

## Electronic Filing System Part 2 - What Purpose does the SmartCard Serve?

By [Sylvia Low](#) of Bizibody Pte Ltd

---

### INTRODUCTION

During the conduct of our training courses and EFS - implementation consultancy, one of the most frequent questions we are asked relates to the requirement that all actions through the EFS must be preceded by "inserting" the client's Smart Card into the Smart Card Reader. Why and what purpose does this serve? The answer you are most likely to receive from a harassed trainer who has more than three more hours of an intensive "hands-on" workshop is - to authenticate the sender of the document and to ensure its integrity. Short sharp and succinct, but what does it mean?

We recognise that this question deserves a far more considered response. For this reason we take this opportunity to explain to our clients why the courts have placed its trust on the Smart Card to fulfill the onerous responsibility of ensuring security of electronic transmission. While we cannot avoid some technical jargon involved in explaining PKI and cryptography, we will try our best to do it in terms that a non-techie would understand.

To begin -

### 1. WHY THE NEED FOR SECURITY AND AUTHENTICITY?

The Internet is a notoriously insecure medium as information travels through different shared networks and digital cables before it reaches its final destination. The possibility of interception of digital mail is a real problem as evidenced by the regular occurrence of breaches of security on the Internet; such as "sniffing" (capturing information on a network that is meant for another recipient); "cracking" (unauthorised entry and modification of computer networks) and "spoofing" (taking on the identity of the sender or recipient).

In conventional modes of filing (or service) of legal documents, responsibility is placed on the court clerk or process server to deliver the document by hand, in its original form and intact, to the recipient (an officer of the court or a law firm) who signs an acknowledgement of receipt. To replace conventional modes of delivery, the Internet must provide the same, if not higher, standards of security and proof of delivery.

Public Key Infrastructure ("PKI") Technology has been developed by computer scientists to perform such a function - principally, it allows information to be "digitally signed" by the sender, then sent over in a "sealed envelope" so that only the intended recipient is able to break the seal and read the information.

## 2. HOW DOES PKI WORK?

This is the complicated bit that requires the use of words such as "asymmetric cryptosystem" and "mathematical algorithms"; a full understanding of which requires a degree in advanced applied mathematics.

If you are still with me up to this point, I promise you that the following explanation will impart a sufficient understanding of how PKI works (or at least its essence) to satisfy all except the most die-hard mathematical theorist.

PKI technology comprises 2 fundamental processes - Firstly, the application of a pair of different but mathematically related "keys", one for encrypting data (ie, transforming data into unintelligible form), and another for returning it to its original legible form. Each party owns a pair of keys, one of which is secret (the private key) and the other is publicly known (the public key). It is computationally unfeasible to derive knowledge of the private key from knowledge of the public key; Secondly, the application of the private key performs a hash function on the message. The resulting encryption is sometimes called the sender's "digital signature". However it is more than a mere signature appended to a message. The encryption packet is derived from, and is therefore unique to, both the message and the sender's private key that is used to create it.

How PKI works is explained step-by-step with reference in [this diagram](#) - [\[click here to view\]](#).

### Step 1

The lawyer inserts his smart card into the smart card reader when instructed to do so by the EFS Application. This has the effect of applying the lawyer's private key to encrypt the data that he is transmitting to the court.

### Step 2

The Court receives the encrypted packet, and applies the lawyer's public key to decrypt the data.

This action performs the following security functions -

- a. authentication of the sender (WHO sent the message);
- b. non-repudiation by the sender (he is STOPPED from denying that he sent it); and
- c. integrity of the message sent (proof of ORIGINALITY)

### Step 3

Additionally, the lawyer may choose the "encrypt data" option when prompted to do so by EFS Application. This has the effect of applying the court's public key to the data. The Court applies its private key to the encrypted packet in order to read it. The result is that only the intended recipient (the Court) is able to receive and decrypt the data; thereby ensuring that confidentiality and exclusive knowledge is achieved.

## 3. HOW DOES THE SMART CARD MAKE USE OF PKI TECHNOLOGY TO AUTHENTICATE THE SENDER AND

#### **ENSURES THAT THE DATA IS SECURE WHEN FILING / SERVING THROUGH EFS?**

The Smart Card contains a micro-chip processor that comprises the owner's public key; and the Smart Card Reader is the instrument that computationally generates the owner's private key from his public key and applies the private key to the document that is being filed / served.

#### **4. WHY DO YOU HAVE TO "REGISTER" AT THE JUDICIARY IN ORDER TO RECEIVE YOUR SMART CARD?**

An imposter could substitute his own public key for that of the rightful lawyer; and use his (the imposter's) own private key to encrypt the data he sends to the court in the name of the lawyer or decrypt the data he receives from the court that is meant for the lawyer. To prevent this, the Judiciary has taken on the role of the Certifying Authority to bind every key-pair to the identity of the owner. The Judiciary issues each lawyer his own public key (contained in the Smart Card) upon proof of positive identification. While the Certification Authority keeps a record of all public keys and the identity of owners of each public key, each owner's private key is computationally generated from his public key and the Certification Authority has no knowledge of it.

#### **5. DOES THIS MEAN THAT USE OF THE SMART CARD MAKES EVERY DIGITAL TRANSMISSION ABSOLUTELY SECURE AND FRAUD-PROOF?**

No. Clearly fraud is possible in any system, and PKI technology will not protect the security of the transmission in the following circumstances - (1) The applicant misrepresenting his identity to the Certifying Authority; and (2) The owner losing control of his public key through theft, misuse or misplacement.

#### **6. DOES THE USE OF THE SMART CARD FULFILL THE EVIDENTIAL RESPONSIBILITY IN RELATION TO THE AUTHENTICATION OF THE SENDER, ORIGINALITY OF THE MESSAGE AND PROOF OF DELIVERY?**

Yes. Order 63A of the Rules of Court was amended in 1999 to address this issue. Under the amended rules, the affixation of the authentication code to any document sets up the presumption that - (1) the document has not been altered since the code was affixed; (2) the document was made and transmitted by the registered owner of the code or his authorised agent; and (3) the code was affixed with the intention of signing or approving the document.

#### **7. WHERE CAN I READ MORE ABOUT DIGITAL SIGNATURES, PKI AND ITS APPLICATIONS FOR THE LEGAL INDUSTRY?**

Find out more about Digital Signatures and how it works at -

- <http://www.netlawtools.com/security/emailsecurity1.html>
- <http://www.abanet.org/lpm/newsletters/net2d/s98orr.html>
- <http://www.pgp.com>

- <http://www.netrust.com.sg>

Find out how different jurisdictions have adopted PKI as the standard in secure digital communication -

- Canada - <http://www.juricert.com>
- USA - <http://www.abanet.org/scitech/ec/isc/dsg-tutorial.html>
- EU - <http://www.itsecurity.com/papers/digsig.htm>
- General Issues - <http://ilpf.org/digsig/issues.htm>

Copyright © 2001 Bizibody Pte Ltd

---

### **Author Biodata**

As official Trainers and IT Vendors for the EFS FE-Web, Bizibody has helped more than 160 law firms implement EFS in their office. We provide FREE preliminary consultation on the different aspects of EFS implementation, including - integration with your existing IT setup, upgrades and maintenance, your options for broadband internet access, software & licensing requirements and budget allocation. If you have any questions regarding EFS, send them to - Serena Lim or Sylvia Low at 325 2704 or email to [efs@bizibody.biz](mailto:efs@bizibody.biz)

[Click here](#) to send feedback on the article.