The "smart revolution" begins

by Maciej Rossudowski and Hein S Venter

Have you ever noticed how many different aspects of our lives are getting "smarter"? There are "smart" phones, "smart" cars, "smart" houses, in which all kinds of systems can be electronically controlled, and also the "smart card", of which the most widely used form is the Subscriber Identity Module (SIM) card that is the "mind" of our cellphones.

The smart card can also be used by governments to digitise the population registry, as well as by financial institutions, such as banks, to replace the existing credit card, and by organisations and residential premises as secure access cards. If all of these credit and access cards could be replaced by a *single* reliable smart card, one could indeed talk about "a smart card revolution."

What is a smart card?

A smart card is typically a plastic card in which an integrated circuitry chip (ICC) is embedded. This ICC contains a processor, a certain memory capacity and some program instructions.

It has the ability to process information, which makes it more secure than the existing credit card. One smart card can also be linked to any number of credit cards. The user then simply indicates to the smart card which credit card to select in order to make a payment.

Employees and residents of secure areas are nowadays issued with one or more access cards with which to enter secure parking areas, buildings and sectors in buildings. It is therefore quite possible for one person to end up carrying a number of cards, which is extremely inconvenient and insecure. A single smart card can replace all a user's previous credit and access cards.

One card performs many functions

The disadvantage of using a single smart card to perform all these functions is that it makes the surveillance and monitoring of private citizens by "Big Brother" a whole lot easier. Consequently, a unique architecture needs to be implemented that allows a single smart card to perform all the actions of several different types of cards, such as credit cards and access control cards, while maintaining a high level of privacy and personal information integrity.

The architecture needs to be simple in design, able to activate the different roles that the smart card is required to perform, and it should be user-friendly and easy to process.

An example of this kind of architecture is shown in Figure 1.

This architecture consists of the following elements:

- **The Trusted Third Party (TTP):** An independent organisation that allows two unrelated entities to trust each other because both the entities trust the independent organisation.
- **The smart card:** The card used to perform a task such as paying for purchases by means of a credit card-style transaction.
- **The final entity** (in such a credit card-style transaction): The user's bank.

How the smart card works

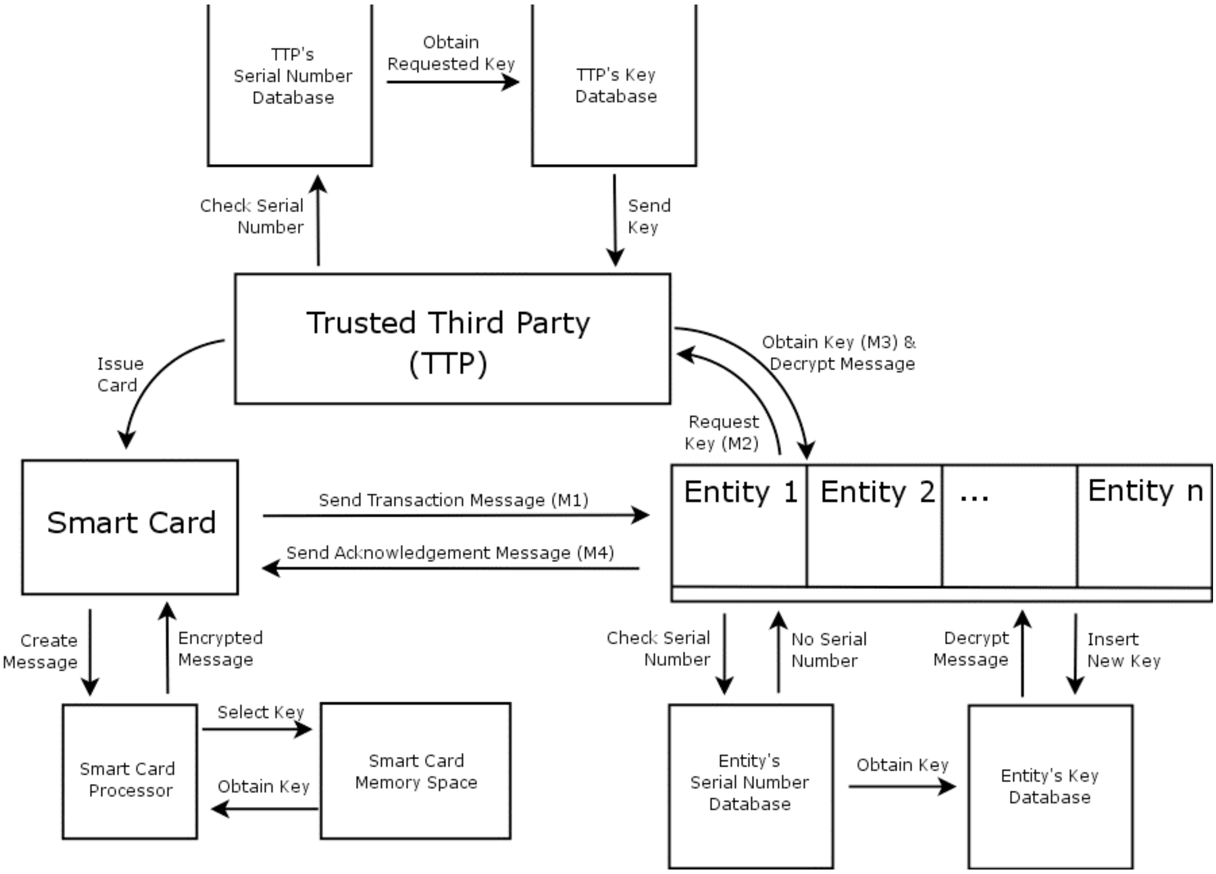
The trusted third party issues a person (the user) with a smart card and stores the user's details (the serial number of the card, the user's first name, family name, date of birth, ID number and a data segment) on the smart card. The data segment contains hundreds of encryption keys randomly generated by the trusted third party and used to guarantee the security and privacy of all the tasks performed by the user.
A record of the data segment is stored on the smart card and is associated with its serial number.

When a transaction is performed, the user enters a personal identification number (PIN) as authentication and selects the credit card or bank to which the transaction should be sent. The smart card encrypts the details of the transaction with a randomly selected encryption key value from the data segment. The encrypted data, serial number of the smart card, and the number of the encryption key value used to encrypt the data are sent to the bank that the user has selected
(M1 in Figure 1).

The bank does not possess the correct encryption key value to successfully decrypt the transaction details and cannot fulfil the requested transaction. It therefore sends the serial number and the number of the encryption key value to the trusted third party via a secure channel (M2 in Figure 1). The trusted third party locates the data segment associated to the particular serial number value, uses the number of the encryption key to retrieve the appropriate encryption key value and deletes it from the data segment. The encryption key value is then sent back to the bank (M3 in Figure 1). The bank successfully decrypts the transaction details received from the smart card and fulfils the request.

A new encryption key value (EK2) is created by the bank and stored in its database. The bank associates it with the serial number value of the smart card, manufactures a reply to the smart card, which consists of the bank's identification code, whether or not the request was fulfilled, and the new EK2 value. This reply is encrypted with the original encryption key value (EK1) and sent back to the smart card (M4 in Figure 1). The smart card decrypts the message, replaces the encryption key value (EK1) used to encrypt this transaction with the new encryption key value (EK2) and associates the new encryption key value with the bank's identification code.

Whenever the user chooses to perform another transaction with that particular bank, the smart card searches its memory for an encryption key that is



→ *1. An overview of the architecture that will allow cross-application use of a single smart card*

assigned to the bank's identification code. Once found, it uses the encryption key to encrypt the transaction message. The encrypted message is then sent to the bank. The bank recognises the serial number of the smart card because its value is stored within the bank's database, and it locates the associated encryption key with which to decrypt the message.

It is usable, reliable and secure

This last step is fundamental to the usability of the architecture. If it is not performed, two critical problems appear. It would be necessary to contact the trusted third party for each transaction that the user wishes to perform (the "Big Brother" effect). The encryption keys on the card would be used up quickly and the card would need to be replaced.

Once the user has therefore performed one (initial) transaction with a bank, the trusted third party is not required to assist with any future transactions. The privacy of transactions will now be protected because the transaction details have been encrypted, and the user and the bank will only need to be contacted after the initial transaction has taken place. Although the trusted third party might be able to infer that a particular user undertook a transaction with a particular bank(s), it cannot obtain any information about the transaction itself.

This architecture has the flexibility to be used in a wide variety of applications, from banking to access control. It protects privacy by encrypting every message that the smart card sends, and it uses a new encryption key for each message.

The greatest advantage of this architecture is its usability and reliability, as it offers users and financial institutions a high degree of privacy and superior usability by allowing cross-application usage from a single smart card.

With architecture of this kind, one can truly talk about "a smart card revolution" that will make life easier and more convenient without opening up possibilities of unethical surveillance and criminal intrusion.

***Mr Maciej Rossudowski** and **Prof Hein Venter** are associated with the University of Pretoria's Department of Computer Science. For more information on the work of the Information and Computer Security Architectures (ICSA) Research Group of the University of Pretoria, contact AM Rossudowski at amrossudowski@cs.up.ac.za or Prof HS Venter at hsventer@cs.up.ac.za*