

## **Choosing an appropriate Security Model – ITSO as an example**

Most of us use smartcards in some form or another. A look through your wallet will confirm this. In the modern world we live in, we carry a variety of smartcards around with us, from our bank cards and credit cards to our travel card and sometimes we require a card to give us access to the office buildings we work in. We also have them in our mobile phones where they ensure that we get to speak to whom we want, and that we are billed correctly. With so many cards it seems inevitable that many cards will become few, with one card that can perform the functions of many. How do we know whether our private and confidential information for each application will remain in the secure environments that will keep our information protected? After all, security is a chain; it's only as strong as the weakest link.

### **There are already established and trusted forms of security – so why worry?**

One of the newest forms of security at the moment is that of biometrics. Biometric verification is any means by which a person can be uniquely identified by evaluating one or more distinguishing biological traits. Unique identifiers include fingerprints, hand geometry, earlobe geometry, retina and iris patterns, voice waves, DNA, and signatures. A current example is the use of biometrics in schools whereby children are using their fingerprint to identify themselves when paying for their lunch. This is a controversial system that has raised several debates.

The use of biometrics in digital security has multiple problems. The means for acquiring biometric records can be expensive and are not always easy to retrieve. Once an individual's biometrics have been compromised, they are compromised for life and can never be trusted again.

The major issue concerning the use of biometrics within the general public is that there is a great resistance in handing over personal data and it is viewed as an intrusion of privacy. The infrastructure concerning biometrics must be robust in order for it to be sustainable. This infrastructure is not always user friendly and can be difficult to operate.

One commonly suggested form of security used is that of PKI (Public Key Infrastructure) whereby a framework is created using a robust, secure method for exchanging information based on key cryptography. PKI works

through the use of a public and a private key pair that is obtained and shared through trusted authorities (Certificate Authority, Registration Authority, etc.).

For example when you pay for goods or services using your credit card, data is exchanged and received through these private and public keys and a digital certificate is provided to confirm the authenticity of both parties. The Digital certificate holds the owner's name, serial number, expiration date, digital signature and public key. The CA takes liability for the authenticity of the public key produced by the certificate, thus enabling a secure communication environment.

Flaws, however, do exist within a PKI security system. Since the private keys and digital certificates for PKI are often stored in PC hard drives, physical access to the PC by users other than the private key holder could compromise the security of encrypted data and digital signatures.

Digital certificates are more suited to transactions that don't require the certificate to reside on the smartcard itself. Smartcards have limits regarding the amount of information they can hold. It is not always feasible to place a digital certificate onto a smartcard, as it significantly reduces the memory available and can leave the card with little or no available space to hold any other applications.

Scheme operators really want to be able to choose a security environment that suits their needs and do not want to over-engineer a solution. What is the point of buying a heavy safe to protect a ten-Euro note when it is safe enough and much more convenient in your wallet? However, if you have thousands of Euros of gold to protect, then a safe makes more sense. If you have both cash and gold, then you need both a wallet and a safe – and know when to use which one.

## **So what is the alternative?**

Ecebs have devised a patented technology that provides a 'best fit for all' for smartcard deployments. Our technology is a major advance in the simplification of the deployment and use of Smartcards. It creates a viable and secure environment for multi-application cards in which space and functionality is not compromised. Multefile™ is in effect a framework and platform that allows you to develop smartcard applications and solutions quickly and flexibly. It will also work with a variety of applications and security approaches and can be used to provide other applications such as I.D., computer logon, PIN or password applications, payment applications such as EMV etc. All of these applications may have different requirements for the security of the system involved i.e. may be based on PKI (certificate based asymmetric), triple DES authentication (symmetric), user name and password, PIN verification. Multefile™ is used to support and manage these different requirements to security.

## **Proven Technology**

Multefile™ enabled solutions from Ecebs have made it possible for any organisation to securely devise, implement and manage its own smartcard products. It enables rapid timescales for changing and updating applications that would not otherwise be available.

## **The ITSO security model**

A prime example of where this type of technology has been successfully deployed is within the UK transport industry via the ITSO specification. ITSO is a nonprofit making organisation that is owned by its members, who represent local government bodies, transport operators and suppliers. The ITSO specification has enabled interoperable smartcards to become a reality in the U.K.

ITSO was developed in 1998 by UK Transport Executives with the mission to manage and develop the technology specifications that make interoperable, multi-modal public transport a reality. ITSO is unique in transport smartcard schemes in that it covers all components - card, point of service and back office systems. In other words, it allows transport operators and local authorities to deploy fully integrated end to end smart card ticketing solutions. It allows operators the option to 'mix and match' elements, such as cards, software and equipment from different suppliers.

To ensure security throughout, a system that can be trusted by all parties known as the ITSO Security Management System (ISMS) was developed. This enables licensed ITSO members to be confident in the overall integrity of their ITSO compliant deployments. The ISMS works in conjunction with the ITSO secure application model (ISAM). These are located in every POST (point of sale terminal) and HOPS (a back office system which processes and stores all transaction information).

Through the interaction of these two components (ISMS and ISAM), trust is created and enforced through the use of symmetric and asymmetric key cryptography. These keys ensure evidence exists for each ticket transaction and that no such event can be lost or modified. In simple terms, it provides commuters with a smooth, time efficient and secure journey process.

Ecebs designed the ITSO Secure Application Module (ISAM) which is the security enforcing component present in all terminal equipment, e.g. ticket machines and access gates, as well as in every element of the ITSO back office systems. Ecebs also developed and continues to support the ITSO

Security Management System (ISMS) which sits at the top of the pyramid of trust in the ITSO hierarchy. Both the ISMS and the ISAM contain embedded elements of our core software technology, Multefile™.

Multefile™ plays an integral role in the ITSO security system as it handles all ITSO specific security functions through the use of symmetric and asymmetric cryptography. The core component of ITSOs security, the ISAM can carry a huge amount of data which must be structured and managed. The ISAM and ISMS are systems based on Multefile™ which enables the entire ITSO system to be updated in real-time. This enables the full system to remain secure at all times. If any security breach were to occur the ISMS, enabled by Multefile™, would simply send new cryptographic keys to the ISAM which in turn would update the entire system via the HOPS.

As proven in the ITSO deployment, Multefile™ enabled smartcards are far more competitive by adapting to change as a matter of course instead of an exceptional and most often, costly event.

ITSO based interoperable ticketing has proven to be a huge success in the U.K. and allows the opportunity to have more than just travel entitlements on a smartcard. Ecebs smartcard knowledge and experience has allowed us the opportunity to play a key role in the ITSO environment from its very beginning.

The use of multi-function smartcards is on the increase and the capabilities exist for one card to be a transport card, bank card, library card, loyalty card etc. It is pretty easy technically to deliver a system with a card that you could use to withdraw money, board a train from Paris and paying for your coffee all on the one card. Sorting out the commercial relationships is a far bigger issue! These different functions are enabled on one smartcard through different applications that reside on the card and each application requires its own level of security. Worldwide there are many different smartcard deployments which require different levels of security and these are approached and resolved in a large variety of ways. Systems such as ours are emerging that help you to 'glue' these together and also allow you to change things after issuance. In the ITSO example, the systems allow for new cryptographic keys to be issued, amended and additional security to be added.

Multefile™ allows smartcard deployments to be future proof as changes, amendments and/or additions can be carried out after the deployment has been implemented with no disruption to the operation. Updates can effect changes on an individual card whilst all other cards remain unchanged and as a result maintain the security of the full deployment. This also enables a powerfully personal smartcard within a large or small scale deployment. This benefits both the user and business. Multefile™ technology minimises the future financial impact for smartcard operators, but still offers a solution that can grow with the changing needs of both operator and customer.

---

## **About Ecebs**

Ecebs don't try to sell only an 'off the peg' solution to our customers, we listen to the customers' requirements and devise product and solutions that meet and exceed the customers' business case without the need to replace legacy systems. Moreover once you have an Ecebs product, based on our Multefile™ technology, there is a stream of benefits available.

Ecebs can also provide a choice of components and solutions to assist and enable customers in the rollout of schemes which require ITSO technology.

Further information can be found on the Ecebs website at:

[www.ecebs.com](http://www.ecebs.com)

Alternatively, contact Ecebs directly via email at:

[enquiries@ecebs.com](mailto:enquiries@ecebs.com)

Or by phone on +44(0) 1355 272911