymmetric encryption algorithm.

It is called the public-key cryptography because the encryption key can be made public: Anybody can use the public key to encrypt a message but only the specific person with the corresponding private key decrypt the message. This works in reverse as well, if you encrypt a message with a private key only the corresponding public key can decrypt the message. By safely storing the one key secret (private key) and publishing the second key (public key) to a trusted public directory we are able to authenticate identity, verify integrity, ensure privacy, authorise access and support non-repudiation over the Internet.

The PK infrastructure relies on the availability and integrity of the public key as well as the secrecy of the private key. We make the public key widely available by submitting our details to a trusted certification authority. The certification authority then generates and publishes the digital certificates that link people and computers to a specific public key. If you want to send an encrypted message to a business partner you find his digital certificate at the certification authority, extract the public key from it and send him a message encrypted with his public key. If the private key was indeed kept secret only one intended person will be able to decrypt the sent message.

The whole public key infrastructure is a lot more complex and involves issues like key lengths, generating session keys, issuance managing, renewing, revoking, securing digital certificates etc. There are many different methods, techniques and algorithms that can be applied in the PKI but for brevity we will not go into it here.

1.2 PKI FLAW

If we generate keys to the recommended guidelines for asymmetric keys, it becomes infeasible to calculate the private key from the public key in any reasonable time. Brute force attacks on the strong encryption mechanisms takes way too long so other easier ways had to be found to exploit the PKI.

It is a known fact that any system is only as secure as the weakest link. In an e-commerce environment, using the public key infrastructure, the user is considered to be the so called “weakest link in the security chain” [FAPS]. In any online transaction you have the service provider computer, communication channel and the end user. The service providers’ servers are usually setup and maintained by IT experts that comply with various security standards and follow industry best practices. Confidential information can be safely sent over public communication lines with the use of strong encryption. The end user is however using a computer that is running an anti-virus, hopefully with the latest virus definitions and is under the impression that the computer is secure.

The average computer user is aware of security threats like viruses and spyware, but their limited computer knowledge doesn’t allow them to respond or even identify any of such threats, often resulting in an insecure environment. This insecure environment can lead to the disclosure of sensitive personal data that is being stored or processed on the computer. [COSJ].

The user is the biggest pitfall of the PKI but we can no longer blame end users for their ignorance or lack of knowledge but should rather develop a better solution for identification and authentication that can be used in the e-commerce environment by everybody.

2 PROBLEM OVERVIEW

The worst scenario in the PKI occurs when your private key gets stolen or worse copied. How can it happen? After receiving a digital certificate that was created by a Certification Authority this certificate together with your private key get stored on your computer. Your private key will be stored on your computer protected by a password or a pass phrase.

- By having physical access to the computer the private key can be used or copied. The password protecting the private key is created by the end user so the chances that the private key is protected by a strong password are very slim.
- If your computer isn’t properly secured your private key can be compromised by viruses.
- You can only use the private key from the computer that it is installed on and this often requires you to carry an unprotected copy of the private key. You then install the key onto a system that could be insecure or you forget to delete the key after you used it.

These are the problems which are usually faced with the management of the private keys.

3 AVAILABLE SOLUTIONS

There are solutions that do address the issues of private key management in the PKI. Some of them are software solutions whilst others hardware based. I will touch up on some of these devices.

3.1 Biometrics

This requires you to authenticate yourself with a biometric like your fingerprint, handprint retina scan etc. The only advantage biometrics carries with it is that the long password/encryption key protecting the key doesn’t have to be memorised by the user but instead it is replaced with something that the user is. This solution has the downfall that the private key and the password are both kept on the computer and can be spoofed. This solution also cannot be used on a large scale as compatible biometric devices and relevant software have to be installed everywhere and a central database of enrolled users has to exist. People are very reluctant to use public biometric devices because of the perceptions that associated with them, hygiene and the big brother effect [IAIA].

3.2 Smart Cards

Smart cards have the ability to securely store data like private keys. Access can be gained to the private key when a correct password is entered. In order for the necessary encryption to be done with the private key it has to be temporarily copied onto the host computer where it can be spoofed(new smart cards exist that can do public key encryption). Smart cards offer a secure storage device for private keys for people that need to use their private keys on different computers.

Downfall is that each computer needs to have its own smart card readers installed and the private key is protected by a password that can be spoofed from the computer. [BPSC]

3.3 USB Dongles

These small devices are made specifically for the PKI. They are used for onboard key generation, key storage and encryption. This is one of the best solutions available. You have high interoperability because it is a USB device, all encryption is done on the device itself so the private key never leaves the USB device. The only pitfall of this device is that the key is protected by a password that is created by the user. Whenever the user wants to use the private key like signing an email he will be prompted to enter his password. This password can then be spoofed by viruses etc. Like I mentioned earlier most passwords created by users are weak and can be easily cracked by brute force.

These are the most common found solutions which are available to the public. Each of them has their own advantages and their pitfalls but nevertheless they make the PK infrastructure more secure in their own way.

4 PROPOSED SOLUTION

My proposal is a combination of the above discussed solutions. The research I have conducted up to now indicates that the optimal solution would be a device that can do the following:

- Securely store data
- Be tamper proof
- Perform public key encryption
- Perform symmetric key encryption
- Generate keys
- Biometric identify and authentication

Whilst the device has to have complex functionalities the device still has to be interoperable, portable, true plug & play, self contained and most off all it has to be practical.

The device that I have attained for my research is a 128MB Thumbdrive Swipe USB memory stick made by Trek [TREK]. This device is basically a USB memory stick integrated together with a self contained capacitive biometric fingerprint reader [UPEK]. Trek was the first company to come out with a self contained Biometric USB device that doesn't need any preloaded software or drivers on the computer (USB drivers have to be loaded for Microsoft Windows 98 or older). This memory stick is a great device for secure data storage but besides the fact that it offers very high interoperability, high data storage and higher security of the data, it doesn't solve the PKI problem by itself.

The USB stick can already be used to securely store your private key and only the person with the enrolled finger can get access to it. Fingerprint enrolment, matching and storing is done on the USB stick so there is no way to digitally spoof the fingerprint unlike the possibility of spoofing passwords, pass phrases and biometric templates of the above mentioned solutions. What we want to accomplish is to fully integrate the USB memory stick with the Windows platform so that it can be used as a secure storage area for the private keys, means to digitally sign documents and provide public key cryptography to any windows based application that requires it. The development of these solutions will be taken up in two phases.

4.1 SBMS v1 – Secure Biometric Memory Stick (1st Phase)

The Thumbdrive has two storage areas namely the public and private storage space. To gain access to the public storage area you just put the memory stick into the computers USB port and it acts like a normal USB memory stick, however if you want to access the private storage area you

first have to authenticate yourself with your previously enrolled finger. When access is granted to the private storage area the device acts just like a standard USB memory stick, but now all the data that you copy onto the memory stick is encrypted for the authenticated user. To fully utilize this device custom software has to be written with the SDK to interface the USB device.

Firstly we will need a standalone program that will be stored on the public storage part of the memory stick and run automatically when the device is plugged into a computer. This program will then allow you to logon to the memory stick so you can get access to the private storage area where your private key is stored or to digitally sign document. If you want to digitally sign a document you first have to have access to the private storage area. If you are logged on the program will:

1. fetch a copy of the private key from the private storage area of the memory stick and pass it to the computer
2. make a hash of the document
3. encrypt the hash
4. attach it to document
5. delete the copy of the private key from the computer

Secondly having this device you want to be able to use your private key to perform encryption, digital signing, security user login, email encryption, disk encryption, VPN authentication, and other secure client functions. To develop applications that would perform these functions would take a big team of software developers, a lot of time and money. There is however a simpler solution of using existing applications with the biometric memory stick (see Fig 4.1.1), the solutions is CryptoAPI. What is CryptoAPI?

The Cryptography API contains functions that allow applications to encrypt or digitally sign data in a flexible manner, while providing protection for the user's sensitive private key data. All cryptographic operations are performed by independent modules known as cryptographic service providers (CSPs). One CSP, the Microsoft RSA Base Provider, is included with the operating system. [MS01]

Applications that provide encryption functions usually refer to the cryptoAPI to perform these functions. For the SBMS v1 model to work a modified version of the Microsoft RSA Base Provider CSP (Cryptography Service Provider) will have to be written that will work together with the Thumbdrive Swipe. This CSP has to be modified so that it will use the private area of the memory stick as a Key Database. Installing the modified Microsoft certified CSP onto the computer will allow all applications that use cryptoAPI to use the biometric memory stick to store all their keys.

Unfortunately this is the extent that the memory stick can be used with the supplied SDK. The SBMS v1 model will only be used as storage are for the Key Database and for the developed program that will be able to digitally sign document and verify digital signatures on documents.

4.2 SBMS v2 (2nd Phase)

There is a need however to make the device go one step further. This is going to be done by moving all the private key and session key encryption from the computer to the memory stick. The Thumbdrive Swipe is a product that is widely available to the public as a secure storage device that uses symmetric encryption for storage and biometrics for user identification/authentication. This device cannot handle any sort of public key encryption and even though it does symmetric encryption there is no interface to encryption module through the SDK that we got from TREK.

The next step is to build an add-on device that will handle all the encryption and key generation (see fig 4.2.1). With the new add-on in place we will be able to keep the private and session keys stored securely on the memory stick and use them to encrypt messages in a secured environment on the add-on device where the keys cannot be spoofed. The CPS will be modified so that the messages that need to be encrypted/decrypted by the private key will be sent to the new add-on device. These encrypted messages will then be sent back to the CPS. The SBMS v2 is a

prototype solution we are looking into making but its success is totally depended on the ability to make the add-on encryption device. The SBMS v2 model is a flexible solution that can offer its e-commerce users the piece of mind that their electronic identity cannot be stolen by digital spoofing.

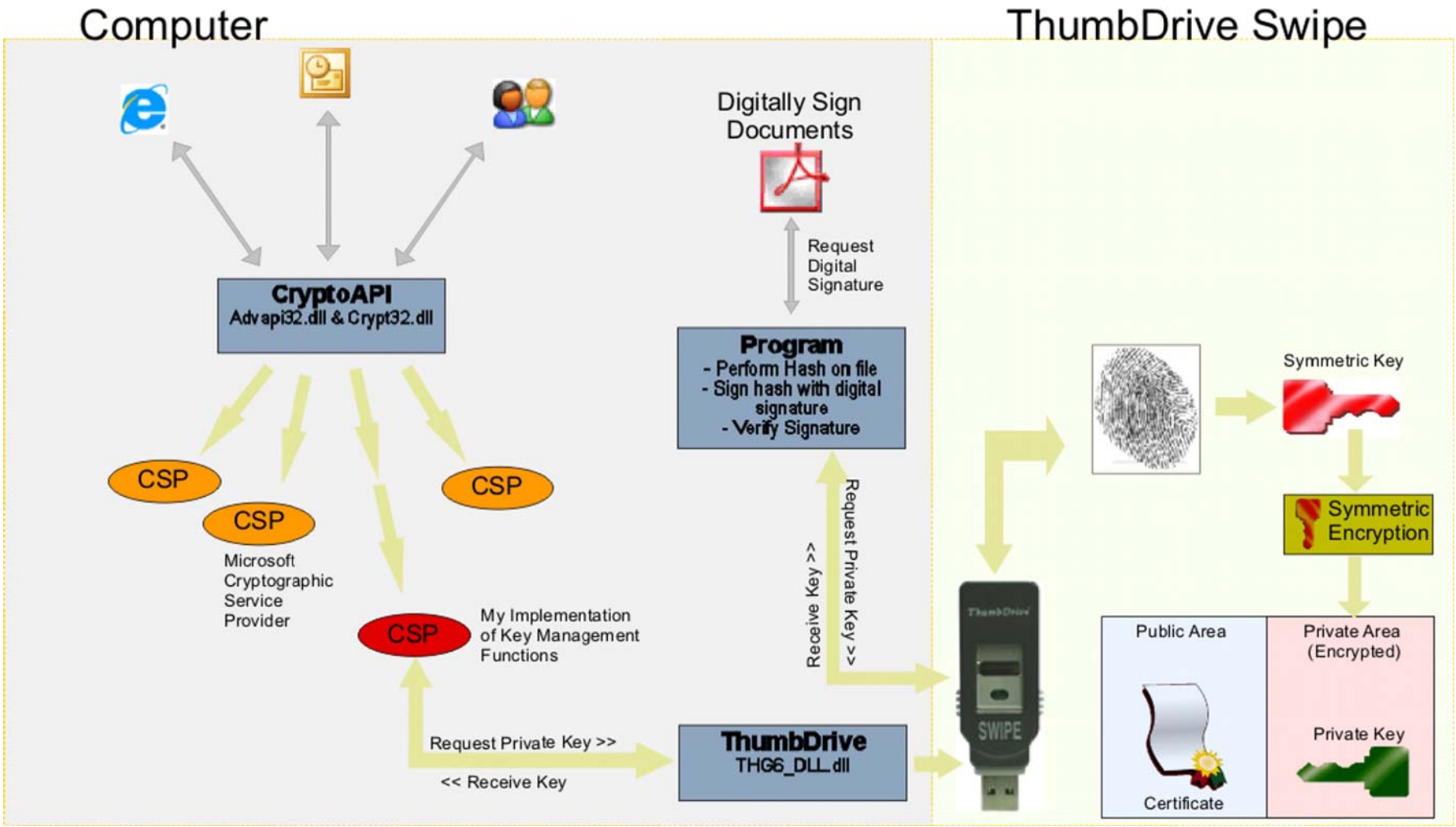

Fig 4.1.1 Working Model of SBMS v1

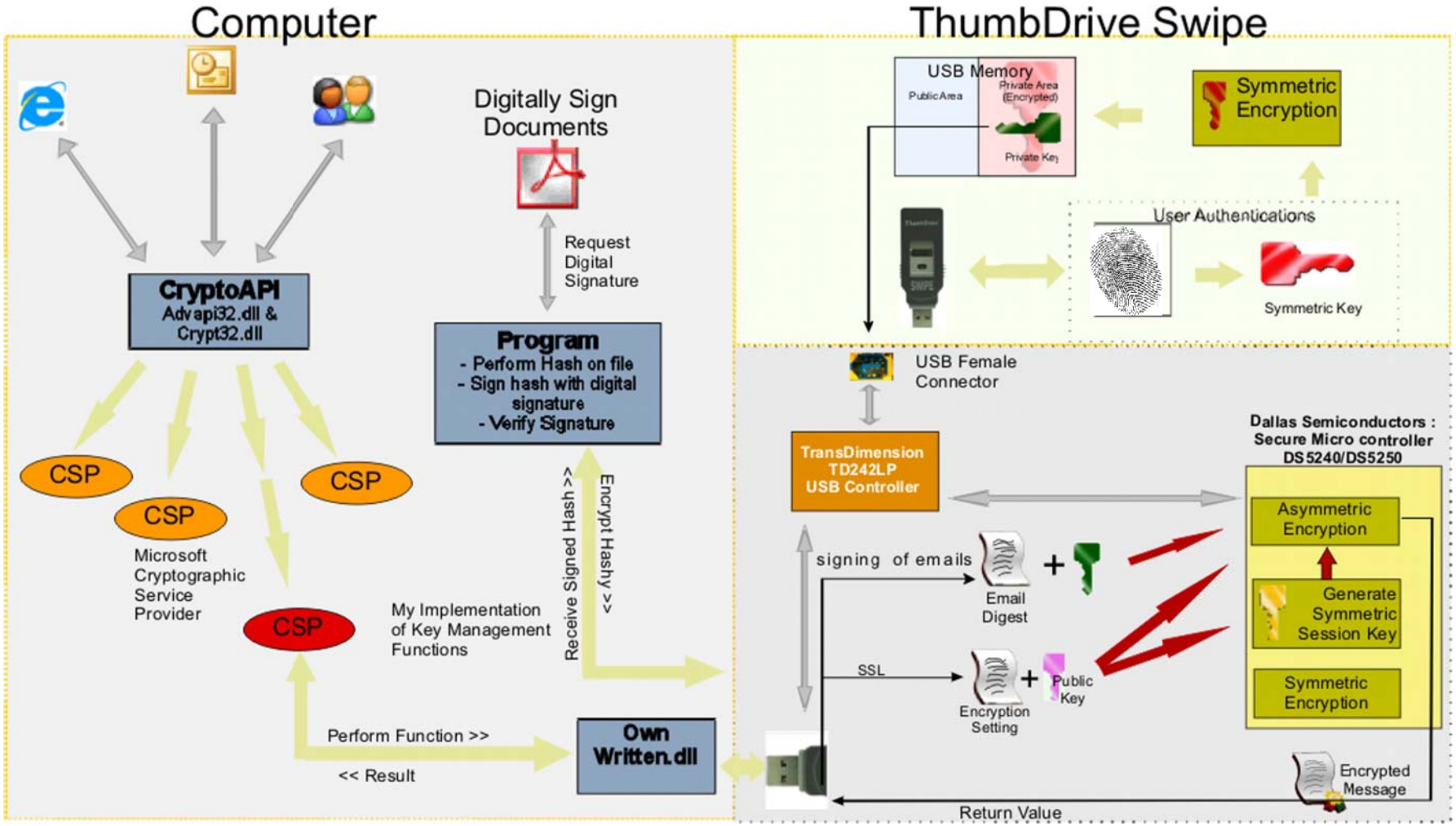

Fig 4.2.1 Working Model of SBMS v2

5 CONCLUSION

There is a need to increase client side security if we want to have trust on Internet. The end users computers are the weakest link in Public Key Infrastructure and this is a solution that addresses this. This research project is still in its infancy stages and I'm sure that a lot of obstacles will be faced before we reach a functional SBMS v2 model. The increase of secure storage devices available on the market has shown that there is a demand for an interoperable secure portable PK device.

6 REFERENCES

[IAIA]: John D. Woodwrd, Jr., Nicholas M. Orlans, Peter T.Higgins

Biometrics – Identity Assurance in the Information Age

ISBN 0-07-222227-1

[TREK]: TREK, Global Engineering solutions provider. Press Release.

(Available on the Internet at: http://www.trek2000.com.sg/press12.htm

Accessed on 15/02/2005)

[UPEK]: UPEK, Hardware Fingerprint Authentication

(Available on the Internet at: http://www.upek.com/support/dl_devkit_e06.asp

Accessed on 15/02/2005)

[COSJ]: Carl Ellison and Bruce Schneier

Computer Security Journal, Volume XVI Number 1, 2000. "Ten risks of PKI: What you're not being told about public key infrastructure"

(Available on the Internet at: http://www.schneier.com/paper-pki.pdf

Accessed on 17/02/2005)

[BPSC]: Frangopoulos, E.D. and Venter, L.M.

Biometric Protection Of Smartcards Through Fingerprint Matching: A Technological Overview And Possible Directions

(Available on the Internet at: http://www.infosecsa.co.za/proceedings2004/011.pdf

Accessed on 13/03/2005)

[FAPS]: Carl W. Tunrner, Merrill Zavod, William Yurick

Factors that Affect the Perception of Security and Privacy of E-Commerce Web Sites

(Available on the Internet at: http://www.sosresearch.org/publications/icecr01.pdf

Accessed on 13/03/2005)

[10XM]: 10xMarketing,

(Available on the Internet at: http://www.10xmarketing.com/e-commerce-statistics/

Accessed on 19/03/2005)

[MS01]: MSDN,

(Available on the Internet at: http://msdn.microsoft.com/library/default.asp?url=/library/en-us/dncapi/html/msdn_cryptapi.asp

Accessed on 02/04/2005)